Skyscraper Project

Version: October 12, 2022

Compiler: HAO PENG
hao_peng@mit.edu

Peking University
Massachusetts Institute of Technology
Preface

This is a note containing subtle or important materials I encountered while studying. I started this project in the fall of my third undergraduate year (October 2019) in Peking University, noticing that I have a poor memory and consistently forget what I have already learned. So it came to me that I can compile all the proofs of theorems I cannot recall that is hard and subtle yet appearing over and over again. But finally it turns out I want to make it as comprehensive as possible. Here it is!

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

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

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

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

- Use less words and more math symbols and equations, and use plain English, so that even those who don’t speak English can understand without much effort.
- A theorem is a proposition that seems more important or general among others.
• A lemma is a statement that seems to be only useful proving its corresponding proposition or theorem.

• A corollary is a proposition that can be deduced quite easily from it corresponding proposition or theorem.

• A conjecture is a statement whose proof is unknown yet.

• The naming of lemmas/propositions/theorems/conjectures by multiple authors follows the lexicographical order.

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

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

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

The writing style of this note is influenced by various literature, including beautiful writings of J. S. Milne, especially [Mil17][Mil17d] and [Mil08].

Copyright issue: It should be made clear that I took proofs from many different places, so nothing in this note should be considered originated from me. Until I get a full extensive references of this note, I have few rights to the material. But I am currently too busy being a graduate student, so many references are still missing. Tell me if you think I should cite you. Nevertheless, I hope this note can contribute to my study and help anyone who read it. But it comes with no warranty, please use at your own risk.

How to cite this note: Don’t cite this note for now.
“And they said, Go to, let us build us a city and a tower, whose top may reach unto heaven; and let us make us a name, lest we be scattered abroad upon the face of the whole earth.”

–Genesis 11:1-9
### Table of Contents

**Chapter 1 – Mathematical Logic and Foundations**

1.1 Zermelo-Fraenkel Set Theory with Choice ...................................................... 1  

1.2 Model Theory ............................................................................................... 14  

**Chapter 2 – Algebras**

2.1 Group Theory ............................................................................................... 31  

2.2 Abstract Algebra .......................................................................................... 48  

2.3 Linear Algebra ............................................................................................. 73  

2.4 More on (Non-Commutative)Algebras ......................................................... 92  

2.5 Lie Algebras ................................................................................................. 108  
2.6 Infinite Dimensional Lie Algebras ................................................................. 143

2.7 Reflection Groups and Coxeter Groups .......................................................... 144

2.8 Algebraic K-Theory ....................................................................................... 155

2.9 Hopf Algebras .................................................................................................... 158
(1) Hopf Algebras. (2) Commutative Hopf Algebras. (3) Quiver Hecke Algebra.

Chapter 3 – Categories and Algebraic Topology

3.1 Categories ......................................................................................................... 165

3.2 Categorical Logic ............................................................................................ 189

3.3 Homological Algebra ....................................................................................... 197

3.4 Derived Categories ........................................................................................... 212

3.5 Differential Graded Algebras ............................................................................. 233
(1) dg-Categories. (2) Sheaves of DGAs.

3.6 Topology I ......................................................................................................... 234

3.7 Model Categories ............................................................................................ 254

3.8 Topology II ....................................................................................................... 267
(1) Topological Groups. (2) Hausdorff Geometry. (3) Spaces from Algebraic Geometry. (4) Spectral Spaces.
3.9 Algebraic Topology I: Homotopies ................................................................. 279

3.10 Algebraic Topology II: Homologies and Cohomologies ................................................................. 295

3.11 Fiber Bundles & K-Theory ......................................................................... 314

3.12 Simplicial Homotopy Theory ...................................................................... 336

3.13 Higher Topos Theory .................................................................................. 356
(1) Introduction. (2) $\infty$-Categories. (3) $\infty$-Category of $\infty$-Categories. (4) Limits and Colimits. (5) Presentable and Accessible $\infty$-Categories. (6) $\infty$-Algebras. (7) Topological Cyclic Homology Theory(Scholze).

3.14 Stable $\infty$-Categories ............................................................................... 362
(1) Stable $\infty$-Categories. (2) Monoidal $\infty$-Categories.

Chapter 4 – Commutative Algebras

4.1 Commutative Algebra I .................................................................................. 363

4.2 Commutative Algebra II .................................................................................. 379

4.3 Commutative Algebra III .............................................................................. 402

4.4 Commutative Algebra IV .............................................................................. 419

4.5 $p$-adic Commutative Algebras ...................................................................... 445
(1) $F_p$-Algebras. (2) $p$-Local Rings. (3) Witt Theory. (4) $\delta$-Rings.
4.6 Derived Commutative Algebras ................................................................. 460

4.7 Divided Power Algebras ............................................................................. 473
(1) de Rham Complex.

4.8 Almost Ring Theory .................................................................................. 482

Chapter 5 – Algebraic Geometry I: Scheme Theory

5.1 Sites, Sheaves and Stacks .......................................................................... 491

5.2 Ringed Topoi, Ringed Sites, Ringed G-Spaces and Schemes ......................... 515

5.3 Cohomology on Ringed Sites ....................................................................... 535

5.4 Properties of Schemes ................................................................................. 557

5.5 Quasi-Coherent Sheaves on Schemes .......................................................... 585

5.6 More Properties of Schemes ....................................................................... 607

5.7 Cohomology of Schemes ............................................................................. 625

5.8 Topics in Schemes ...................................................................................... 639
5.9 Resolution of Singularities .................................................................................. 659
5.10 Varieties ............................................................................................................. 660
(1) Varieties. (2) Projective Varieties. (3) Birational Geometry. (4) Others. (5) Relative
Varieties.

5.11 Curves .............................................................................................................. 667
(1) Basics. (2) Vector Bundles. (3) Singularities and \( \delta \)-Invariants. (4) Linear Series. (5) Hyper-
Curves.

5.12 K3 Surfaces ..................................................................................................... 689

Chapter 6 – Weil Cohomologies and Motives

6.1 Intersection Theory ............................................................................................ 691
for Line Bundles.

6.2 Algebraic de Rham Cohomology ........................................................................ 716
(1) de Rham Complexes. (2) De Rham Cohomologies. (3) Cup Products. (4) Poincaré Duality.

6.3 Étale Fundamental Groups .................................................................................. 719
(1) Étale Connected Components. (2) Étale Fundamental Groups. (3) Galois Inverse Problem.

6.4 Étale Cohomology Theory .................................................................................. 721
(1) Basics. (2) Constructible Sheaves. (3) Base Changes. (4) Lower Shriek Functor. (5) Co-
homology with Compact Support. (6) Finiteness Theorems. (7) \( \ell \)-adic Étale Cohomologies.
(8) Curves.

6.5 Pro-Étale Cohomology ....................................................................................... 740
(1) Introduction. (2) Ring-Theoretical Stuff.

6.6 Crystalline Cohomology .................................................................................... 742

6.7 Prismatic Cohomology ....................................................................................... 750
(1) Prisms. (2) Perfect Prisms. (3) Integral Perfectoid Rings. (4) Prismatic Site. (5) Hodge-
Tate Comparison. (6) Proof of Hodge-Tate Comparison. (7) Derived de Rham Cohomology.
(8) Derived Prismatic Cohomology. (9) \( q \)-de Rham Cohomology. (10) Étale Comparison.
(11) Almost Purity.

6.8 Motives ............................................................................................................. 767
(1) Weil Cohomology Theories. (2) Pure Motives. (3) Mixed Motives. (4) Standard Conjec-
tures.
**Chapter 7 – Algebraic Geometry II: Group Theory**

### 7.1 Group Schemes I: Structure Theory .............................................................. 777

### 7.2 Group Schemes II: Solvable Groups ...................................................................... 797

### 7.3 Group Theory III: Reductive Groups .................................................................. 809

### 7.4 Topics in Group Schemes .................................................................................. 819
1. over Finite Fields.

### 7.5 Formal Groups and $p$-Divisible Groups ........................................................... 820

### 7.6 Geometric Invariant Theory .............................................................................. 835

### 7.7 Moduli Problems .............................................................................................. 836

### 7.8 Algebraic Stacks .............................................................................................. 850

### 7.9 Group Algebraic Spaces ..................................................................................... 852
1. Quotient of Groupoids.  2. Quotients of Schemes.

### 7.10 Higher Dimensional Geometry ....................................................................... 854

**Chapter 8 – Algebraic Geometry III: Derived Algebraic Geometry**

### 8.1 Simplicial Commutative Algebras .................................................................... 855

### 8.2 Andre-Quillen-Cohomology ............................................................................ 861

### 8.3 Derived Algebraic Geometry(Lurie) ................................................................ 867
Chapter 9 – Algebraic K-Theory of Schemes

9.1 K-Theory of Schemes ................................................................................................. 869
   (1) K-Groups of Schemes.

9.2 Brauer-Grothendieck Groups .................................................................................. 870
   (1) Brauer Groups. (2) Brauer Groups of Fields. (3) Severi-Brauer Varieties. (4) Norm Residue
   Isomorphism Theorem.

Chapter 10 – Condensed Mathematics and Analysis

10.1 Profinite Cohomology .............................................................................................. 877
   (1) Group Cohomology. (2) Cohomology of Profinite Groups. (3) Galois Cohomology.

10.2 Condensed Mathematics(Scholze) ........................................................................ 889
   (1) Introduction. (2) Condensed Objects. (3) Cohomologies. (4) LCAs. (5) Solid Abelian

10.3 Topological Commutative Algebra ........................................................................ 894
   (1) Topological Abelian Groups and Rings. (2) Valuation Rings. (3) Valuations. (4) Affinoid
   Algebras. (5) Huber Rings. (6) Analytic Points and Analytic Huber Pairs. (7) Huber and

10.4 Real Analysis ........................................................................................................... 923

10.5 Complex Analysis .................................................................................................... 933
   (1) Basics. (2) Complex Integration. (3) Series and Product Developments. (4) Analytic
   Continuations. (5) Theorems. (6) Harmonic Functions. (7) Elliptic Functions. (8) Special
   Functions. (9) Multi-Variable case.

10.6 General Functional Analysis ................................................................................... 954
   (1) Topological Vector Space. (2) Completeness. (3) Dual Space. (4) Banach Space.

10.7 Archimedean Functional Analysis ........................................................................ 959
   (1) Topological Vector Space. (2) Various Spaces and Duality. (3) Convexity. (4) Duality

10.8 Archimedean Banach Algebra ................................................................................ 975
   (5) Hilbert-Schmidt Operators and Trace Classes.

10.9 Analysis on Locally Compact Groups .................................................................... 991
   (1) Locally Compact Groups. (2) Unitary Representations. (3) Locally Compact Abelian
10.10 Harmonic Analysis ................................................................. 1019
(1) Distributions. (2) Fourier Analysis on $\mathbb{R}^n$. (3) Sobolev Space. (4) Fourier Analysis on $\mathbb{T}^n$.

10.11 Differential Operators ......................................................... 1026

10.12 D-modules ............................................................................ 1034

10.13 Dynamic System .................................................................. 1035

Chapter 11 – Differential Geometry

11.1 Geometric Analysis ............................................................... 1045

11.2 Riemannian Geometry ............................................................. 1063

11.3 Low Dimensional Topology .................................................... 1079

11.4 Differential Forms in Algebraic Topology(Bott-Tu) ..................... 1082
(1) Basics.

11.5 Symplectic Geometry ............................................................. 1083
(1) Basics.

11.6 Lie Groups ............................................................................. 1084

11.7 Complex Geometry ................................................................ 1109

11.8 Kähler Geometry ................................................................. 1117
11.9 Locally Symmetric Spaces ................................................................. 1130
(1) Symmetric Spaces. (2) Decompositions of Symmetric Spaces. (3) Non-Compact Type.
(7) Quotients of Hermitian Symmetric Domains.

11.10 Compactifications of Locally Symmetric Spaces ............................... 1135

11.11 Calabi-Yau Manifolds .................................................................... 1136

Chapter 12 – Algebraic Number Theory

12.1 $p$-adic Analysis ........................................................................... 1137
(1) (Ultranormed) Valuation Theory. (2) Ultranormed Banach Spaces. (3) $p$-adic Analysis.

12.2 Algebraic Number Theory ............................................................... 1146
(5) Adele and Idele. (6) Fourier Analysis on Adeles and Ideles.

12.3 Quadratic Forms over Fields ......................................................... 1171
(1) Quadratic Forms. (2) Witt Theory. (3) Witt Ring. (4) Quaternion Algebras. (5) over
Local or Finite Fields. (6) over Global Fields. (7) Algebraic Extensions.

12.4 Cohomology of Number Fields ...................................................... 1184
(1) Abstract Class Field Theory. (2) Local Class Field Theory. (3) Global Class Field Theory.
(4) Brauer Groups of Local and Global Fields. (5) Decomposition Law. (6) L-Series and
(9) Cohomology of Global Fields.

12.5 Transcendental Number Theory ..................................................... 1201
(1) Transcendental Numbers. (2) Periods. (3) Periods and Differential Equations. (4) Periods
and L-Functions. (5) Periods and Motives.

Chapter 13 – Arithmetic Geometry

13.1 Pseudo-Algebraically Closed Fields ............................................. 1203

13.2 Diophantine Geometry .................................................................. 1204
(1) over Local Fields. (2) over Global Fields. (3) Artin’s Conjecture. (4) Weil Heights. (5) Dio-

13.3 Arithmetic of Algebraic Groups .................................................... 1216
(1) over $p$-adic Number Fields. (2) Over Global Fields. (3) over Adeles.

13.4 Arithmetic Subgroups .................................................................... 1220
(1) Arithmetic Subgroup of Lie Groups.
13.5 Arithmetic of Abelian Varieties ...................................................... 1221

13.6 Surfaces and Arithmetic Surfaces ...................................................... 1249

13.7 Reductions ..................................................................................... 1254
(1) Semistable Reductions. (2) Reduction of Curves.

13.8 Arithmetic of Elliptic Curves ............................................................ 1256

13.9 Complex Multiplication Theory ......................................................... 1280

13.10 Arithmetic Moduli of Elliptic Curves ................................................. 1290
(1) Moduli Problems.

13.11 Arithmetic of K3 Surfaces ............................................................... 1291

13.12 ℓ-adic Étale Cohomologies over Finite Fields .................................... 1292

13.13 Rational Points on Abelian Varieties ................................................. 1312

13.14 Shimura Varieties ........................................................................... 1318

13.15 Mordell-Lang Conjecture (Faltings Theorem) .................................... 1321
(1) Tate Hom Conjecture. (2) Heights of Abelian Varieties. (3) Finiteness Theorems. (4) Curves.

13.16 Tate Conjecture & Hodge Conjecture .............................................. 1325
(1) Statements. (2) over Finite Fields. (3) K3 Surfaces. (4) Hodge Conjecture.
Chapter 14 – $p$-Adic Geometry

14.1 Galois Representations .................................................................1331

14.2 $p$-adic Hodge Theory .................................................................1337
(1) Intro. (2) $(\varphi, \Gamma)$-modules. (3) Isocrystals. (4) Admissible Representations. (5) $\mathbb{C}_p$-Admissibility and Hodge-Tate Representations. (6) Sen’s Theory and Hodge-Tate Representations. (7) Admissible Representations. (8) Crystalline Representations.

14.3 $p$-adic Modular Forms ...............................................................1350

14.4 $\mathbb{F}_p$-Schemes ......................................................................1351
(1) Perfect Schemes.

14.5 Formal and Rigid Geometry .........................................................1353

14.6 $p$-adic Uniformizations ...............................................................1372
(1) Mumford Curves.

14.7 Rapoport-Zink Spaces ................................................................1373
(1) Isocrystals with Additional Structures. (2) Period Domain. (3) Algebraic Groups of EL/PEL Types.

14.8 Adic Spaces and Perfectoid Spaces (Scholze) ............................1381

14.9 Fargues-Fontaine Curve ..............................................................1406

14.10 Pro-Étale Sites on Perfectoids and Diamonds ............................1429
(1) Properties of Perfectoid Spaces. (2) Pro-Étale Site and v-Site. (3) Morphisms of v-Stacks. (4) Diamonds.
Chapter 15 – Representation Theory

15.1 Classical Representation Theory ..........................................................1441
(1) Topological Representations. (2) Linear Representation of Finite Groups. (3) Symmetric Groups. (4) Locally Profinite Groups.

15.2 Modular Representations ..................................................................1461
(1) Block Theory. (2) Unequal Characteristic. (3) Equal Characteristic.

15.3 Representations of Algebraic Groups ...............................................1462

15.4 Complex Representations of Finite Groups of Lie Type ...................1469

15.5 Bruhat-Tits Theory .......................................................................1477

15.6 Representations of (Non-Compact)Lie Groups ................................1478
(1) Basics. (2) Finite-Dimensional Representations. (3) (g, K)-Modules. (4) Unitary Representations.

15.7 Automorphic Representations of GL(n) over Archimedean Local Fields......1495

15.8 Admissible Representations of GL(n) over p-Adic Number Fields ...........1513

15.9 Cuspidal Representations ..............................................................1542
(1) GL(n). (2) SL(n).

15.10 Adelic Automorphic Representations of GL(n) .............................1543

15.11 Modular Forms .............................................................................1555

15.12 Overview of the Langlands Program .............................................1576
(1) Langlands Program. (2) Local Langlands. (3) Global Langlands Correspondence. (4) Beyond Endoscopy.
15.13 Local Langlands for GL(n) over p-Adic Fields ..................................................1580
(1) Local Langlands for p-adic GL(n). (2) Cuspidal Representations. (3) Simple Characters.
(4) Tame Lifting. (5) Description of the Langlands Correspondence.

15.14 Automorphic Forms Beyond GL(2) .......................................................................1583
(1) Automorphic Forms on Unitary Groups. (2) Quaternionic Modular Forms. (3) Theta Correspondence. (4) Weil Representations. (5) Gan-Gross-Prasad Conjecture.

15.15 Representations of Semisimple Lie Algebras and Category O .................................1589
(1) Semisimple Representations. (2) Verma Modules. (3) Weyl Character Formula. (4) Category O.

15.16 Trace Formulae ...........................................................................................................1598
(1) Introduction. (2) Trace Formulae.

Chapter 16 – L-Functions

16.1 L-Functions Attached to Motives .................................................................................1601
(1) over Finite Fields. (2) over Global Fields. (3) Motivic L-Functions. (4) Abelian Varieties.
(5) Elliptic Curves. (6) Tamagawa Number Conjecture. (7) Others.

16.2 L-Functions Attached to Automorphic Representations .............................................1607

16.3 L-Functions Attached to Galois Representations ........................................................1633

16.4 p-adic L-Functions ........................................................................................................1636
(1) p-Adic L-Functions. (2) Iwasawa Main Conjectures. (3) Iwasawa Main Conjectures for GL(2).

16.5 Heegner Points ..............................................................................................................1637

16.6 Gan-Gross-Prasad Conjecture .....................................................................................1640
(1) Introduction. (2) restriction Problems. (3) Statements. (4) Arithmetic Fundamental Lemma.

16.7 Colmez Conjecture .......................................................................................................1641
(1) Averaged Colmez Conjecture.

16.8 BSD Conjecture ..........................................................................................................1642
(1) Statements. (2) Low Rank Cases. (3) over Function Fields. (4) Motivic BSD Conjectures.
16.9 Shimura-Taniyama-Weil Conjecture .............................................................1646
(1) Modularity. (2) L-Functions. (3) Fermat’s Last Theorem.

16.10 Special Values of L-Functions .....................................................................1649
(1) Deligne Conjecture. (2) Beilinson-Bloch Conjecture. (3) Bloch-Kato Conjecture. (4) Height Pairings.

16.11 Riemann Conjecture ..........................................................................................1651
(1) Hilbert-Pólya Conjecture.

Chapter 17 – Arakelov Geometry
17.1 Arithmetic Intersection Theory .....................................................................1653
(1) Arithmetic Riemann-Roch.

17.2 Arakelov Geometry ..........................................................................................1654
(1) Metrized Line Bundles.

Chapter 18 – Theoretical Physics
18.1 Quantum Mechanics ..........................................................................................1655
(1) Basics. (2) Quantum Computations. (3) Quantum Algorithms.

18.2 Quantum Field Theory ......................................................................................1660
(1) Supersymmetric Quantum Field Theory. (2) Topological Quantum Field Theory.

Chapter 19 – Combinatorics
19.1 Combinatorics ....................................................................................................1663
(1) Graph Theory. (2) Ramsey’s Theory. (3) Polytopes. (4) Hilbert’s 3rd Problem.

Chapter 20 – Others
20.1 Elementary Mathematics ....................................................................................1671
(1) Algebra. (2) Number Theory.

20.2 French to English Dictionary ............................................................................1675

Chapter – Notations

Chapter – References

Chapter – Index
1 Mathematical Logic and Foundations

1.1 Zermelo-Fraenkel Set Theory with Choice

Main references are [H-J99], [Model Theory Marker].
Set theory is one choice of foundation of mathematics. And many propositions need efforts to be made rigorous. Another choice of foundation of mathematics is the homotopy type theory(HoTT).

1 Basic Axioms

Axiom (1.1.1.1) [Axiom of Existence]. There exists a set which has no elements.

Axiom (1.1.1.2) [Axiom of Extensionality]. If every element of $X$ is an element of $Y$ and every element of $Y$ is an element of $X$, then $X = Y$.

Cor. (1.1.1.3). There is at most one set which has no elements, it is called the empty set $\emptyset$ or 0.

Def. (1.1.1.4). Write $x \in X$ if $x$ is an element of $X$.

Def. (1.1.1.5). Write $A \subset B$ iff $\forall x, x \in A \Rightarrow x \in B$.

Axiom (1.1.1.6) [Axiom Schema of Comprehension]. For any set $A$, if $P(x)$ is a property of elements of $A$, there is a set $B$ that $x \in B$ iff $x \in A$ and $P(x)$, it is denoted by $B = \{ x \in A | P(x) \}$.

Axiom (1.1.1.7) [Axiom of Pairs]. For each $A, B$, there is a set $C$ that $x \in C$ iff $x = A$ or $x = B$.

Axiom (1.1.1.8) [Axiom of Unions]. For any set $S$, there exists a set $U$ that $x \in U$ iff $x \in A$ for some $A \in S$.

Axiom (1.1.1.9) [Axiom of Power Sets]. For any set $S$, there exists a set $P$ that $x \in P$ iff $x \subset S$.

Def. (1.1.1.10) [Successors]. The successor of a set $x$ is $S(x) = x \cup \{x\}$.

Def. (1.1.1.11) [Inductive Sets]. A set $I$ is called inductive if $0 = \emptyset \in I$ and if $n \in I$, then $n + 1 \in I$, where $n + 1 = S(n)$ the successor.

Axiom (1.1.1.12) [Axiom of infinity]. An inductive set (1.1.1.11) exists.

Def. (1.1.1.13) [Natural Numbers]. The set of natural numbers $\mathbb{N}$ is defined to be $\{ x \in I_0 | x \in I$ for all inductive set $I \}$, where $I_0$ is an inductive set given by (1.1.1.12).

Cor. (1.1.1.14) [Inductive Principle]. If $P(x)$ is a property that $P(0)$, and $P(n)$ implies $P(n + 1)$, then $P(n)$ for each natural number $n$. 
Proposition (1.1.15). \( \mathbb{N} \) is a linearly ordered set.

Proof: Cf. [Set Theory Jech P43].

Corollary (1.1.16) [Inductive Principle Second Version]. If \( P(x) \) is a property that \( P(0) \), and \( P(k) \) holds for all \( k < n \) implies \( P(n) \), then \( P(n) \) for each natural number \( n \).

Proof: Use induction principle (1.1.14) for the property \( Q(n) : P(k) \) for all \( k < n \). Then \( Q(n) \) implies \( Q(n + 1) \).

2 Cardinals

Theorem (1.1.2.1) [Cantor-Schröder-Bernstein]. If there is an injection from \( A \) to \( B \) and an injection from \( B \) to \( A \), then there is a bijection from \( A \) to \( B \). Thus the ordering of the cardinal is well-defined.

So we can denote \( |A| \leq |B| \) iff there is an injection from \( A \) to \( B \). Then if \( |A| \leq |B| \) and \( |B| \leq |A| \), then \( |A| = |B| \).

Proof: Let \( f : A \to B \), \( g : B \to A \) be injection, then use the above lemma (1.1.2.2) for \( g \circ f(A) \subset g(B) \subset A \).

Lemma (1.1.2.2). If \( A_1 \subset B \subset A \) with \( |A| = |A_1| \), then \( |A| = |B| \).

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

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

Definition (1.1.2.3) [Cardinal Numbers]. A cardinal number is an equivalence class of sets, where equivalence is given by bijections. It is used to describe the ‘size’ of a set.

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

The cardinal number of \( \mathbb{N} \) is denoted by \( \aleph_0 \).

Countable and Uncountable Sets

Definition (1.1.2.4) [Countable Sets]. A set is called countable iff it has the cardinality of \( \aleph_0 \) (1.1.2.3).

It is called finite if it has the cardinality of \( n \) for some natural number \( n \). It is called uncountable iff it is not countable or finite.

Proposition (1.1.2.5). The subset or image of an at most countable set is at most countable.

Proof:

Proposition (1.1.2.6). The product of two countable sets is countable. (Use diagonal enumerating).

Proof:

Proposition (1.1.2.7). A countable union of almost countable subsets is almost countable.

Proof: It suffices to prove the countable case, the rest follows from (1.1.2.5). For this, choose an enumerating \( a_n(k) \) for each \( A_n \), the \( \cup A_n \) is the image of \( \mathbb{N} \times \mathbb{N} : (n, k) \mapsto a_n(k) \). Then it is countable by (1.1.2.6).

Proposition (1.1.2.8). The set of finite sequences and hence the set of finite subsets of a countable set is countable.

Proof: The desired set equals \( \cup_k A^k \), which is countable by (1.1.2.6) and (1.1.2.7).


1.1. ZERMELO-FRAENKEL SET THEORY WITH CHOICE

Cardinal Arithmetics

Def. (1.1.2.9). The sum, multiplication and exponentiation of two ordinal is the cardinality of the set $A \bigcup B$, $A \times B$ or $A^B$ respectively.

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

Prop. (1.1.2.10). $\aleph_0 \times \aleph_0 = \aleph_0$ by (1.1.2.6). And $\kappa \times \kappa = \kappa$ for any infinite cardinal, if one uses the axiom of choice by (1.1.5.3).

Prop. (1.1.2.11). The image of a set $X$ has cardinals no more than $X$, if axiom of choice holds.

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

Prop. (1.1.2.12)[Cantor]. $\# P(X) = 2^{\# X}$, and $|X| < |P(X)|$.

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

Prop. (1.1.2.13)[Cardinality Arithmetic of $\aleph_0$]. For cardinality arithmetics involving $\aleph_0$, Cf.[Set Theory Jech P98].

Prop. (1.1.2.14). if $|B| = 2^{\aleph_0}$ and $|A| \leq \aleph_0$, then $|B - A| = 2^{\aleph_0}$. In fact, $|B - A| = |B|$ for any $|A| < |B|$, if one uses the axiom of choice.

Proof: By (1.1.2.13), we can assume $B = \mathbb{R} \times \mathbb{R}$, then project $A$ onto the coordinate axis, then $\pi(A)$ has cardinality $\leq \aleph_0$, so there is a $x_0 \notin \pi(A)$, so $x_0 \times \mathbb{R} \subset B - A$, so $|B - A| = 2^{\mathbb{R}}$.

For the general case, ?

Conj. (1.1.2.15)[The Continuum Hypothesis]. There is no cardinal $\kappa$ that $\aleph_0 < \kappa < 2^{\aleph_0}$.

Notice $2^{\aleph_0} \geq \aleph_1$ by Cantor’s theorem (1.1.2.12), and this hypothesis is equivalent to $2^{\aleph_0} = \aleph_1$.


3 Orderings

Def. (1.1.3.1)[Ordering]. A partial ordering on a set $A$ is a relation $<$ on $A$, or equivalently a subset $C \subset A \times A$ that

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

It is called a total ordering if moreover it satisfies

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

A poset is just a partially ordered set.

Def. (1.1.3.2)[Reverse Ordering]. The reverse ordering $A^{op}$ of an ordered set $A$ is the same set $A$ with the ordering reversed.

Def. (1.1.3.3)[Cofinality]. The cofinality of or a poset (i.e partially ordered set) $\alpha$ is the is the smallest cardinality $\delta$ of a cofinal subset of $\alpha$. 
Def. (1.1.3.4) [\(\kappa\)-Filtered Poset]. For a cardinal \(\kappa\), a poset is called \(\kappa\)-filtered if for any subset unbounded from above has cardinality \(\geq \kappa\).

Def. (1.1.3.5) [Directed Set]. A directed set is a poset that 3-filtered and non-empty.

Def. (1.1.3.6). In a poset \(P\), two elements \(p, q\) are called compatible if there is an \(r \in P\) that \(r < p, r < q\).

Def. (1.1.3.7) [\(\kappa\)-Chain Condition]. For a cardinal \(\kappa\), a poset \(P\) is said to satisfy the \(\kappa\)-chain condition if for any subset \(A \subset P\) that elements of \(A\) are pairwise incompatible (1.1.3.6), then \(|A| \leq \kappa\).

Total Ordering

Def. (1.1.3.8) [Well-Ordering]. A linear ordering is just a total ordering. A linear ordering is called a well-ordering if every nonempty subset has a minimal element.

Def. (1.1.3.9) [Lexicographical Ordering]. If given a family of linearly ordered set \(A_i\) indexed by a well-ordered set \(I\), then there is a linear ordering on \(\prod_I A_i\), where \((f_i) < (g_i)\) iff \((f_i) \neq (g_i)\) and for the minimal \(i_0\) (well-ordering used) that \(f_{i_0} \neq g_{i_0}, f_{i_0} < g_{i_0}\). It is called the lexicographical ordering.

Def. (1.1.3.10). An ordered set \(X\) is called dense iff for each \(a < b\), there is a \(x\) that \(a < x < b\).

Def. (1.1.3.11) [Least Upper Bound]. An ordered set \(A\) is said to have the least upper bound property if any subset \(A_0 \subset A\) bounded above has a least upper bound. It is said to satisfy the greatest lower bound property if \(A^{op}\) satisfies the least upper bound property.

Prop. (1.1.3.12) [Cantor]. Any two ordered set that is countable, dense and has no endpoints are isomorphic. In particular, any of these is isomorphic to the set of rational numbers \(\mathbb{Q}\).

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

Cor. (1.1.3.13). Any countable linearly ordered set can be mapped isomorphically into \(\mathbb{Q}\).

Def. (1.1.3.14). A initial segment of an ordered set \(W\) is the ordered set \(W[a] = \{ x \in W \mid x < a \}\).

Lemma (1.1.3.15). If \(W\) is a well-ordered set, then any increasing function \(f : W \to W\) satisfies \(f(x) \geq x\).

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

Cor. (1.1.3.16). A well-ordered set cannot be isomorphic to an initial segment of itself, and an automorphism of a well-ordered set must be identity.

Proof: Use the above lemma (1.1.3.15), if it is isomorphic to \(W[a]\), then \(f(a) < a\), contradiction. For any automorphism, \(f(x) \geq x, f^-(x) \geq x\), so \(f(x) = x\). \(\square\)
Prop.(1.1.3.17) [Comparison of Well-Orderings]. A cut of a well-ordered set is well-ordered. And for any two well-ordered sets $W_1, W_2$, either they are isomorphic, or one of them is isomorphic to a initial segment of another.

Proof: The three cases are mutually exclusive by (1.1.3.16), so it suffices to show one of them holds.

Define a set $f = \{(x, y) \in W \times W | W_1[x] \cong W_2[y]\}$. (1.1.3.16) shows $f$ is injective and monotone in both coordinates. Now we want to prove that if the domain of $f$ is not all $W_1$, then it is an initial segment, and the image is all $W_2$, this will finish the proof.

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

Complete Linear Ordering

Def.(1.1.3.18) [Complete Ordering]. A cut of an ordered set $X$ consists of two disjoint nonempty subsets $A \cup B = X$ that $a < b$ for any $a \in A, b \in B$.

It is called a Dedekind cut if $A$ doesn’t have a maximal element. It is called a gap if $A$ doesn’t have a maximal element and $B$ doesn’t have a minimal element.

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

Prop.(1.1.3.19). A complete ordered set has the least upper bound property and greatest lower bound property.

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

Prop.(1.1.3.20) [Completion of Ordering]. There is an obvious ordering on the set $C$ of all Dedekind cuts of $X$, and $X$ embeds into $C$ by $b \mapsto \{x | x < b\} \cup \{x | x \geq b\}$.

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

Proof: Cf.[Set Theory Jech P88]. \qed

Prop.(1.1.3.21) [Real Numbers]. $Q$ has a unique completion ordering $R$, called the set of real numbers. $R$ is not countable.

Proof: $R$ is a dense linear ordering without endpoints, so by (1.1.3.12) if it is countable then it is isomorphic to $Q$, but this is not possible because $Q$ is not complete. \qed

Prop.(1.1.3.22). $|P(\mathbb{N})| = |2^\mathbb{N}| = |R|$, which is denoted by $2^{\aleph_0}$. By(1.1.3.21), $\aleph_0 < 2^{\aleph_0}$.

Proof: The first equality is by (1.1.2.12). Now by the construction of $R$, it can be embedded into $P(\mathbb{N})$, so $|R| \leq |P(Q)| = |P(\mathbb{N})|$. Conversely, $|2^\mathbb{N}| \leq |R|$ by decimal representation, so they are equal by Bernstein(1.1.2.1). \qed
4 Ordinals

Def. (1.1.4.1)[Ordinal Numbers]. A set is called transitive iff each element of $T$ is a subset of $T$. A set $\alpha$ is called a ordinal number iff $\alpha$ is transitive and well-ordered by inclusion.

Prop. (1.1.4.2). If $\alpha$ is an ordinal, then $S(\alpha) = \alpha \cup \{\alpha\}$ is also an ordinal, obviously. Thus any natural number is an ordinal by definition.

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

Lemma (1.1.4.3).
1. If $\alpha$ is an ordinal, then $\alpha \notin \alpha$.
2. Every element of an ordinal is an ordinal.
3. If ordinals $\alpha \subseteq \beta$, then $\alpha \in \beta$. That is, for ordinals, $\subseteq$ is the same as $\in$.

Proof:  
1. If $\alpha \in \alpha$, then contradiction to the fact $\in$ is a ordering (1.1.4.1).
2. To show $x \in \alpha$ is transitive, it suffices to show that if $u \in v \in x$, then $u \in x$, because then $v$ is a subset of $x$. But this follows from the fact $\in$ is an ordering. And because $x \subseteq \alpha$, the inclusion of $x$ is the restriction of inclusion in $\alpha$, so it is a well-ordering.
3. Consider $\beta - \alpha$, it has a minimal element $\gamma$. Notice $\gamma \subseteq \alpha$, because otherwise there is an element of $\beta - \alpha$ smaller than $\gamma$, by definition (1.1.4.1).

Now we show $\gamma = \alpha$, then it will follow that $\alpha \in \beta$. For this, if $\delta \in \alpha$ and $\delta \notin \gamma$, then $\gamma \in \delta$ or $\gamma = \delta$. But then this implies that $\delta \in \alpha$ because $\alpha$ is an ordinal, contradicting the fact $\gamma \in \beta - \alpha$.

Prop. (1.1.4.4)[Ordinal is Well-Ordered]. Define the ordering of ordinal by $\alpha < \beta$ iff $\alpha \in \beta$. The ordering of ordinals is a total ordering and is a well-ordering.

Proof: If $\alpha \beta \in \gamma$, then $\alpha \in \gamma$ because $\gamma$ is transitive. If $\alpha \in \beta \in \alpha$, then $\alpha \in \alpha$, contradicting (1.1.4.3).

Given any two ordinals, $\alpha \cap \beta$ is also an ordinal by definition. If $\alpha \cap \beta = \beta$ or $\alpha$, then $\alpha \subseteq \beta$, hence $\alpha \in \beta$ by (1.1.4.3). If $\alpha \cap \beta \subseteq \alpha$ and $\alpha \cap \beta \subseteq \beta$, then $\alpha \cap \beta \subseteq \alpha \cap \beta$, contradiction.

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

Cor. (1.1.4.5)[Supremum Ordinal]. Any set of ordinals has a supremum ordinal, it is just $\cup_{\alpha \in X} \alpha$.

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

Now if $\alpha \in X$, then $\alpha \subset \cup X$, so $\alpha \leq \cup X$ by (1.1.4.3). And if $\alpha \in \gamma$ for some ordinal $\gamma$, then $\cup X \subseteq \gamma$. So $\cup X$ is truly the supremum.

Cor. (1.1.4.6). For any set $X$ of ordinals, there is an ordinal $\alpha$ that is not in $X$, just choose $S(\cup X)$.

Axiom (1.1.4.7)[Axiom Scheme of Replacement]. Let $P(x, y)$ be a property that for each $x$ there exists uniquely a $y$ that $P(x, y)$, then for each set $A$ there is a set $B$ that for each $x \in A$ there is an element $y \in B$ that $P(x, y)$. 

Prop. (1.1.4.8). Every well-ordered set is isomorphic to a unique ordinal. So we can regard an ordinal as an equivalence class of isomorphic well-ordered sets.

Proof: Cf. [Set Theory Jech P111]. □

Cor. (1.1.4.9) [Cardinal as Initial Ordinal]. The axiom of choice together with (1.1.4.4) asserts that every cardinal has a unique smallest ordinal, called the initial ordinal. So we can identify cardinal number $\alpha$ as an ordinal that is the initial ordinal $\omega_\alpha$ of $\alpha$. Anyway, cardinal number is fewer than ordinal numbers.

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

Prop. (1.1.4.10) [Transfinite Induction/Recursion]. If a property defined for the set of ordinals satisfies:

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

Transfinite recursion:

Proof: □

Ordinal Arithmetic

Cf. [Set Theory Jech Chap5.5].

Def. (1.1.4.11). We use infinite recursion to define addition of ordinals as

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

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

Remark (1.1.4.12) [Cardinal and Ordinal Arithmetics]. Note that the ordinal arithmetics may be smaller than the ordinal sum of the corresponding initial ordinal (1.1.4.9), because operations of initial ordinals may not be initial, the deeper reason is that the cardinal case, we can rearrange the order to get a smaller ordinal.

Prop. (1.1.4.13). The addition and multiplication of ordinals are of the order type of $\alpha \uplus \beta$ in adjunction order and $\alpha \times \beta$ in lexicographical order respectively, Cf. [Set Theory Jech P120,122]

Cantor Normal Form

Prop. (1.1.4.14) [Cantor Normal Form]. Any ordinal $\alpha$ can be expressed uniquely as the form $\alpha = \sum_{i<n} \omega^{\beta_i}$, where $\beta_0 \geq \beta_1 \geq \ldots \beta_{n-1}$ are ordinals.

Proof: Cf. [Jech Set Theory P124]. □

Prop. (1.1.4.15) [Goodstein Sequence]. The weak Goodstein sequence is a sequence that $m_2$ is any positive integer, $m_{k+1}$ is $m_k$ written in $k$-basis and replacing the base by $k + 1$, and then minus 1.
The Goodstein sequence is a sequence that \( m_2 \) is any positive integer, \( m_{k+1} = m_k \) written in \( k \)-basis and even the exponents in \( k \)-basis and and replacing the base by \( k+1 \), and then minus 1.

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

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

Similarly for Goodstein sequences, just replace every base \( k \) by \( \omega \).

\[ \square \]

5 Alephs

**Prop. (1.1.5.1).** For any set \( A \), there is a least ordinal that is not equipotent to any subset of \( A \), called the Hartogs number of \( A \). This is clearly an initial ordinal.

**Proof:** By axiom schema of replacement, any well-ordered subsets of \( A \) is equipotent to an ordinal, and also by axiom schema of replacement, there is a set \( H \) that for any well-ordering of subsets of \( A \) in \( P(A \times A) \), this ordered sets is equipotent to a \( \alpha \in H \). Then use (1.1.4.6) to find a minimal ordinal that is not equipotent to any subset of \( A \). In fact, this is just \( h(A) = \{ \alpha \in H | \alpha \) equipotent to some subset of \( A \} \).

\[ \square \]

**Def. (1.1.5.2) [Aleph].** The alephs for ordinal numbers are defined recursively: \( \aleph_0 = \omega \), \( \aleph_{\alpha+1} = h(\aleph_\alpha) \), and \( \aleph_\alpha = \sup \{ \aleph_\beta | \beta < \alpha \} \) for a limit ordinal \( \alpha \). By definition \( \alpha_\alpha < \aleph_\beta \) when \( \alpha < \beta \).

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

Notice: to avoid confusion, when do arithmetic of ordinal numbers, \( \aleph_\alpha \) is written as \( \omega^{\aleph_\alpha} \).

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

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

\[ \square \]

**Aleph Arithmetics**

**Prop. (1.1.5.3).** \( \aleph_\alpha \cdot \aleph_\alpha = \aleph_\alpha \).

**Proof:** Cf. [Set Theory Jech P134].

\[ \square \]

**Cor. (1.1.5.4).** \( \aleph_\alpha \cdot \aleph_\beta = \aleph_\beta \) for \( \alpha \leq \beta \), and \( n \cdot \aleph_\beta = \aleph_\beta \).

So \( \aleph_\alpha + \aleph_\beta = \aleph_\beta \) for \( \alpha \leq \beta \), and \( n + \aleph_\beta = \aleph_\beta \).
6 Natural Numbers and Real Numbers

Prop.(1.1.6.1). \((\mathbb{N}, <)(1.1.1.15)\) is a well-ordered set.

Proof: □

Example(1.1.6.2)[Examples of Countable Sets].

- \(\mathbb{Z}\).
- \(\mathbb{Q}\).

Arithmetic of Real numbers

Prop.(1.1.6.3). The set of real numbers \(\mathbb{R}(1.1.3.21)\) can be endowed with a field structure, making it an ordered field.

Proof: Cf.[Set Theory Jech P175]. □

Prop.(1.1.6.4). \(\mathbb{R}\) satisfies the least upper bound hypothesis.

Proof: □

7 The Axiom of Choice

Def.(1.1.7.1). Let \(S\) be a system of sets, a function \(g\) defined on \(S\) is called a choice function iff \(g(X) \in X\) for each \(X \in S\).

Prop.(1.1.7.2)[Zermelo]. The following are equivalent:
1. (the axiom of choice)There exists a choice function for very system of sets.
2. (the well-ordering principle)Every set can be well-ordered.
3. (Zorn’s lemma)If every chain in a partially ordered sets has a upper bound, then the partially ordered set has a maximal element.

Proof: 2 → 1: If \(A\) is well-ordered, then \(P(A)\) clearly has a choice function, that is the minimal element of a set.
1 → 2: Use transfinite recursion, Cf.[Set Theory Jech P137].
2 → 3, 3 → 2: Cf.[Set Theory Jech P142]. □

Axiom(1.1.7.3)[the Axiom of Choice]. Any system of sets has a choice function.

Prop.(1.1.7.4). Every infinite set \(X\) has a countable subset, if the axiom of choice holds.

Proof: Choose a well-ordering of it(1.1.7.2), then it is an infinite ordinal. Then the initial segment of the first ordinal \(X[\omega]\) is a countable subset. □

Prop.(1.1.7.5). For every infinite set \(S\), there exists a unique aleph \(\aleph_\alpha\) that \(|S| = \aleph_\alpha\).

Proof: choose a well-ordering of \(S(1.1.7.2)\), then it is an infinite ordinal, and it has the same cardinality as an initial cardinal by(1.1.4.9), thus the result. □

Cor.(1.1.7.6). For any sets \(A\) and \(B\), either \(|A| \leq |B|\) or \(|B| \leq |A|\).

Proof: Because the ordinal is totally ordered(1.1.4.4). □
8 Filters and Ultrafilters

Def.(1.1.8.1)[Filter]. For a poset $P$, a filter on $P$ is a subset $F$ that
- If $p < q$ and $p \in F$, then $q \in F$.
- If $p, q \in F$, then there is an $r \in F$ that $r < p, r < q$.

Def.(1.1.8.2)[Filter on Sets]. Let $S$ be a non-empty set, a filter on $S$ is a filter $F$ on $\mathcal{P}(S)$ that
- $\emptyset \notin F$.

Def.(1.1.8.3)[Finite intersection property]. A family of subsets of a set is said to have the finite intersection property if any finite collection of elements of this family is non-empty.

Lemma(1.1.8.4). Let $G$ be a collection of subsets of $S$ that has the finite intersection property, then there is a smallest filter $F$ that $G \subset F$. It is just the collection of subsets of $S$ that contain some finite intersection set of elements of $G$.

Def.(1.1.8.5)[Ultrafilter]. An ultrafilter is a filter $F$ that for every subset $X$, $X \in F$ iff $S - X \notin F$. A prime ideal is an ideal that for every subset $X$, $X \in F$ iff $S - X \notin F$.

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

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

Conversely, if $F$ is maximal filter but not ultra, then there is a $X$ that $X \notin F, S - X \notin F$. Let $G = F \cup \{X\}$, then any finite intersection of elements of $G$ is not empty: $X_1 \cap \ldots \cap X_n \cap X \neq 0$ otherwise $S - X \in F$. So there is a filter containing $G$ by(1.1.8.4), contradiction. \qed

Prop.(1.1.8.6) [Pushforward of Filters]. If $\mathcal{F}$ is a (ultra)filter on $X$ and $f : X \to Y$ is a function, then $f_*(\mathcal{F}) = \{A \subset Y | f^{-1}(A) \in \mathcal{F}\}$ is a (ultra)filter on $X$, called the pushforward filter of $\mathcal{F}$.

Prop.(1.1.8.7). For an ultrafilter $\mathcal{F}$ on $X$, if $U_i \notin \mathcal{F}$, then $\sum_{i=1}^{n} U_i \notin \mathcal{F}$.

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

Prop.(1.1.8.8). Any filter can be extended to an ultrafilter(maximal filter), if the axiom of choice is used.

Proof: Use Zorn’s lemma(1.1.7.2). It suffices to prove that a union of a chain of filters is a filter, which is trivial. \qed

Cor.(1.1.8.9). Non-principal ultrafilter exists on any infinite set. And in fact, any non-principal ultrafilter contains all the cofinite sets.

For any non-principle ultrafilter, it cannot contains a single pt $\{x\}$, so it contains every cofinite set.
1.1. ZERMELO-FRAENKEL SET THEORY WITH CHOICE

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

Def. (1.1.8.10) [$\kappa$-Completeness]. Let $\kappa$ be an uncountable cardinal, then a field $F$ on a set $S$ is called $\kappa$-complete if for every cardinal $\lambda < \kappa$, if $X_\alpha \in F$ for every $\alpha < \lambda$, then $\cap_{\alpha < \lambda} X_\alpha \in F$.

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

Closed unbounded and Stationary Set

Silver’s Theorem

9 Combinatorial Set Theory

Def. (1.1.9.1) [Notations]. For a set $S$, let $[S]^r$ be the set of subsets of $S$ of order $r$. Let $\kappa, \lambda$ be cardinals, we write $\kappa \rightarrow (\lambda)^r_s$ as a shorthand for: for any set $S$ with $|S| = \kappa$ and every partition of $[S]^r$ into $s$ classes, there exists a subset $H \subset S$ that $[H]^r$ is in the same class, and $|H| \geq \lambda$.

Prop. (1.1.9.2) [Ramsey’s Theorem]. For any positive natural number $r, s$ if we color the $r$-subsets of a set with cardinality $\aleph_0$ into $s$ families, then there is a subset of cardinal $\aleph_0$ that all its $r$-subsets are colored the same.

Cor. (1.1.9.3). Every infinite linearly ordered set contains a subset isomorphic to $(\mathbb{N}, <)$ or $(\mathbb{N}, >)$.

Proof: Choose a well ordering of it. Then consider this new ordering and the original ordering. Then there is an infinite set that is compatible with the original ordering, or converse. Then its initial segment of order type $\omega_0$ satisfies the requirement. □

Def. (1.1.9.4) [Weakly Compact Cardinals]. An weakly compact cardinal is an uncountable cardinal $\kappa$ that $\kappa \rightarrow (\kappa)^r_s$ for any $r, s \in \mathbb{Z}_+$.

Prop. (1.1.9.5). Weakly compact cardinals are strongly inaccessible.


Trees

Def. (1.1.9.6). A tree is a partial ordered set $T$ that there is a minimal element $r$ and for each $x$, \{y \in T | y < x\} is finite and linearly ordered.

A tree is called of finite branched for each $x$, there is a finite set \{y_1, \ldots, y_r\} is $T$ that $y_i > x$ and if $z > x$, then $z \geq y_i$ for some $i$.

Def. (1.1.9.7) [Height]. For any node $x$, \{y \in T | y < x\} is a well-ordered set, which is isomorphic to an ordinal by (1.1.4.8), it is called the height of $x$. $T_\alpha$ denotes the set of all nodes of $T$ of order $\alpha$. The least $\alpha$ that $T_\alpha \neq \emptyset$ is called the height of $T$.

A branch is a maximal chain in $T$, its length is its ordinal. The length is always smaller than the height of the tree. If it equals the height of the tree, it is called cofinal.

Def. (1.1.9.8). A subtree is a subset $T'$ of $T$ that if $x \in T'$, $y < x$, then $x \in T'$.

An antichain of a tree $T$ is a subset $A \subset T$ that any two elements in $A$ are incomparable.

Def. (1.1.9.9). A path through $T$ is a morphism of ordering from $\omega$ to $T$. 

Lemma (1.1.9.10) [König’s Lemma]. If $T$ is an infinite finite branching tree, then there is a path through $T$.

Proof: Use recursion to choose for each $n$ an element that has infinite successors. □

Def. (1.1.9.11). An Aronszajn tree is a tree of height $\kappa$ and all its level sets are at most countable, but has no branches of length $\kappa$.

Prop. (1.1.9.12). An Aronszajn tree of height $\omega_1$ exists.

Proof: Cf. [Set Theory Jech P228]. □

10 The Axiom of Foundation

11 Large Cardinals

Def. (1.1.11.1) [Abstract Measures]. Let $S$ be a non-empty set, then an abstract measure on $S$ is a non-trivial probabilistic measure $\mu$ on the measurable space $(S, \mathcal{P}(S))$ that $\mu(\{a\}) = 0$ for any $a \in S$.

Def. (1.1.11.2) [Regular Cardinal]. A cardinal is called regular if it is not a sum of $\lambda$ cardinals $\kappa_i$ that $\lambda < \kappa$ and $\kappa_i < \kappa$.

Def. (1.1.11.3) [Strong Limit]. A cardinal $\kappa$ is called a strong limit if $2^\lambda < \kappa$ for any $\lambda < \kappa$.

Def. (1.1.11.4) [Strongly Inaccessible Cardinal]. A cardinal $\kappa$ is called strongly inaccessible (SI) if it is regular (1.1.11.2) and is a strongly limit.

Def. (1.1.11.5) [Weakly Inaccessible Cardinal]. A cardinal $\kappa$ is called weakly inaccessible if it is regular and is a limit cardinal.

Prop. (1.1.11.6) [Measure and CH]. If there exists an abstract measure on $2^{\aleph_0}$, then the Continuum Hypothesis fails.


Prop. (1.1.11.7). If there is a measure on a set $S$, then some cardinal $\kappa \leq |S|$ is weakly inaccessible.


Prop. (1.1.11.8). Let $\mu$ be a $\{0, 1\}$-valued measure on $S$, then $U = \{X \subseteq S|\mu(X) = 1\}$ is a non-principal $\sigma$-complete ultrafilter of $S$

Prop. (1.1.11.9) [Stanislaw-Ulam Dichotomy]. If there exists a measure on some set, then either there exists a $\{0, 1\}$-valued measure on some set, or there exists a measure on $2^{\aleph_0}$.


Def. (1.1.11.10) [Measurable Cardinals]. A measurable cardinal is an uncountable cardinal $\kappa$ on which there exists a non-principal $\kappa$-complete ultrafilter.

Prop. (1.1.11.11). A measurable cardinal is strongly inaccessible.

Def. (1.1.11.12) [Small Categories]. Given a regular cardinal $\kappa$, a set $S$ is called $\kappa$-small if it has cardinality smaller than $\kappa$. A category $\mathcal{C}$ is called $\kappa$-small if the set of all objects of $\mathcal{C}$ is $\kappa$-small, and the set of all morphisms of $\mathcal{C}$ is $\kappa$-small.

Throughout the whole book, we will fix a strongly inaccessible cardinal $\kappa$ and call a set or category small if it is $\kappa$-small. And a category is called essentially small if it is equivalent to a small category.

12 Forcing Construction of Cohn

Def. (1.1.12.1) [Dense Subset]. In a poset $P$, a subset $D \subseteq P$ is called dense if for any $p \in P$, there is a $q \in D$ that $q < p$. If $\mathcal{D}$ is a collection of dense subsets of $P$, a filter $G \subseteq P$ is called $\mathcal{D}$-generic if $D \cap G \neq \emptyset$ for all $D \subset \mathcal{D}$.

Prop. (1.1.12.2). If $\mathcal{D}$ is a countable collection of dense subsets of $P$, then there is a $\mathcal{D}$-generic filter $G$.

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

Axiom (1.1.12.3) [Martin’s Axiom]. If $P$ is a partially ordered set satisfying the countable chain condition (1.1.3.7), and $D$ is a collection of dense subsets of $P$ with $|D| < 2^{\aleph_0}$, then there is a $D$-generic filter on $P$. 
1.2 Model Theory

Basic references are [Model Theory Marker] and [Mathematical Logics Hamilton]. The exercises of [Model Theory Marker] is important.

1 Mathematical Logics

Turing Machine and Computability

Prop.(1.2.1.1) [Turing Machine]. For the ring structure of \( \mathbb{N} \), there is a \( \mathcal{L} \)-formula \( \varphi(e, x, s) \) that \( \mathbb{N} \models T(e, x, s) \) iff the Turing machine coded with \( e \) halts on input \( x \) within \( s \) steps. So the set of halting computation is definable by the formula: \( \exists s \varphi(e, x, s) \).

Proof: Cf.[Models of Peano Arithmetic Kaye]. □

Def.(1.2.1.2) [Recursively Enumerable Sets]. A set \( S \) of the natural numbers is called recursively enumerable iff there is an algorithm that the set of input numbers that halts is exactly \( S \). Equivalently, a recursively enumerable set is a set that there is an algorithm that 'enumerates' the members of \( S \).

Prop.(1.2.1.3) [Hilbert’s 10-th Problem]. For any recursively enumerable set \( A \subset \mathbb{N}^n \), there is a polynomial \( P(X_1, \ldots, X_n, Y_1, \ldots, Y_m) \) that
\[
A = \{ \bar{x} \in \mathbb{N}^n : \mathbb{N} \models \exists y_1 \exists y_2 \ldots, \exists y_mp(x, \bar{y}) = 0 \}
\]


2 Structure and Theories

Basics

Def.(1.2.2.1) [Boolean Algebra]. A Boolean algebra is a set \( B \) with Boolean connectives \( \land, \lor, 0, 1 \), where:
- \( \land \) is a symmetric function \( B \times B \to B \) that \( \varphi \land \varphi = \varphi \);
- \( \lor \) is function \( B \to B \) that \( \neg \circ \lor = \text{id} \);
- 0,1 are nullary operations that \( \neg 0 = 1, \text{and} \ x \land 0 = 0, \text{and} \ x \land \neg x = 0 \).
Sometimes \( \lor \) is also used, which is defined as \( \varphi \lor \psi = \neg(\neg \varphi \land \neg \psi) \).

Prop.(1.2.2.2). The power set of any set is a Boolean algebra with \( \land = \cap \) and \( \lor(A) = X - A \).
In fact, every Boolean algebra can be embedded as a subalgebra of a power set algebra of some set by(3.6.2.16).

Def.(1.2.2.3) [Languages and Structures]. A language \( \mathcal{L} \) is a set of symbols, where a symbol is indeterminants that are labeled constant symbol \( C \), function symbol (of finite arity) \( \mathcal{F} \) or relation symbol (of finite arity) \( \mathcal{R} \).
For a language \( \mathcal{L} \), a \( \mathcal{L} \)-structure on a set \( M \) is an assignment for each constant symbol \( c \) an element \( c^M \in M \), for each function symbol \( f \) of arity \( n \) a function \( f^M : M^n \to M \), and for each
relation symbol $R$ of arity $m$ a subset $R^M \subseteq M^m$. These $c^M, f^M, R^M$ are called interpretations of $\mathcal{L}$.

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

**Def. (1.2.2.4) [Formulae].** For a language $\mathcal{L}$, the set of **terms** is the smallest set $\mathcal{T}$ that $c \in T$ for each constant symbol $c$, $x_i \in T$ for each variable symbol, and if $t_1, \ldots, t_n \in \mathcal{T}$ and $f \in \mathcal{F}$, then the symbol $f(t_1, \ldots, t_n) \in \mathcal{F}$.

An **atomic formula** is a symbol of the form $t_1 = t_2$ or $R(t_1, \ldots, t_n)$, where $t_i$ are terms.

The set of $\mathcal{L}$-**formulae** is the smallest set $\mathcal{W}$ that any atomic formula is in $\mathcal{W}$, and if $\varphi, \psi \in \mathcal{W}$, then $\neg \varphi, \varphi \land \psi$ are in $\mathcal{W}$, and adjunction with the **qualifier symbol** $\exists x_i \varphi$ is in $\mathcal{W}$.

A **free variable in a formula** is a $x_i$ that is not qualified with $\forall$ or $\exists$, otherwise it is called bound.

A **sentence** is a formula without free variables.

A **theory** is a set of sentences in a language $\mathcal{L}$.

**Remark (1.2.2.5) [Simplifications].** $\varphi \rightarrow \psi$ is the simplification of $\neg \varphi \lor \psi$, $\varphi \leftrightarrow \psi$ is the simplification of $(\varphi \rightarrow \psi) \land (\psi \rightarrow \varphi)$.

Even $\lor$ is the simplification of $\neg (\neg \varphi \land \psi)$, and $\forall x_i \varphi$ is the simplification of $\neg (\exists x_i \neg \varphi)$.

**Def. (1.2.2.6) [First Order Logic].** A **first order logic** is a $\mathcal{L}$-structure that only elements in $M$ are quantified with $\forall$ or $\exists$. For example, "Every bounded subsets has a least upper bound" cannot be expressed as a formulae in a first order logic of $\mathbb{R}$.

**Def. (1.2.2.7) [Truth].** Let $\varphi$ be a formula with free variables $\overline{v} = (v_1, \ldots, v_m)$, then we inductively define $\mathcal{M} \models \varphi(\overline{a})$ as follows:

- If $\varphi$ is $t_1 = t_2$ where $t_1, t_2$ are terms, then $\mathcal{M} \models \varphi(\overline{a})$ if $t_1^\mathcal{M}(\overline{a}) = t_2^\mathcal{M}(\overline{a})$.
- If $\varphi$ is $R(t_1, \ldots, t_n)$, then $\mathcal{M} \models \varphi(\overline{a})$ if $(t_1^\mathcal{M}(\overline{a}), \ldots, t_n^\mathcal{M}(\overline{a})) \in R^\mathcal{M}$.
- If $\varphi$ is $\neg \psi$, then $\mathcal{M} \models \varphi(\overline{a})$ if $\mathcal{M} \not\models \psi(\overline{a})$.
- If $\varphi$ is $\psi \land \theta$, then $\mathcal{M} \models \varphi(\overline{a})$ if $\mathcal{M} \models \psi(\overline{a})$ and $\mathcal{M} \models \theta(\overline{a})$.
- If $\varphi$ is $\exists v_j \psi(\overline{v}, v_j)$, then $\mathcal{M} \models \varphi(\overline{a})$ is there is a $b \in M$ that $\mathcal{M} \models \psi(\overline{a}, b)$, and we say $\mathcal{M}$ **satisfies** $\varphi(\overline{a})$. Notice if there is no free variables, $\varphi(\overline{a})$ just writes $\varphi$.

**Def. (1.2.2.8) [Models].** If $T$ is a theory and the $\mathcal{L}$-structure $M$ satisfies all $\varphi \in T$, then $M$ is called a **model** of $T$, and writes $M \models T$.

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

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

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

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

**Prop. (1.2.2.9) [Quantifier-Free Formulae].** Suppose $\mathcal{M}$ is a substructure of $\mathcal{N}$ and $\overline{a}$ is a tuple in $\mathcal{M}$. If $\varphi(\overline{a})$ is a quantifier-free formula, then $\mathcal{M} \models \varphi(\overline{a})$ iff $\mathcal{N} \models \varphi(\overline{a})$.

**Proof:** Cf. [Model Theory P11].

**Prop. (1.2.2.10).** If $\mathcal{L}$-structures $\mathcal{M} \cong \mathcal{N}$, then $\mathcal{M}$ is elementarily equivalent to $\mathcal{N}$. 

\[\square\]
Proof: This seemingly trivial proposition still needs proof, and the proof uses induction, just as that of (1.2.2.9).

Def. (1.2.2.11) [Logical Consequence]. Let \( T \) be an \( \mathcal{L} \)-theory and \( \varphi \) an \( \mathcal{L} \)-sentence, then \( \varphi \) is called a **logical consequence** of \( T \), writes \( T \models \varphi \), if for any \( \mathcal{L} \)-structure \( \mathcal{M} \) that \( \mathcal{M} \models T \), \( \mathcal{M} \models \varphi \).

**Definable Sets and Interpretability**

Def. (1.2.2.12). Let \( \mathcal{M} \) be an \( \mathcal{L} \)-structure, a subset \( X \) of \( \mathcal{M}^n \) is called **definable** iff there is an \( \mathcal{L} \)-formula \( \varphi(v_1, \ldots, v_n, w_1, \ldots, w_m) \) and a tuple \( \bar{b} \in \mathcal{M}^m \) that \( X = \{ \bar{a} \in \mathcal{M}^n : \mathcal{M} \models \varphi(\bar{a}, \bar{b}) \} \). Moreover if \( A \subset M \), \( X \) is called **\( A \)-definable** iff \( y_i \in A \).

Prop. (1.2.2.13) [Examples of Definable Sets]. The definability of some sets are often nontrivial, using many number theories. For example, Cf. [Marker P20].

Prop. (1.2.2.14). There is an inductive characterization of definable sets, Cf. [Marker P22].

Prop. (1.2.2.15). If \( \mathcal{M} \) is an \( \mathcal{L} \)-structure, If \( X \subset \mathcal{M}^n \) is \( A \)-definable, then very \( \mathcal{L} \)-automorphism of \( \mathcal{M} \) that fixes \( A \) pointwise will fixes \( X \) setwise.

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

Cor. (1.2.2.16). \( \mathbb{R} \) is not definable in \( \mathbb{C} \).

Proof: If \( \mathbb{R} \) is definable, it is definable over a finite set \( A \subset \mathbb{C} \), Let \( r, s \) be algebraically independent over \( A \) and \( r \in \mathbb{R}, s \notin \mathbb{R} \). This can be done, otherwise \( \mathbb{C} \) or \( \mathbb{R} \) is finite transcendental over \( \mathbb{Q} \), then \( |\mathbb{C}| = |\mathbb{Q}|(2.2.6.3) \), which is impossible by (1.1.3.21). Then there is an automorphism \( \sigma \) of \( \mathbb{C} \) fixing \( A \) that \( \sigma(r) = s \), so \( \mathbb{R} \) is not definable by (1.2.2.15).

Def. (1.2.2.17) [Definably Interpretability]. An \( \mathcal{L}_0 \)-structure \( \mathcal{N} \) is called **definably interpreted** in an \( \mathcal{L} \)-structure \( \mathcal{M} \) if there is a definable set \( X \subset \mathcal{M}^n \) that we can interpret the symbols of \( \mathcal{L}_0 \) as definable subsets and functions of \( X \) and the resulting \( \mathcal{L}_0 \)-structure is isomorphic to \( \mathcal{N} \).

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

Def. (1.2.2.18) [Interpretability and Quotient Construction]. An \( \mathcal{L}_0 \)-structure \( \mathcal{N} \) is called **interpretable** in an \( \mathcal{L} \)-structure \( \mathcal{M} \) iff there is a definable set \( X \subset \mathcal{M}^n \) and a definable equivalence relation \( E \) on \( X \), that we can interpret the symbols of \( \mathcal{L}_0 \) as definable subsets and functions of \( X/E \) and the resulting \( \mathcal{L}_0 \)-structure is isomorphic to \( \mathcal{N} \).

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

Prop. (1.2.2.19). Any structure for a countable language can be interpreted in a graph.

Proof:
3 Some Theories Often Used

Def. (1.2.3.1) [Languages].
- \( L_r \) is defined to be the language of rings.
- \( L_{or} \) is defined to be the language of ordered rings.

Def. (1.2.3.2) [Theories].
- \( ACF \) is defined to be the theory of alg.closed fields, w.r.t \( L_r \).
- \( ACF_p \) is defined to be the theory of alg.closed fields of char \( p \).
- \( DAG \) is defined to be the theory of non-trivial torsion-free divisible Abelian groups, w.r.t. \( L_r \).
- \( DLO \) is the theory of dense linear orders without endpoints.
- \( ODAG \) is the theory of nontrivial divisible Abelian groups.
- \( RCF \) is the theory of real closed fields w.r.t \( L_{or} \).

4 Basis Techniques

Def. (1.2.4.1) [Definitions for Theories]. A theory \( T \) is said to have the witness property iff whenever \( \varphi(v) \) is an \( L \)-formula with one free variable \( v \), there is a constant symbol \( c \) that \( T \models (\exists v \varphi(v) \rightarrow \varphi(c)) \).

A theory \( T \) is called maximal iff for any \( L \)-sentence, either \( \varphi \in T \) or \( \neg \varphi \in T \).

A theory \( T \) is called complete iff for any \( L \)-sentence, either \( T \models \varphi \) or \( T \models \neg \varphi \).

Def. (1.2.4.2) [Proof System]. A proof of a \( L \)-sentence \( \varphi \) from a theory \( T \), denoted by \( T \vdash \varphi \), is a

Prop. (1.2.4.4). If \( L \) is a recursive language and \( T \) is a recursive \( L \)-structure, then \( \{ \varphi | T \vdash \varphi \} \) is recursively enumerable.

Prop. (1.2.4.5). The halting computation set is not computable.

Cor. (1.2.4.6). The full theory \( Th(\mathbb{N}) \) of the ring structure of \( \mathbb{N} \) is undecidable.
Proof: If such an algorithm exists, then we can use it to compute whether the sentence
\[ \varphi(e, x) = \exists s T((1 + \ldots + 1, 1 + \ldots + 1, s)) \]
is computable. Then this will contradicts the fact that halting computation set is not computable (1.2.4.5).

\[ \square \]

Prop. (1.2.4.7) [Gödel's Completeness Theorem]. Let \( T \) be an \( \mathcal{L} \)-theory and \( \varphi \) is an \( \mathcal{L} \)-sentence, then \( T \models \varphi \) iff \( T \vdash \varphi \).

Proof: ?

\[ \square \]

Cor. (1.2.4.8) [Consistent and Satisfiable]. A theory \( T \) is consistent iff it is satisfiable.

Proof: If \( T \) is satisfiable, then it is clearly consistent, and if \( T \) is not satisfiable, then there are no models for \( T \), so \( T \models \neg \forall \varphi \) by definition, so \( T \vdash \varphi \) by Gödel’s completeness theorem.

\[ \square \]

Cor. (1.2.4.9) [Lemma on Constants]. Suppose \( T \vdash \varphi(\bar{c}) \) and \( \bar{c} \) is a tuple of constants not appearing in \( T \), then \( T \vdash \forall x \varphi(x) \).

Proof: We use the Gödel’s completeness theorem (1.2.4.7), and notice this theorem is obviously true for \( \vdash \) replaced by \( \models \). Notice we can add the constants to \( \mathcal{L} \), thus \( \varphi(\bar{c}) \) has no free variables.

\[ \square \]

Ultraproducts of Theories

Def. (1.2.4.10) [Ultraproducts of Theories]. If \( M_i, i \in I \) is a collection of \( \mathcal{L} \)-structures and \( \mathcal{F} \) is an ultrafilter on \( I \), then the ultraproduct \( \prod_I M_i / \mathcal{F} \) of \( M_i \) is a \( \mathcal{L} \)-structure defined as:

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

Prop. (1.2.4.11) [Łoś Theorem]. Let \( M_i, i \in I \) be \( \mathcal{L} \)-structures and \( \mathcal{F} \) be an ultrafilter on \( I \). Let \( \varphi(\bar{x}) \) be a first-order logic formula in the free variables \( \bar{x} \), and let \( (a_i) \) be a tuple of elements from \( \prod_I M_i / \mathcal{F} \), then
\[ \prod_I M_i / \mathcal{F} \models \varphi([a_i]) \iff \{ i \in I | M_i | \models \varphi_i(\bar{a}) \} \in \mathcal{F}. \]

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

\[ \square \]

Cor. (1.2.4.12). An ultraproduct of models for a theory \( T \) is also a model for \( T \).

Cor. (1.2.4.13) [Non-Standard Model for \( Th(R) \)]. Consider \( R \) in the language \( \mathcal{L}_r \), where \( \mathcal{L}_r \) is the language of rings, (i.e., the ring structure), let \( \mathcal{F} \) be a non-principle ultrafilter on \( \mathbb{N}(1.1.8.9) \), and consider the ultraproduct \( \mathcal{R} = \prod_{i \in \mathbb{N}} R / \mathcal{F} \), which is called an ultrapower of \( R \).

Notice each factor satisfies \( Th(R) \), so \( \mathcal{R} \) also satisfies \( Th(R) \).
Cor. (1.2.4.14). Using ultraproduct construction, we can find a field of characteristic 0 that has exactly one algebraic extension in each degree.

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

Prop. (1.2.4.15) [Keiler-Shelah Theorem]. Two \( L \)-structures \( \mathcal{M} \) and \( \mathcal{N} \) are elementary equivalent iff there is an index set \( I \) and an ultrafilter \( \mathcal{F} \) on \( I \) that \( \prod_{I} M / \mathcal{F} \cong \prod_{I} N / \mathcal{F} \).

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

Compactness Theorem and Henkin Construction

Lemma (1.2.4.16). Suppose \( T \) is a maximal and finitely satisfiable \( L \)-theory with the witness property, then \( T \) is satisfiable. In fact, \( T \) has \( \kappa \) constant symbols, then there is a model \( \mathcal{M} \models T \) that \( |\mathcal{M}| \leq \kappa \).

Proof: Cf.[Marker, P35]. □

Lemma (1.2.4.17). Let \( L \) be a finitely satisfiable \( L \)-theory, then there is a language \( L \subset L^* \) and a \( T \subset T^* \) a finitely satisfiable \( L^* \)-theory that any \( L^* \)-theory extending \( T^* \) has the witness property. And we can choose \( |L^*| = |L| + \aleph_0 \).

Proof: We first show there is a language \( L \subset L_1 \) and a finitely satisfiable \( L_1 \)-theory \( T \subset T_1 \) that witnesses all \( L \)-formulae: We add a constant symbol \( c_\varphi \) for each \( L \)-formula \( \varphi \), and add sentences \((\exists v \varphi(v)) \rightarrow \varphi(c_\varphi)\) to \( T \), then this \( T_1 \) is finitely satisfiable, because for any finite subset \( \Delta \) of \( T_1 \), only f.m. constant symbols appear, and we have a model \( \mathcal{M} \) for \( \Delta \cap T \), thus we can interpret \( c_\varphi \) as the element \( a \) that \( \mathcal{M} \models \varphi(a) \), if \( \mathcal{M} \models \exists v \varphi(v) \). Now we can inductively define \( L_n, T_n \), and consider their union, then this satisfies the desired conditions. And the cardinality is also clear. □

Lemma (1.2.4.18). If \( T \) is a finitely satisfiable \( L \)-theory, then there is a maximal (1.2.4.1) finitely satisfiable \( L \)-theory \( L \subset L' \).

Proof: it is easy to construct a maximal satisfiable \( L \)-theory, and it is truly maximal in sense of (1.2.4.1): for any sentence \( \varphi \), if \( T \cup \varphi \) is not finitely satisfiable, there is a finite set \( \Delta \subset T \) that \( \Delta \models \neg \varphi \). Then we claim \( T \cup \neg \varphi \) is finitely satisfiable: for another finite set \( \Sigma \), because \( \Delta \cup \Sigma \) is finitely satisfiable and \( \Delta \models \neg \varphi \), \( \Sigma \cup \neg \varphi \) is satisfiable. □

Prop. (1.2.4.19) [Strong Compactness Theorem]. If \( T \) is a finitely satisfiable \( L \)-theory and \( \kappa \) is an infinite cardinal that \( \kappa > |L| \), then there is a model of \( T \) of cardinality at most \( \kappa \).

Proof: By (1.2.4.17), we get a desired language \( L^* \) of cardinality \( \leq \kappa \), and a theory \( T^* \), and by (1.2.4.18), we can assume \( T^* \) is maximal and finitely satisfiable, and it has the witness property. Then (1.2.4.16) says there is a model of cardinality \( \leq \kappa \). □

Cor. (1.2.4.20) [Compactness Theorem]. A theory \( T \) is satisfiable iff every finite subset of \( T \) is satisfiable.

Remark (1.2.4.21). Notice the compactness theorem is also a consequence of the completeness theorem (1.2.4.7): if \( T \) is not satisfiable, then it is not consistent by (1.2.4.8). Let \( \sigma \) be a proof of a contradiction in \( T \), then \( \sigma \) consists of f.m. sentences in \( T \), which consists of a finite unsatisfiable subset \( T_0 \) of \( T \).
It is clear provable using ultrafilters: If there is a family of structures \( \{M_\Delta\} \) indexed by the collection of all finite subsets of \( T \), with \( M_\Delta \models \Delta \) for all \( \Delta \in I \) where \( I \) is the set of all finite subsets of \( T \).

Then we want to find an ultrafilter \( F \) on \( I \) that for all \( \varphi \in T \), \( \{\Delta | \Delta \models \varphi \} \in F \), then we can use Leo's theorem (1.2.4.11) to show that \( \prod_I M_\Delta / F \) is a model for all \( \varphi \in T \). Now in fact we make pick a ultrafilter over the filter generated by all the \( A_\varphi = \{\Delta | \varphi \in \Delta \} \), because \( M_\Delta \models \Delta \). In fact, this is the case because \( A_\varphi \) has the finite intersection property trivially.

**Cor. (1.2.4.22).** If \( T \models \varphi \), then \( \Delta \models \varphi \) for some finite \( \Delta \subset T \).

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

**Cor. (1.2.4.23) [Torsion Elements].** Let \( L \) be a language containing \( \{\cdot, e\} \), the language of groups, and \( T \) is a theory extending the theory of groups, let \( \varphi(v) \) be an \( L \)-formula. If for any \( n \) there is a \( G_n \models T \) and \( G_n \) has an element of finite order greater than \( n \), then there is an \( L \)-structure \( G \) that \( G \models T \) and \( G \) has an element of infinite order.

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

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

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

then the theory \( T^* \) is finitely satisfiable by hypothesis, so \( T^* \) is satisfiable by compactness theorem. \( \square \)

**Cor. (1.2.4.24) [Larger than All Natural Number].** Consider \( L \) the language of ordered rings, let \( Th(\mathbb{N}) \) be the theory of \( \mathbb{N} \), then there is an \( L \)-structure \( M \models Th(\mathbb{N}) \) and \( M \) has an element that is larger than every natural number.

*Proof:* The same proof as that of (1.2.4.23), but use

\[
T^* = Th(\mathbb{N}) \cup \{ 1 + \cdots + 1 < c \}^{n \text{-times}}
\]

\( \square \)

**Prop. (1.2.4.25) [Model of a Given Cardinality].** If \( T \) is an \( L \)-theory with infinite models, then if \( \kappa \) is an infinite cardinal that \( \kappa \geq |L| \), then there is a model of \( T \) of cardinality \( \kappa \).

*Proof:* Let \( L^* = L \cup \{c_\alpha : \alpha < \kappa\} \), where \( c_\alpha \) are pairwise different new constants, and \( T^* \) be the \( L^\ast \) theory \( T \cup \{c_\alpha \neq c_\beta, \alpha < \beta < \kappa\} \), then any model for \( T^* \) must has cardinality \( \geq \kappa \). But then we use strong compactness theorem (1.2.4.19), it suffices to show \( T^* \) is finitely satisfiable: for any finite \( \Delta \subset T^* \), there are only f.m. new constant symbols, thus we can use the infinite model \( M \) to interpret the constant symbols randomly, thus we are done. \( \square \)
1.2. MODEL THEORY

**Complete Theories**

**Def.(1.2.4.26).** Let \( \kappa \) be an infinite cardinal and \( T \) is a theory with models of size \( \kappa \). \( T \) is called \( \kappa \)-categorical iff any two models of \( T \) of cardinality \( \kappa \) are isomorphic.

**Prop.(1.2.4.27).** The theory of torsion-free divisible Abelian groups is \( \kappa \)-categorical for all \( \kappa > \aleph_0 \).

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

**Prop.(1.2.4.28)[Vaught’s Test].** Let \( T \) be a satisfiable theory with no finite models, if \( L \) is \( \kappa \)-categorical for some \( \kappa \geq |L| \), then \( T \) is complete.

*Proof:* If there is a sentence \( \varphi \) that \( T \not\models \varphi \) and \( T \not\models \neg \varphi \), so \( T_0 = T \cup \{ \varphi \} \) and \( T_1 = T \cup \{ \neg \varphi \} \) is satisfiable. They both have infinite models by hypothesis, so by (1.2.4.25) there are models of cardinal \( \kappa \) for \( T_0 \) and \( T_1 \), but they cannot be isomorphic, contradiction. So \( T \) is complete. \( \square \)

**Prop.(1.2.4.29)[Recurve Complete Satisfiable is Decidable].** If \( T \) is a recursive complete satisfiable theory in a recursive language \( L \), then \( T \) is decidable.

*Proof:* Because \( T \) is satisfiable, The set of all \( \varphi \) that \( M \models \varphi \) and the set of all \( \varphi \) that \( M \models \neg \varphi \) are disjoint, and their sum is the set of all sentences by completeness. By Gödel’s completeness theorem, this is equivalent to \( M \vdash \varphi \) or \( M \vdash \neg \varphi \). Then by (1.2.4.4), they are both enumerable, so it is decidable by definition. \( \square \)

**Up and Down(of Cardinality)**

**Def.(1.2.4.30)[Elementary Embedding].** An \( L \)-structure embedding \( j : M \to N \) is called an elementary embedding, denoted by \( M \prec N \), if for any \( L \)-formula \( \varphi \),

\[
M \models \varphi(\pi) \iff N \models \varphi(j(\pi)).
\]

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

Isomorphisms are elementary embeddings by (1.2.2.10).

**Def.(1.2.4.31)[Diagrams].** Let \( M \) be an \( L \)-structure, then we can add to \( L \) constant symbols for each element of \( M \), and the class \( \text{Diag}(M) \) of atomic diagrams of \( M \) is sentences of the form \( \varphi(m_1, \ldots, m_n) \), where \( \varphi \) is an atomic \( L \)-formula or the negation of an atomic \( L \)-formula, and \( M \models \varphi(m_1, \ldots, m_n) \). And the class \( \text{Diag}_{el}(M) \) of elementary diagrams of \( M \) is sentences of the form \( \varphi(m_1, \ldots, m_n) \) where \( \varphi \) is an \( L \)-formula that \( M \models \varphi(m_1, \ldots, m_n) \).

**Prop.(1.2.4.32)[Diagrams and Embedding].** The diagram and elementary diagram is very important in constructing embeddings of theories: Let \( N \) be an \( L_M \)-structure, then:

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

**Prop.(1.2.4.33)[Upward Löwenheim-Skolem Theorem].** Let \( M \) be an infinite \( L \)-structure and \( \kappa \) be an infinite cardinal that \( \kappa \geq |M| + |L| \), then there is an \( L \)-structure \( N \) of cardinality \( \kappa \) that \( M \) embeds into \( N \).

*Proof:* \( \text{Diag}_{el}(M) \) is clearly satisfiable, so by (1.2.4.25), there is an \( L^* \)-model \( N \) of cardinality \( \kappa \) that \( M \prec N \). \( \square \)
Prop. (1.2.4.34) [Tarski-Vaught Test]. A substructure $\mathcal{M}$ of a structure $\mathcal{N}$ is an elementary substructure iff for any formula $\varphi(v, \overline{w})$ and $\overline{a} \in M$, if there is $b \in N$ that $\mathcal{N} \models \varphi(b, \overline{a})$, then there is a $c \in M$ that $\mathcal{N} \models \varphi(c, \overline{a})$.

Proof: Cf. [Marker P45]. □

Prop. (1.2.4.35) [(Downward) Löwenheim-Skolem Theorem]. Suppose $\mathcal{M}$ is an $\mathcal{L}$-structure and $X \subseteq \mathcal{M}$, then there is an elementary submodel $\mathcal{N}$ that $X \subseteq \mathcal{N}$ and $|\mathcal{N}| \leq |X| + |\mathcal{L}| + \aleph_0$.

Proof: Cf. [Marker P46]. □

Def. (1.2.4.36) [Universal Sentences]. A universal sentence is a sentence of the form $\forall v \varphi(v)$, where $\varphi$ is quantifier-free.

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

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

Prop. (1.2.4.37) [Universal Axiomation]. An $\mathcal{L}$-theory $T$ has a universal axiomatization iff for any $\mathcal{N} \subseteq \mathcal{M}$, if $\mathcal{M} \models T$, then $\mathcal{N} \models T$.

Proof: Cf. [Marker P47]. □

Prop. (1.2.4.38) [Universal Consequences]. If $T$ is an $\mathcal{L}$-theory, then $A \models T_{\forall}$ iff there is an $\mathcal{M} \models T$ that $A \subseteq \mathcal{M}$.

Proof: If $A \subseteq \mathcal{M}$, then $A \models T_{\forall}$, by (1.2.4.37). Conversely, if $A \models T_{\forall}$, then consider $\text{Diag}(A)$, then it suffices to show $\text{Diag}(A)$ is satisfiable. If it is not, then by compactness theorem (1.2.4.20) there is a finite set that is not satisfiable, and the part coming from diagrams of $M$ can be expressed by a single formula $\chi(\overline{a})$, where $\chi$ is quantifier-free, $\overline{a} \in M$, $\mathcal{M} \models \chi(\overline{a})$, and we are saying that $T \cup \{\chi(\overline{a})\}$ is not satisfiable, then $T \models \neg \chi(\overline{a})$.

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

Prop. (1.2.4.39) [Elementary Chain]. If $\mathcal{M}_i$ is a chain of $\mathcal{L}$-structures that $\mathcal{M}_i \prec \mathcal{M}_j$ for any $i < j$, then we can define there union $\mathcal{M} = \cup \mathcal{M}_i$. Then $\mathcal{M}$ is an elementary extension of each $\mathcal{M}_i$.

Proof: Use induction on formulas to show that

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

for all $\mathcal{L}$-formulas $\varphi$. This is true for quantifier-free formula by (1.2.2.9), and if this is true for $\varphi, \psi$, then this is true for $\neg \varphi$ and $\varphi \land \psi$. For the sentence $\varphi = \exists v \psi(v, \overline{w})$, if $\mathcal{M}_i \models \psi(b, \overline{a})$ for some $b$, then so does $\mathcal{M}$. Conversely, if $\mathcal{M} \models \psi(b, \overline{a})$ for some $b$, then $b \in \mathcal{M}_j$ for some $j$, then $\mathcal{M}_j \models \varphi$, by the condition, $\mathcal{M}_i \models \varphi$ also. □

Back and Forth Argument

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

Prop. (1.2.4.40) [Cantor]. The theory $DL0(1.2.3.2)$ is $\aleph_0$-categorical and complete.

Proof: It is $\aleph_0$-categorical by (1.1.3.12), and it is complete, by Vaught’s test (1.2.4.28), as it has no finite models. □
5 Quantifier Elimination

**Def.(1.2.5.1)** [Quantifier Elimination]. A theory is said to have quantifier elimination if for each formula \( \varphi(\overline{v}) \), there is a quantifier-free formula \( \psi(\overline{v}) \) such that \( T \models \forall \overline{v}(\varphi(\overline{v}) \leftrightarrow \psi(\overline{v})) \).

**Lemma (1.2.5.2)**. Suppose \( \mathcal{L} \) contains a constant symbol \( c \), \( T \) is an \( \mathcal{L} \)-theory, and \( \varphi(\overline{v}) \) is an \( \mathcal{L} \)-formula, then the following are equivalent:

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

**Proof**: 1 \( \rightarrow \) 2 is clear, because a quantifier-free formula \( \psi(\overline{v}) \) is preserved under substructure by (1.2.2.9).

2 \( \rightarrow \) 1. Cf.[Marker, P74]. \( \Box \)

**Lemma (1.2.5.3)**. Let \( T \) be an \( \mathcal{L} \)-theory that for any quantifier-free \( \mathcal{L} \)-formula \( \theta(\overline{v},w) \), there is a quantifier-free formula \( \psi(\overline{v}) \) that \( T \models \forall \overline{v}(\varphi(\overline{v}) \leftrightarrow \psi(\overline{v})) \), then \( T \) has quantifier elimination.

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

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

**Prop.(1.2.5.4)** [Criterion for Quantifier Elimination]. Combining (1.2.5.2) and (1.2.5.3), we get: If \( T \) is an \( \mathcal{L} \)-theory that for all quantifier-free \( \mathcal{L} \)-formula \( \varphi(\overline{v},w) \) and models \( M, N \models T \), and \( A \subset M \cap N, \overline{v} \in A \), and if there is \( b \in M \) that \( M \models \varphi(\overline{v},b) \) will imply there is \( c \in N \) that \( N \models \varphi(\overline{v},c) \), then \( T \) is quantifier-free.

**Def.(1.2.5.5)** [Algebraically Prime Models]. A theory \( T \) is said to have algebraically prime models if for any \( A \models T \) and an embedding \( i : A \to M \) that for any other \( N \models T \), any embedding \( j : A \to N \) factors through \( i \).

**Def.(1.2.5.6)** [Simply Closed Model]. If \( M, N \) are models of \( T \), and \( M \subset N \), then \( M \) is called simply closed in \( N \), denoted by \( M \prec_s N \), iff for any quantifier-free formula \( \varphi(\overline{v},w) \) and \( \overline{v} \in M^n \), if \( N \models \exists w \varphi(\overline{v},w) \), then so does \( M \).

**Prop.(1.2.5.7)** [Quantifier Elimination Test]. If \( T \) is an \( \mathcal{L} \)-theory that has algebraically prime models, and any inclusion of models for \( T \) is simply closed, then \( T \) has quantifier elimination.

**Proof**: This is an immediate consequence of (1.2.5.4). \( \Box \)

**Def.(1.2.5.8)** [Model Complete]. An \( \mathcal{L} \)-theory \( T \) is called model complete if \( M \prec N \) whenever \( M \subset N \). A complete theory is clearly model complete.

**Prop.(1.2.5.9)**. If \( T \) has quantifier elimination, then \( T \) is model complete.

**Proof**: If \( M \subset N \), let \( \varphi(\overline{v}) \) be an \( \mathcal{L} \)-formula, and \( \overline{v} \in M \), then there is a quantifier-free formula \( \psi(\overline{v}) \) such that \( T \models \forall \overline{v}(\varphi(\overline{v}) \leftrightarrow \psi(\overline{v})) \). By (1.2.2.9), the formula \( \psi(\overline{v}) \) passes between \( M \) and \( N \), so \( M \models \varphi(\overline{v}) \iff M \models \psi(\overline{v}) \iff N \models \psi(\overline{v}) \iff N \models \varphi(\overline{v}) \). \( \Box \)
**Prop.(1.2.5.10) [Minimal Model and Completeness].** If $T$ is model-complete and there is a minimal model $M_0$ that $M_0$ embeds into every model of $T$, then $T$ is complete.

*Proof:* Clearly any model is elementary equivalent to $M_0$, thus clearly $T$ is complete. □

**Prop.(1.2.5.11) [Eliminating Algorithm].** Let $T$ be a decidable theory with quantifier elimination, then there is an algorithm to find the elimination $\psi$ of a given formula $\varphi$.

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

**Examples of Quantifier Elimination**

**Prop.(1.2.5.12).** The theory $DLO(1.2.3.2)$ has quantifier elimination.

*Proof:* Cf.[Marker P72]. □

**Lemma(1.2.5.13).** $DAG(1.2.3.2)$ has algebraically prime models.

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

**Prop.(1.2.5.14).** $DAG$ has quantifier elimination.

*Proof:* We use(1.2.5.7) By?? $DAG$ has algebraically prime models, thus it suffices to show any inclusion of models for $DAG(1.2.3.2)$ is simply closed: For any torsion-free divisible Abelian groups $H \subset G$, $\varphi(\bar{a}, w)$ quantifier-free, $\bar{a} \in H$, $b \in G$ that $G \models \varphi(\bar{a}, w)$. Then $\varphi$ is a disjunction of conjunctions of atomic or negated atomic formulas, and we need to prove $H \models \varphi(\bar{a}, w)$.

So we may assume $\varphi$ is conjunction of atomic formulas and negated atomic formulas:

$$\varphi(\bar{a}, w) \leftrightarrow \bigwedge(g_i + m_i w = 0) \land \bigwedge(h_i + m'_i w \neq 0).$$

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

**Cor.(1.2.5.15).** The theory $DAG$ is complete, by(1.2.5.10), as $(\mathbb{Q}, +, 0)$ embeds in every model of $DAG$, and(1.2.5.14)(1.2.5.9).

**Prop.(1.2.5.16).** The theory $ODAG$ is a complete theory with quantifier elimination. In particular, any ordered divisible Abelian group is elementarily equivalent to $(\mathbb{Q}, +, <)$, by completeness.

*Proof:* Cf.[Marker, P80]. □

**Prop.(1.2.5.17) [Presburger Arithmetic].** Presburger arithmetic is a complete decidable theory with quantifier elimination in the language $\mathcal{L}^*$.

*Proof:* Cf.[Marker, P84]? □

**Strongly Minimal Theory**

**Def.(1.2.5.18) [Strongly Minimal Theory].** A theory $T$ is called strongly minimal iff for any $\mathcal{M} \models T$, every definable subset of $\mathcal{M}$ is either finite or cofinite.

**Prop.(1.2.5.19).** $DAG(1.2.3.2)$ is strongly minimal.

*Proof:* Cf.[Marker P78]. □
6 Algebraically Closed Fields

Lemma (1.2.6.1). $ACF_p(1.2.3.2)$ is $\kappa$-categorical for all uncountable cardinal $\kappa$.

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

Prop. (1.2.6.2). The theory $ACF_p$ is complete, by (1.2.6.1) and (1.2.4.28).

Cor. (1.2.6.3). $ACF_p$ is decidable, in particular, $\text{Th}(\mathbb{C})$, the first-order theory of the fields of complex numbers, is decidable.

Proof: $ACF_p$ is complete by (1.2.6.1) and (1.2.4.28), it is clearly recursive, and it is clearly satisfiable, so use (1.2.4.29).

Prop. (1.2.6.4) [First order Lefschetz Principle]. Let $\varphi$ be a sentence in the language of rings, the following are equivalent:
1. $\varphi$ is true in $\mathbb{C}$.
2. $\varphi$ is true in every(some) alg.closed field of char 0.
3. For $p$ large/there exists arbitrary large $p$, $\varphi$ is true in any alg.closed field of char $p$.

Proof: 1, 2 are equivalent because $ACF_p$ is complete (1.2.6.2) and use Gödel’s completeness theorem. If 2 is true, then $ACT_0 \models \varphi$, so by (1.2.4.22), then some $\Delta \models \varphi$. So for $p$ sufficiently large, $ACF_p \models \Delta$, so $ACF_p \models \varphi$ for $p$ large.
If $ACF_0 \models \neg \varphi$, then $ACF_0 \models \neg \exists \varphi$ by completeness (1.2.6.2), so by above argument, $ACF_p \models \neg \exists \varphi$ for $p$ large, contradiction.

Cor. (1.2.6.5) [Ax]. Any injective polynomial map from $\mathbb{C}^n$ to $\mathbb{C}^n$ is surjective.

Proof: By Lefschetz principle (1.2.6.4), it suffices to show this for $(\mathbb{F}_p)^{alg}$ for $p$ large. If this is not true, then choose the coefficients of the coordinate map of $f$, and the coordinates of an element that is not in the image, then the subfield $k$ they generated is algebraic over $\mathbb{F}_p$, so it is finite, and clearly $f$ is also surjective on $k^n$, contradiction.

Cor. (1.2.6.6). Let $K \subset L$ be alg.closed fields, and $V, W$ be varieties defined over $K$, and $f$ is a polynomial isomorphism of $V$ and $W$ over $L$, then there is a polynomial isomorphism of $V$ and $W$ over $K$.

Proof: Let $f$ have degree $d$. Then we can write a formula $\Psi$ saying that there is an embedding of $K$ into $M$ and there is a polynomial bijection of $V$ and $W$ over $M$, then $L \models \Psi$, and because $ACF$ is complete (1.2.6.2), $K \models \Psi$, too. Thus there is also an isomorphism over $K$.

Prop. (1.2.6.7). $ACF_\forall$ is the theory of integral domains.

Proof: Clearly a ring is a subring of an alg.closed field iff it is an integral domain, so the result follows from (1.2.4.38).

Prop. (1.2.6.8). $ACF$ has qualifier elimination.
Proof: Use (1.2.5.5), clearly it has algebraically prime models (1.2.6.7), and we need to check simply closedness.

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

Cor. (1.2.6.9). \( ACF \) is model-complete, by (1.2.5.9).

Lemma (1.2.6.10). Let \( K \) be a field, then the subsets of \( K^n \) defined by atomic formulas are exactly Zariski closed subsets. And a subset of \( K^n \) that is quantifier-definable iff it is a Boolean combination of Zariski closed subsets (constructible). (Clear).

Prop. (1.2.6.11). \( ACF \) is strongly minimal.

Proof: Because by quantifier elimination (1.2.6.8), every definable set is a finite Boolean combination of sets of the form \( V(p) = 0 \), where \( p \in K[X] \), but \( V(p) \) is either finite or all of \( K \). \( \square \)

Elimination of Imaginaries in Alg.Closed Fields

Def. (1.2.6.12) [Algebraicity]. Let \( M \) be an \( L \)-structure and \( A \subset M \), then for \( b \in M \), \( b \in acl(A) \) if there is a formula \( \varphi(x, \overline{y}) \) and \( \pi \in A \) that \( M \models \varphi(b, \pi) \), and \( \{ x \in M | M \models \varphi(x, \pi) \} \) is finite.

Def. (1.2.6.13) [Algebraicity over Equivalence Class]. Let \( M \) be an \( L \)-structure and \( E \) a definable equivalence relation on \( M^n \), then we say a element \( c \in M \) is algebraic over \( \overline{a}/E, b_1, \ldots, b_m \) if there is a formula \( \varphi(c, \overline{y}, \overline{\pi}) \) that

1. \( M \models \varphi(c, \overline{a}, \overline{b}) \).
2. If \( \overline{a} E \overline{a}' \), then \( M \models \varphi(c, \overline{a}, \overline{b}) \iff \varphi(c, \overline{a}', \overline{b}) \).
3. \( \{ x | M \models \varphi(x, \overline{\pi}, \overline{b}) \} \) is finite.

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

Lemma (1.2.6.14). Suppose \( \overline{c} \) is algebraic over \( \overline{a}/E, \overline{d}, \overline{b} \), and \( \overline{b} \) is algebraic over \( \overline{a}/E, \overline{d} \), then \( \overline{c} \) is also algebraic over \( \overline{a}/E, \overline{d} \).

Proof: Cf. [Marker, P92]. \( \square \)

Lemma (1.2.6.15). Suppose \( K \) is an alg.closed field and \( E \) is a definable equivalence relation on \( K^n \), and \( \psi(\overline{x}, \overline{y}, \overline{d}) \) defines \( E \). If \( \overline{a} \in K^n \), then there is a \( \overline{c} \in K^n \) algebraic over \( \overline{a}/E, \overline{d} \) s.t. \( \overline{c} E \overline{a} \).

Proof: Cf. [Marker, P92]. \( \square \)

Prop. (1.2.6.16) [Elimination of Imaginaries]. Let \( K \) be an alg.closed field, \( A \subset K \), and \( E \) is an \( A \)-definable equivalence relation on \( K^n \), then for some \( l \) there is an \( A \)-definable function \( f : K^n \to K^l \) that \( x E \overline{y} \iff f(\overline{x}) = f(\overline{y}) \).

Proof: Cf. [Marker, P92]. \( \square \)
7 Real Closed Fields

Prop. (1.2.7.1). The class of real closed fields is an elementary class (1.2.2.8) of $L_r$-structures.
Proof: The real closed fields are axiomatized by:
- Axioms for fields.
- For each $n \geq 1$, the sentence $\forall x_1 \ldots \forall x_n (x_1^2 + \ldots + x_n^2 + 1 \neq 0)$.
- $\forall x \exists y (y^2 = x \lor y^2 + x = 0)$.
- For each $n \geq 0$, the sentence $\forall x_1 \ldots \forall x_n \exists y (y^{2n+1} + \sum_{i=0}^{2n} x_i y^i = 0)$.
These truly axiomatize real closed fields, by (2.2.9.7).

Prop. (1.2.7.2). Let $F$ be a real closed field, then the definable sets in $F^n$ w.r.t the $L_{or}$ is also definable w.r.t. $L_r$.
Proof: Because we can replace all instances $t_i < t_j$ by $\exists v (v \neq 0 \land t_i + v^2 = t_j)$.

Prop. (1.2.7.3). $RCF$ is the theory of ordered integral domains (easy).

Cor. (1.2.7.4). $RCF$ has algebraically prime models.
Proof: Let $D$ be an ordered domain, and let $R$ be a real closure of the fraction field of $D$ compatible with the ordering of $D$. Let $F$ be another real closed field extension of $D$, then let $K$ be the algebraic closure of the fraction field of $D$ in $F$, then $K$ is a real closed field by (2.2.9.7), then by (2.2.9.12) there is an isomorphism of $R \cong K$ extending $D \to K$, thus embeds $R$ into $F$ extending $D \to F$.

Prop. (1.2.7.5). $RCF$ has quantifier elimination (w.r.t. $L_{or}$).
Proof: Use (1.2.5.5), it has algebraically prime models by (1.2.7.4), and we need to check simply closedness: Let $F \subset K$ be RCFs, $\varphi(v,\overline{a})$ be a quantifier-free formula and let $\overline{a} \in F, b \in K$ that $K \models \varphi(b,\overline{a})$. Then there are polynomials that

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

If any $p_i \neq 0$, then $b$ is algebraic over $F$, but then $b \in F$ because $F$ is real closed. So we may assume $\varphi(v,\overline{a}) \leftrightarrow \bigwedge q_i(v) > 0)$. Then because $q_i(b) > 0$ and $q_i$ has f.m. zeros, by intermediate property (2.2.9.9), we can find a nbhd of $b$ that is interval with endpoints in $F$ that $q_i > 0$, and because $F$ is dense (char 0), there is an element $b'$ that $F \models \varphi(b',\overline{a})$.

Cor. (1.2.7.6). $RCF$ is complete and decidable. Thus it is just the theory of $(\mathbb{R},+,-,\cdot,\langle\rangle)$, and it is decidable.
Proof: It is model-complete by (1.2.5.9), and it has a minimal model that is the field $\mathbb{R}_{alg}$ of algebraic numbers in $\mathbb{R}$, then it is complete by (1.2.5.10). It is decidable by (1.2.4.29).

Prop. (1.2.7.7) $[RCF$ is O-Minimal]. The theory $RCF(1.2.3.2)$ is o-minimal.
Proof: Because $RCF$ has quantifier elimination, every definable set of a real closed field $R$ is semialgebraic, thus it is clearly a disjoint union of intervals and points.
Semia
gebraic Sets

Def. (1.2.7.8) [Semia
gebraic Sets]. Let $F$ be an ordered field, then $X \subset F^n$ is called semi-
gebraic if there it is a Boolean combination of sets of the form $\{ \bar{x} | p(\bar{x}) > 0 \}$, where $p(\overline{X}) \subset F[\overline{X}]$.

Prop. (1.2.7.9) [Tarski-Seidenberg Theorem]. If $F$ is a real closed field, the semialgebraic sets are closed under projection.

Proof: This is because quantifier elimination (1.2.7.5) implies semialgebraic sets are just definable
sets, and the projection of a definable set is also definable. □

Cor. (1.2.7.10). The composite of two semialgebraic functions are semialgebraic.

Prop. (1.2.7.11) [Closure of Semialgebraic Sets]. Let $F$ be a real closed field and $A \subset F^n$ be semialgebraic, then the closure of $A$ in the Euclidean topology is also semialgebraic.

Proof: The closure of $A$ is defined by

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

Thus it is definable, and thus semialgebraic by quantifier elimination (1.2.7.5). □

Prop. (1.2.7.12). Let $F$ be a real closed field and $X \subset F^n$ be closed and bounded, $f$ be a continuous semialgebraic function, then $f(X)$ is closed and bounded.

Proof: If $F = \mathbb{R}$, then this follows from (3.6.5.2) that $X$ is compact hence the image is also compact hence closed and bounded. As we can formulate a sentence asserting the conclusion. Thus the theorem follows as $RCF$ is complete (1.2.7.6). □

Lemma (1.2.7.13). For $R$ a real closed field and $f : R \to R$ semialgebraic, then for any interval $U$ there is an element $x$ that $f$ is continuous at $x$.

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

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

Prop. (1.2.7.14). For $R$ a real closed field and $f : R \to R$ semialgebraic, then $f$ is discontinuous only at f.m. points.

Proof: The discontinuous points of $f$ is definable by

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

thus it is a finite union of intervals and points, by $o$-minimality (1.2.7.7), but it must be f.m. points, by (1.2.7.13). □

Def. (1.2.7.15). We can naturally define the notion of definably connected and definably arcwise connected sets in $R^n$. 

Def.(1.2.7.16)[Cells]. For an real closed field $F$, we inductively define $n$-cells:

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

Prop.(1.2.7.17)[Uniform Bounding]. Let $X \subset F^{m+1}$ be semialgebraic, then there is a natural number $N$ that if $\overline{a} \in F^n$ and $X_{\overline{a}} = \{y | (\overline{a}, y) \in X\}$ is finite, then $|X_{\overline{a}}| < N$.

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

Now let $\Gamma$ be the theory

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

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

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

Then by compactness theorem, there is some f.m. sentences of $\Gamma$ that is unsatisfiable, thus the conclusion follows.

Prop.(1.2.7.18)[Cell Decomposition]. Let $F$ be a real closed field, then any semialgebraic set $X \subset F^m$ is a finite disjoint union of cells.

Proof: Cf.[Marker, P103].

8 $O$-Minimal Structures

Cf.[O-Minimal Structures].

Def.(1.2.8.1)[O-Minimal Structure]. An ordered structure is called $o$-minimal if any definable set is a finite union of intervals with endpoints in $M \cup \{\pm \infty\}$ and points.

Def.(1.2.8.2)[General O-Minimal Expansions]. A structure expanding the real closed field $R$ is a collection $\mathcal{S} = (\mathcal{S}^n)$, where $\mathcal{S}^n$ is a family of subsets of $R^n$, that

- Algebraic subsets are in $\mathcal{S}$.
- Each $\mathcal{S}^n$ is a Boolean subalgebra of the powerset of $R^n$.
- $\mathcal{S}$ is stable under Cartesian product and projection.

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

2.1 Group Theory

Main References are [Finite Groups, Issac], [Lan05] and [代数学引论，丁石孙].

1 Notations

Notations(2.1.1.1). • Use notations defined in ??.

2 Magmas

Def.(2.1.2.1)[Binary Operators]. A binary operator on a set $X$ is a map $\circ : X \times X \to X$.

Def.(2.1.2.2)[Unital Operator]. A unital binary operator on a set $X$ is a map $\circ : X \times X \to X$ that has a left and right identity element $1_\circ$.

Prop.(2.1.2.3)[Associative Operators]. An associative operator on a set $X$ is an operator $\circ : X \times X \to X$ s.t. $(x \circ y) \circ z = x \circ (y \circ z)$ for any $x, y, z \in X$.

Def.(2.1.2.4)[Magma]. A magma is a set $X$ with a binary operator $\circ : X \times X \to X$. A unital magma is a magma that the operator is unital. It is called Abelian if $x \circ y = y \circ x$ for any $x, y \in X$.

Prop.(2.1.2.5)[Eckmann-Hilton argument]. If $\circ$ and $\otimes$ are two unital binary operators on a set that commute with each other: $(a \otimes b) \circ (c \otimes d) = (a \circ c) \otimes (b \circ d)$, then they are equal and in fact commutative and associative.

Proof: Firstly the units coincide, because

$$1_\circ = 1_\circ \circ 1_\circ = (1_\otimes \circ 1_\otimes) \circ (1_\otimes \circ 1_\otimes) = (1_\circ \circ 1_\circ) \circ (1_\circ \circ 1_\circ) = 1_\otimes \otimes 1_\otimes = 1_\otimes.$$  

Next

$$a \circ b = (1 \otimes a) \circ (b \otimes 1) = (1 \circ b) \otimes (a \circ 1) = b \otimes a = (b \circ 1) \otimes (1 \circ a) = (b \otimes 1) \circ (1 \otimes a) = b \circ a.$$  

Thus $\circ$ and $\otimes$ coincide and are commutative. Finally for associativity:

$$(a \otimes b) \otimes c = (a \otimes b) \otimes (1 \otimes c) = (a \otimes 1) \otimes (b \otimes c) = a \otimes (b \otimes c).$$  

□

Def.(2.1.2.6)[Monoid]. A monoid is an associative unital magma $(X, \circ)$.


3 Groups

Def. (2.1.3.1) [Groups]. The category of Groups is denoted by $\mathfrak{G}_{\text{rp}}$.

Def. (2.1.3.2) [Generators]. Let $G \in \mathfrak{G}_{\text{rp}}$ and $S \subset G$, then $S$ is said to be a set of generator for $G$ if the only subgroup of $G$ containing $S$ is $G$.

Def. (2.1.3.3) [Normal Subgroups]. A normal subgroup of a group $G$ is a subgroup $N$ that if $x \in G$, then $x^{-1}N x = N$.

Def. (2.1.3.4) [Simple Groups]. A simple group is a group that has no normal subgroups.

Def. (2.1.3.5) [Finitely Generated Group]. A group $G$ is called finitely generated if there is a finite subset $S$ that the only subgroup containing $S$ is $G$ itself.

Def. (2.1.3.6) [Product Subgroups]. Let $G$ be a group and $N, H$ be subgroups such that $N$ is normal in $G$, then $NH = \{x \in G | x = nh, n \in N, h \in H\}$ is a subgroup of $G$, called the product subgroup.

Def. (2.1.3.7) [Coset]. Let $G$ be a group and $H$ a subgroup. Consider the equivalence relation on $G$ s.t. $x \sim y$ iff $x = yh$ for some $h \in H$, then the equivalence classes is denoted by $G / H$, called the right coset of $H$ in $G$. And $G$ acts on this set by left translation.

Prop. (2.1.3.8) [Fundamental Isomorphisms]. Let $G$ be a group and $N, H$ be subgroups such that $N$ is normal in $G$, then

- there is a natural isomorphism $G / NH \cong (G / N) / (H / H \cap N)$ as sets, and if $H$ is also normal, this is an isomorphism of groups.
- there is a natural isomorphism of groups: $H / N \cap H \cong NH / N$.

Proof: 1: Consider the natural isomorphism $N \mapsto NH / H : n \mapsto nH$, then it is a group homomorphism, and the kernel is $N \cap H$, thus we are done.

Cor. (2.1.3.9). if $H_1, H_2$ are subgroups of a group $G$ that has finite indexes, then $H_1 \cap H_2$ also has finite index in $G$.

Prop. (2.1.3.11). If a finite group $G$ has an automorphism $\alpha$ that $\alpha^2 = id$ and $\alpha$ has no fixed point other than $e$, then $G$ is an Abelian group of odd order.
Proof: $G$ is clearly of odd order. Consider the map $g \mapsto \alpha(g)g^{-1}$, then it is injective, hence it is also surjective, and consider $\alpha(\alpha(g)g^{-1}) = g\alpha(g)^{-1} = (\alpha(g)g^{-1})^{-1}$, thus $\alpha(h) = h^{-1}$ for all $h \in G$, thus clearly $G$ is Abelian. \hfill \Box

Prop.(2.1.3.12). If $H$ is a subgroup of a finite group $G$, then $G \neq \bigcup g^{-1}Hg$.

Proof: There are at most $|G\lhd H|$ different summands in the right hand side, so it doesn’t have enough elements. \hfill \Box

Prop.(2.1.3.13). If $G$ is a f.g. group\(^{(2.1.3.5)}\) and $H$ is a group of finite index in $G$, then $H$ is f.g.

Proof: Suppose $G$ has generators $g_i$, we may add their inverses to it, and let $Ht_1, \ldots, Ht_m$ are all the right cosets with $t_1 = 1$, then there are $h_{ij}$ that $t_i g_j = h_{ij} t_{kij}$, then we claim $H$ is generated by $h_{ij}$.

For this, consider any $h = \prod g_i$, then $g_1 = h_{1t} t_{k_1t}$, and we can do this from left to right. Now $h = \prod h_{i_{ij}} t_o$, then $t_o$ must by 1, and we are done. \hfill \Box

Prop.(2.1.3.14). Let $\varphi : G \to H$ be a map of sets between groups s.t. $\# \text{Im}(\varphi) = \infty$, and for each $g \in G$, there is a set $S(g) \in H$ that $\varphi(h)\varphi(g) = \varphi(hg)$ for any $h$ s.t. $\varphi(h) \notin S(g)$, then $\varphi$ is a homomorphism.

Proof: For $g, h \in G$, take $f$ s.t. $\varphi(f) \notin S(g) \cup \varphi(g)^{-1} S(h) \cup \{\varphi(gh)\}$. Then

$$\varphi(f)\varphi(g)\varphi(h) = \varphi(fg)\varphi(h) = \varphi(fgh) = \varphi(f)\varphi(gh),$$

thus $\varphi(g)\varphi(h) = \varphi(gh)$. \hfill \Box

4 Abelian Groups

Remark(2.1.4.1). An Abelian group is the same as a module over $\mathbb{Z}$. Thus the theory of commutative algebra applies in this case.

Prop.(2.1.4.2)[Abelianization]. There is a functor from the category of Abelian semi-groups to the category of Abelian groups that is left adjoint to the forgetful functor, called the Abelianization.

Proof: Define $A'$ to be the quotient

$$\bigoplus_{(a,b) \in A^2} \mathbb{Z} \to \bigoplus_{x \in A} \mathbb{Z} \to A' \to 0,$$

where $1_{(a,b)}$ is mapped to $1_a + 1_b - 1_{a+b}$. Then it can be seen this satisfies the universal property and it is functorial in $A$. \hfill \Box

Prop.(2.1.4.3)[Classifying F.g. Abelian Groups]. Any finitely generated Abelian group is of the form

$$\mathbb{Z}^r \bigoplus_{p_i \text{ primes}} \mathbb{Z}/(p_i^{a_i}),$$

Proof: As $\mathbb{Z}$ is PID, the classifying theorem follows immediately from(2.2.4.21): \hfill \Box
Prop. (2.1.4.4) [Baer-Specker Group]. The group $\prod^N \mathbb{Z}$ is called the Baer-Specker group. Then the natural homomorphism

$$\text{Hom}(\prod^N \mathbb{Z}, \mathbb{Z}) \to \prod^N \mathbb{Z}$$

is injective with image $\bigoplus^N \mathbb{Z}$. In particular, by countability argument, $\prod^N \mathbb{Z}$ is not a free group (4.3.1.5). Moreover, any infinite direct product of $\mathbb{Z}$ is not free, because otherwise the subgroup $\prod^N \mathbb{Z}$ would be free.

Proof: The natural homomorphism is the composite?

$$\text{Hom}(\prod^N \mathbb{Z}, \mathbb{Z}) \xrightarrow{\text{?}} \text{Hom}(\#^N \mathbb{Z}, \mathbb{Z}) \xrightarrow{\eta} \prod^N \mathbb{Z}.$$ 

Thus the assertion follows from (2.1.6.6) and (2.1.6.5).

□

Remark (2.1.4.5). This can be proven in other ways, like using condensed mathematics.

Forms on Abelian Groups

Def. (2.1.4.6) [Quadratic Forms]. For $A \in \text{Ab}$, a function $d : A \to \mathbb{R}$ is called a quadratic form if

- $d(\alpha) = d(-\alpha)$ for any $\alpha \in A$.
- The form $B_d : A \times A \to \mathbb{R}$ $(\alpha, \beta) \mapsto [d(\alpha + \beta) - d(\alpha) - d(\beta)]/2$ is bilinear.

It is called positive semi-definite if moreover $d(\alpha) \geq 0$. And positive-definite if moreover $d(\alpha) = 0 \iff \alpha = 0$.

Prop. (2.1.4.7) [Cauchy-Schwartz]. Let $A$ be an Abelian group and $d$ a positive semi-definite quadratic form over $A$, then

$$|d(\alpha - \beta) - d(\alpha) - d(\beta)| \leq 2\sqrt{d(\alpha)d(\beta)}.$$ 

Proof: Consider the bilinear form $B_d$, then

$$0 \leq d(m\alpha - n\beta) = m^2d(\alpha) + n^2d(\beta) - 2mnB_d(\alpha, \beta).$$

This is true for any $m, n \in \mathbb{Z}$, thus the discriminant $B_d(\alpha, \beta)^2 \leq d(\alpha)d(\beta)$. □

Prop. (2.1.4.8). If $M, N$ are Abelian groups and $d$ is a quadratic form on $M \times N$ s.t. $d(0 \times N) = d(M \times 0) = 0$, then $d$ is bilinear in both $M$ and $N$.

Proof: The bilinear form associated to $d$ satisfies $B_d((a, 0), (0, b)) = d(a, b)$, thus it is clear $d$ is bilinear in $M$ and $N$. □

Def. (2.1.4.9) [Polarization]. Let $\Gamma$ be an Abelian group and $h : \Gamma \to \mathbb{R}$ is a function, then the $r$-th polarization function $P_r(h) : \Gamma^r \to \mathbb{R}$ is defined to be

$$P_r(h)(x_1, \ldots, x_r) = \frac{1}{r!} \sum_{I \subseteq \{1, \ldots, r\}} (-1)^{r - \#I} \prod_{i \in I} x_i.$$ 

Lemma (2.1.4.10).
Proposition 2.1.4.11. There is a natural isomorphism of additive groups

\[ \bigoplus_{j=0}^{r-1} \text{Sym}^j \Gamma^r \cong \{ h : \Gamma \to \mathbb{R} \mid P_r(h) = 0 \} : (A_0, \ldots, A_{r-1}) \mapsto \sum_{i=0}^{r-1} \Delta A_i. \]

Proof: This is an injective map by (2.1.4.10), and for any \( h \) that \( P_r(h) = 0 \), By (2.1.4.10) item 1, this means \( A_{r-1} = P_{r-1}(h) \in \text{Sym}^{-1}\Gamma^r \). Let \( h' = h - \Delta A_{r-1} \), then (2.1.4.10) item 4 shows \( P_{r-1}(h') = 0 \), thus we can use induction to show \( h' = \sum_{i=1}^{r-2} \Delta A_i \), thus \( h = \sum_{i=1}^{r-1} \Delta A_i \).

Proposition 2.1.4.12. Let \( \Gamma \) be an Abelian group, for functions \( h_1, h_2 : \Gamma \to \mathbb{R} \), let \( h_1 = h_2 + O(1) \) denote the fact that \( |h_1 - h_2| \) is bounded on \( \Gamma \). Then there is a natural isomorphism of additive groups:

\[ \bigoplus_{j=0}^{r-1} \text{Sym}^j \Gamma^r \cong \{ h : \Gamma \to \mathbb{R} \mid P_r(h) = O(1) \} / O(1) : (A_0, \ldots, A_{r-1}) \mapsto h(x) = A_0 + A_1(x) + \ldots + A_{r-1}(x, \ldots, x). \]

Proof: The map is injective by (2.1.4.11). To show surjectivity:

By hypothesis and (2.1.4.10), there exists \( C > 0 \) s.t.

\[ |P_{r-1}(h(x_0 + x_1, x_2, \ldots, x_{r-1}) - P_{r-1}(h(x_0, x_2, \ldots, x_{r-1}) - P_{r-1}(h(x_1, x_2, \ldots, x_{r-1})| \leq C. \]

So

\[ |P_{r-1}(h(2^N x_1, x_2, \ldots, x_{r-1}) - 2P_{r-1}(h(2^{N-1} x_1, x_2, \ldots, x_{r-1})| \leq C \]

for any \( N \), and by iterating,

\[ |P_{r-1}(h(2^N x_1, 2^N x_2, \ldots, x_{r-1}) - 2^{r-1}P_{r-1}(h(2^{N-1} x_1, 2^{N-1} x_2, \ldots, 2^{N-1} x_{r-1})| \leq (2^{r-1} - 1)C. \]

Thus

\[ A_{r-1}(x_1, \ldots, x_{r-1}) = \lim_{N \to \infty} \frac{P_{r-1}(h(2^N x_1, 2^N x_2, \ldots, x_{r-1})}{2^{N(r-1)}} \]

exists, and it is clear that \( A_{r-1} \in \text{Sym}^{r-1}\Gamma^r \) and \( A_{r-1}(x_1, \ldots, x_{r-1}) - P_{r-1}(h(x_1, \ldots, x_{r-1}) \leq 2^{r-1}C. \)

Let \( h' = h - \Delta A_{r-1} \), then \( P_{r-1}h' = P_{r-1}h - A_{r-1} = O(1) \), thus we can use induction to show \( h' = \sum_{i=1}^{r-2} \Delta A_i + O(1) \), thus \( h = \sum_{i=1}^{r-1} \Delta A_i + O(1) \).

Corollary 2.1.4.13. Let \( \Gamma \) be an Abelian group and \( h : \Gamma \to \mathbb{R} \) be a function on an Abelian group \( \Gamma \) that

\[ h(\sum_{i=1}^{3} x_i) = \sum_{1 \leq i < j \leq 3} h(x_i + x_j) - \sum_{i=1}^{3} h(x_i) + O(1), \]

then there exists a unique symmetric bilinear pairing \( b \) on \( \Gamma \) and \( l \) a homomorphism \( \Gamma \to \mathbb{R} \), that

\[ h(x) = \frac{1}{2} b(x, x) + l(x) + O(1). \]
Prop.\,(2.1.4.14). Let $M$ be an Abelian group and $b : M \times M \to \mathbb{R}$ is a bilinear form on $M$ that $\text{rad}(B) = 0$, so $b$ defines a bilinear form on $B_\mathbb{Z} : M \otimes \mathbb{Z} \to \mathbb{R}$. Then $b_\mathbb{R}$ is positive-definite iff for any f.g. subgroup $M'$ of $M$ and $C > 0$, $\{ x \in M' | b(x, x) \leq C \}$ is finite.

Proof: We may assume $M$ is f.g.. As $M/M_{\text{tor}}$ is torsion-free, it is a lattice in $M_\mathbb{R}(1.2.3.29)$. Assume $b_\mathbb{R}$ is positive-definite, then it defines a topology on $M_\mathbb{R}$, then $\{ x \in M' | b_\mathbb{R}(x, x) \leq C \}$ is finite because it is a compact discrete set.

Conversely, if $\{ x \in M' | b(x, x) \leq C \}$ is finite and $b_\mathbb{R}$ is not positive-definite, then it is at least semi-positive definite. If $b_\mathbb{R}(y, y) = 0$, then by Cauchy-Schwartz inequality (2.1.4.7), $y$ is in the radical of $b_\mathbb{R}$. By hypothesis $y \notin M_\mathbb{Q}$.

Now choose a basis $e_1, \ldots, e_n$ of $M$, for any $n > 1$, there is a $y_n \in M$ s.t.

$$y_n - ny \in S = \{ \sum \alpha_i e_i | 0 \leq \alpha_i \leq 1 \},$$

and we can use induction.

$$b_\mathbb{R}(y_n, y_n) = b_\mathbb{R}(y_n - ny, y_n - ny)$$

is bounded by the maximal value of $b_\mathbb{R}$ on $S$. These $y_n$ are all different because $y \notin M_\mathbb{Q}$, thus contradicting the hypothesis. \hfill \Box

Prop.\,(2.1.4.15). Let $M \in \text{Ab}$ s.t. $\#M/\#M < \infty$ for some $n \geq 2$ and there is a positive semi-definite symmetric bilinear form $B$ on $M$ s.t. $\{ x \in M | B(x, x) \leq C \}$ is finite for any $C > 0$, then $M$ is f.g..

Proof: Choose a set of generators $\{ x_i \}$ for $M/\#M$. Now there is a constant $C$ that whenever $(x, x) \geq C$,

$$(x - x_i, x - x_i) < 2(x, x), \forall i,$$

because by Cauchy-Schwartz inequality (2.1.4.7), $(x - x_i, x - x_i)$ is similar to $(x, x)$ when $(x, x)$ is large.

Now let $\Gamma = \{ x_1, \ldots, x_s \} \cup \{ x \in \Gamma | (x, x) < C \}$. Then $\Gamma$ is finite by hypothesis. We prove $\Gamma$ generates $M$: Consider the infimum $C_0$ of $(x, x)$ that $x$ is not generated by $M$, then there is a $x$ that $C_0 \leq (x, x) < 2C_0$. Obviously $C_0 \geq C$. Let $x = x_i + ny$ for some $x_i \in \Gamma, y \in M$, then

$$(y, y) = \frac{1}{n^2}(x - x_i, x - x_i) < \frac{2}{n^2}(x, x) \leq \frac{1}{2}(x, x) < C_0.$$

Thus by minimality of $C_0$, $y \in \Gamma$, thus $x \in \Gamma$. \hfill \Box

Def.\,(2.1.4.16)[Lagrangian Decomposition]. Let $A$ be a f.g. Abelian group and $\Gamma : A \times A \to \mathbb{Q}/\mathbb{Z}$ is a bilinear alternating non-degenerate pairing, then a Lagrangian decomposition of $A$ is an Abelian subgroup $B \subset A$ s.t. $\Gamma|_B = 0$, called an isotropic subgroup of $A$, such that $A \cong B \oplus \hat{B}$, and $\Gamma$ is given by

$$\Gamma((x, \chi), (y, \psi)) = \chi(y) \psi(x)^{-1}.$$

Prop.\,(2.1.4.17). Let $A$ be a f.g. Abelian group and $\Gamma : A \times A \to \mathbb{Q}/\mathbb{Z}$ is a bilinear alternating non-degenerate pairing, then $A$ admits a Lagrangian decomposition.

In particular, if $\#A < \infty$, then $\#A$ is a perfect square.

Proof: Because $A$ is f.g., take $x, y$ in $A$ s.t. $\Gamma(x, y)$ has the maximal denominator, then it is easy to see that for any $z \in A$, $z - ax - by \in \text{span}(x, y)_\perp$ for some $a, b \in \mathbb{Z}$, so $A = \text{span}(a, b) \oplus \text{span}(a, b)_\perp$, and we can use induction. \hfill \Box
Finite Abelian Groups

**Prop.(2.1.4.18)** [Characterizing Finite Cyclic Groups]. Let \( G \in \text{Ab}^{\text{fin}} \) that \( \#\{x \in G | x^d = 1 \} \leq d \) for any \( d \geq 1 \), then \( G \) is cyclic.

*Proof:* Consider the subset \( G_d \) of elements of order \( d \), if it is non-empty, choose \( y \in G_d \), then \( \# \langle y \rangle \geq d \), thus \( \langle y \rangle = \{ x \in G | x^d = 1 \} \), which means \( \#G_d \leq \varphi(d) \). Then \( |G| = \sum_{d|n} \#G_d \leq \sum_{d|n} \varphi(d) = n \). Thus \( G_n \neq \emptyset \), which means \( G \) is cyclic. \( \square \)

**Cor.(2.1.4.19).** Any finite subgroup of the multiplicative group of a field is cyclic.

5 Automorphism Group

**Prop.(2.1.5.1).** Any group of order \( > 2 \) have at least 2 automorphisms.

*Proof:* Assume the contrary, consider its inner automorphism, then it is Abelian, and then multiplying by \( p \) for \( p \) large prime is not identity, Then \( |G||p - 1 \) for such \( G \). Now it is clear \( |G| = 2 \), because otherwise we can choose \( p \equiv 2 \mod |G| \). \( \square \)

**Def.(2.1.5.2).** A group is called **complete** if all automorphisms of \( G \) are inner.

**Prop.(2.1.5.3).** \( S_n \) is the automorphism group of \( A_n \) for \( n = 5 \) or \( n \geq 7 \).

*Proof:* \( \square \)

**Prop.(2.1.5.4).** If \( G \) is a non-Abelian simple group, then \( \text{Aut}(G) \) is a complete group.

**Prop.(2.1.5.5).** \( S_n \) are complete groups except for \( S_5 \).

*Proof:* \( S_n \) is the automorphism group of \( A_n \) for \( n = 5 \) or \( n \geq 7 \) by(2.1.5.3), thus it is complete by(2.1.5.4). \( \square \)

**Prop.(2.1.5.6)** [Wielandt]. If \( G \) is a finite group with trivial center, then the sequence

\[
G < \text{Aut}(G) < \text{Aut}(\text{Aut}(G)) < \ldots
\]

must terminate in finite steps.

*Proof:* \( \square \)

6 Free Groups and Presentations

**Def.(2.1.6.1)** [Free Groups]. There is a **free group** functor \( F : \text{Set} \rightarrow \text{Grp} \) that is left adjoint to the forgetful functor.

The image of the set \( [n - 1] \) is denoted by \( F_n \).

*Proof:* For the existence of \( F \), Cf.[Lan05]P66. \( \square \)

**Prop.(2.1.6.2)** [Nielsen-Schreier]. A subgroup \( H \) of a free group \( G \) is a free group. Moreover, a subgroup \( H \) of finite index \( m \) in \( F_n \) is isomorphic to \( F_{1 + m(n-1)} \).
Proof: A free group is the fundamental group of a graph $X$ which is a wedge sum of circles, and there is a covering $X_H \to X$ the $\pi_1(X_H) = H$ by (3.11.1.28). And if $H$ is of index $m$ in a free group $G$, $X_H \to X$ has degree $m$ by (19.1.1.5). Now (19.1.1.5) shows $H = \pi_1(X_H)$ is a free group, and the final assertion follows by comparing two ways of counting Euler number $\chi$. □

Prop. (2.1.6.3). Use the same method as in (2.1.6.2), we can determine all the subgroups of index 2 in $F_2$.

Proof: □

Def. (2.1.6.4) [Earring Group]. For any $n \in \mathbb{Z}_+$, there are group homomorphisms $F_n \to F_{n-1}$ corresponding to the map of sets

$$[n-1] \to F_{n-1} : i \mapsto \begin{cases} [i] & , i \leq n-2 \\ 1 & , i = n-1 \end{cases}.$$ 

The Earring group $\#^{\mathbb{N}}\mathbb{Z}$ is defined to be the subgroup of

$$\lim_{\xrightarrow{n \in \mathbb{N}}} F_n$$

consisting of elements $(w_0, w_1, \ldots, w_n, \ldots)$ s.t. if each $w_n$ is a reduced word, then for any $k \in \mathbb{Z}_+$, the number of $[k]^\pm$ appearing in $w_n$ stablizes.

Prop. (2.1.6.5). The natural homomorphism

$$\eta : \text{Hom}(\#^{\mathbb{N}}\mathbb{Z}, \mathbb{Z}) \to \prod_{\mathbb{N}} \mathbb{Z}$$

is injective with image $\oplus^{\mathbb{N}}\mathbb{Z}$.


Prop. (2.1.6.6). There is a natural group homomorphism $\varepsilon : \#^{\mathbb{N}}\mathbb{Z} \to \prod_{\mathbb{N}} \mathbb{Z}$ that is surjective.

Proof: The $k$-th coordinate of this map is given by omitting all the elements that is not $[k]$. It is clearly surjective. □

Prop. (2.1.6.7) [Smith]. $\#^{\mathbb{N}}\mathbb{Z}$ is not a free group.


List of Presentations of Important Groups

Prop. (2.1.6.8). Let $F$ be a field, then $SL(2, F)$ has a representation as:

$$\langle t(y), n(z), w_1 \rangle, \quad y \in F^*, z \in F$$

quotient the relations:

$$t(y_1)t(y_2) = t(y_1y_2), \quad n(z_1)n(z_2) = n(z_1 + z_2), \quad t(y)n(z)t(y)^{-1} = n(y^2z), \quad w_1t(y)w_1 = t(-y^{-1}).$$
\[w_1 n(z) w_1 = t(-z^{-1}) n(-z) w_1 n(-z^{-1}), \ z \in F^*,\]

And the isomorphism is given by \( \Phi \):

\[t(y) \mapsto \begin{bmatrix} y & \ y^{-1} \end{bmatrix}, \ n(z) \mapsto \begin{bmatrix} 1 & z \end{bmatrix}, \ w_1 \mapsto \begin{bmatrix} -1 & 1 \end{bmatrix}.\]

**Proof:** The map vanishes on the relations is direct calculation. An inverse of \( \Phi \) is constructed by

\[\Psi \left( \begin{bmatrix} a & b \\ c & d \end{bmatrix} \right) = \begin{cases} n(a/c) t(-c^{-1}) w_1 n(d/c) & c \neq 0 \\ t(a n(b/a)) & c = 0 \end{cases}\]

The verification of the inverse is verified by direct calculation. □

**Prop.(2.1.6.9).** Let \( F \) be a field, then \( SL(2, F) \) is generated by \( N(F) \) and any element in \( SL(F) \backslash N(F) \).

**Proof:** Take this element in \( G(F) \backslash B(F) \), left and right multiplying by elements in \( N(F) \), we see it contains some \( \begin{bmatrix} a & -a^{-1} \\ \ a^{-1} & 1 \end{bmatrix} \), then it contains \( \begin{bmatrix} a & -a^{-1} \\ \ a^{-1} & 1 \end{bmatrix}^{-1} N(F) \begin{bmatrix} a & -a^{-1} \end{bmatrix} = \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \). Then it contains \( N(F) \begin{bmatrix} a & -a^{-1} \end{bmatrix} = \begin{bmatrix} * & -a^{-1} \end{bmatrix} \). Left multiplying by \( \begin{bmatrix} 1 & * \\ 0 & 1 \end{bmatrix} \) and right multiplying by \( N(F) \), we see it contains all diagonal matrices in \( SL(2, F) \). So it contains \( SL(2, F) \), by Bruhat decomposition. □

**Prop.(2.1.6.10).** \( SL(2, \mathbb{Z}) \) is generated by \( S = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \) with relations

\[S^4 = 1, \quad (ST)^3 = S^2\]

**Proof:** [Serre, Trees, P81]. □

**Cor.(2.1.6.11) [Modular Group].** \( PSL_2(\mathbb{Z}) = SL_2(\mathbb{Z})/\{\pm 1\} \) is generated by \( S = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \) with relations

\[S^2 = 1, \quad (ST)^3 = 1.\]

**Prop.(2.1.6.12) [Braid Group].** The **Braid group** \( B_n \), defined by \( B_n = \pi_1(\mathbb{C}^n \backslash \bigoplus \{z_i = z_j\}/S^n) \) has a presentation by \( b_i, i = 1, \ldots, n-1 \) and relations

- if \( |i - j| \geq 2 \), then \( b_i b_j = b_j b_i \),
- \( b_i b_{i+1} b_i = b_{i+1} b_i b_{i+1} \).

**Proof:** □

**Cor.(2.1.6.13) [Pure braids].** Due to the covering map \( \mathbb{C}^n \backslash \bigoplus \{z_i = z_j\} \to \mathbb{C}^n \backslash \bigoplus \{z_i = z_j\}/S^n \) with fiber \( S^n \), there is a map \( B_n \to S_n \) which is easily seen to be surjective and with kernel \( P_n = \pi_1(\mathbb{C}^n \backslash \bigoplus \{z_i = z_j\}), \) called the group of **pure braids**.

**Prop.(2.1.6.14).** There is a group homomorphism \( B_3 \to PSL_2(\mathbb{Z}) \) that maps \( a = \sigma_1 \sigma_2 \sigma_1 \) to \( S \) and \( b = \sigma_1 \sigma_2 \) to \( T \). The kernel of this map is the group generated by \( c = a^2 = b^3 \).
7 Sylow Theory

Prop. (2.1.7.1) [Class Equation]. For a finite group $G$, if $G_x = C((x))$, then

$$|G| = |C(G)| + \sum |G|/|G_x|$$

where the summation is over non-trivial conjugate classes of $G$.

*Proof:* Consider the left action of $G$ on itself, and calculate elements. □

Cor. (2.1.7.2) [$p$-Groups are Solvable]. If $G$ is a $p$-group, then $G$ has a non-trivial center. In particular, any $p$-group is solvable.

Cor. (2.1.7.3). If $p||G|$, then $G$ has an element of order $p$.

*Proof:* Follows from Sylow theory and any $p$-group has a non-trivial center. □

Lemma (2.1.7.4). For any $p$-group $G$ acting on a finite set $X$, $|X| \equiv X^G \mod p$ (trivial).

Prop. (2.1.7.5) [Sylow Theorem]. For a finite group of order $|G| = p^k m$.

- There is a Sylow $p$-group.
- For a Sylow $p$-subgroup, any $p$-subgroup is contained in a conjugate of $P$. In particular, any two Sylow $p$-subgroups are conjugate.
- The number of Sylow $p$-groups $n_p$ satisfies: $n_p|m, n_p \equiv 1 \mod p$.

*Proof:* 1: Use induction, let $Z = C(G)$, if $p||Z|$, then $Z$ contains a cyclic group of order $p$. Choose a $p$-Sylow subgroup of $G/C$, then its inverse image in $G$ is a $p$-Sylow subgroup. If $Z$ is prime to $p$, consider the conjugate action of $G$ on $G - Z$, then some conjugacy class has order prime to $p$, by (2.1.7.4), then the stabilizer $H$ of this class satisfies $|G : H|$ is prime to $p$. Thus $H$ contains a $p$-Sylow subgroup by induction.

2: If $Q$ is a $p$-subgroup, then $Q$ acts on $G/P$ by left translation, so it has a fixed element by (2.1.7.4), $QxP = xP$ for some $x$, thus $Q \subseteq xPx^{-1}$.

3: $n_p|m$ by considering the conjugate action of $P$ on the set of conjugates of $P$, then as in the proof of item 2, $P$ is the only fixed element, so $n_p \equiv 1 \mod p$ by (2.1.7.4). □

Lemma (2.1.7.6). If $G$ has a sylow subgroup $H$ that $|G/H|!$ is not divisible by $|G|$, then $G$ is not simple.

*Proof:* Consider the conjugate action of $G$ on the conjugacy classes of $H$, then it is a group homomorphism of $G$ into a subgroup of $S_{|G/H|}$, but the hypothesis shows that it is not injective, thus the kernel is non-trivial normal. □

Prop. (2.1.7.7) [Frattini Argument]. If $G$ is a finite subgroup, $N$ is normal in $G$ and $P$ is a Sylow subgroup of $N$, then $NN_G(P) = G$.

*Proof:* For any element $g \in G$, consider $g^{-1}Pg \subset N$ is a Sylow subgroup of $N$, thus by Sylow theorem (2.1.7.5), there is a $n \in N$ that $g^{-1}Pg = n^{-1}Pn$, thus $gn^{-1} \in N_G(P)$, thus $g \in NN_G(P)$. □

8 Split Extension

Prop. (2.1.8.1) [Cyclic Central Extension Split]. If there is an exact sequence $0 \to \mathbb{Z} \to G \to C \to 0$ where $\mathbb{Z} \subset C(G)$ and $C$ is cyclic, then $G$ is Abelian.

Proof: This is because we can choose an inverse image of a generator of $C$. □

Prop. (2.1.8.2) [Schur-Zassenhaus]. An exact sequence of finite groups $0 \to A \to E \to G \to 0$ must split when $|A|$ and $|G|$ are relatively prime.

Proof: □

Prop. (2.1.8.3). Let $\alpha, \beta : G \to \text{Aut}(H)$ be two actions of $G$ on $H$, then theirs semiproduct sequences

$$1 \to H \to G \rtimes H \to G \to 1$$

are isomorphic iff $\alpha, \beta$ are equivalent modulo $\text{Inn}(H)$.

9 Subnormality

Def. (2.1.9.1) [Normal Series]. A subnormal series of a group $G$ is a descending chain of groups:

$$G = G_0 \triangleright G_1 \triangleright \ldots \triangleright G_r = \{e\}$$

that $G_{k+1}$ is normal in $G_k$. It is called a composite series iff each $G_k/G_{k+1}$ is simple.

Lemma (2.1.9.2) [Butterfly Lemma]. Let $H_1, H_2$ be subgroups of a group $G$, $N_1, N_2$ are normal subgroups of $H_1$ and $H_2$, then there is a canonical isomorphism of groups:

$$N_1(H_1 \cap H_2)/N_1(H_1 \cap N_2) \cong N_2(H_2 \cap H_1)/N_2(H_2 \cap N_1).$$


Prop. (2.1.9.3) [Schreier]. Any two subnormal series of a group $G$ have a common refinement.

Proof: □

Cor. (2.1.9.4) [Jordan-Hölder]. For any two composition series $G = G_0 \triangleright G_1 \triangleright \ldots \triangleright G_r = \{e\}$, $G = G'_0 \triangleright G'_1 \triangleright \ldots \triangleright G'_{r'} = \{e\}$, there $r = r'$, and there exists a permutation $\sigma \in S_{r-1}$ s.t. $G_i/G_{i+1} \cong G'_{\sigma(i)}/G'_{\sigma(i)+1}$.

Def. (2.1.9.5) [Central Series]. A central series of a group $G$ is an ascending chain of groups:

$$\{e\} = Z_0 < G_1 < \ldots < G_r = G$$

that $Z_{k+1}/Z_k$ is in the center of $G/Z_k$.

Prop. (2.1.9.6). A group is

- solvable iff it has a normal series that $G_i/G_{i+1}$ is Abelian.
- nilpotent iff it has an upper central series.

Proof: □
Def. (2.1.9.7) [Supersolvable Groups]. A group $G$ is called a **supersolvable group** iff it has a normal series that $G_i/G_{i+1}$ is cyclic.

If $G$ is finite, this notion is equivalent to solvable.

**Lemma (2.1.9.8) [p-Group is Nilpotent].** Any $p$-group is nilpotent.

**Proof:** Using induction by (2.1.7.2), we see it has a central series, thus nilpotent (2.1.9.6). □

**Prop. (2.1.9.9) [Nilpotent Finite Groups].** If $G$ is a finite group, then the following are equivalent:

- $G$ is nilpotent.
- $N_G(H) > H$ for every proper subgroup $H < G$.
- Every maximal subgroup of $G$ is normal.
- Every Sylow subgroup of $G$ is normal.
- $G$ is a direct product of its non-trivial Sylow subgroups.

**Proof:**

1 $\rightarrow$ 2: Choose a central series $Z_n$, let $Z_n \subset H$ and $Z_{n+1} \not\subset H$, then $[Z_{n+1}, H] \subset [Z_{n+1}, G] \subset Z_{n+1} \subset H$, thus $Z_{n+1} \subset N_G(H)$.

2 $\rightarrow$ 3, 4 $\rightarrow$ 5: trivial.

3 $\rightarrow$ 4 For any $p$-Sylow subgroup $G$, if $N_G(P)$ is proper subgroup, then it is contained in some maximal subgroup $M$, and $M$ is normal, thus by Frattini argument (2.1.7.7), $G = N_G(P)M = M$, contradiction.

5 $\rightarrow$ 1: By lemma (2.1.9.8). □

**Prop. (2.1.9.10) [Jordan-Horder].** For a finite group $G$, any two of its composite series has the same length, then the quotient groups $G_k/G_{k+1}$ are in bijection with each other as sets.

**Proof:** Cf. [代数学引论 P89]. □

**Prop. (2.1.9.11) [Minimal Normal Subgroup].** The minimal normal subgroup $N$ of a finite group $G$ is a direct product of simple groups $L^n$.

**Proof:** Let $N_1$ be a maximal normal subgroup of $N$, then $N/N_1$ is simple, and let $N_i$ be the conjugates of $N_1$ in $G$, then they are all maximal normal subgroup of $N$. the simple groups $N/N_i$ are mutually isomorphic, and $\cap N_i = 1$ by the minimality of $N$.

Now we use induction to prove $N/N_1 \cap \ldots \cap N_i$ is isomorphic to a product of $N/N_1$, which will finish the proof.

Now assume $N_1 \cap \ldots \cap N_{i-1} \not\subset N_i$, then $(N_1 \cap \ldots \cap N_{i-1})N_i = N$, and notice

$N/N_1 \cap \ldots \cap N_i \cong N_1 \cap \ldots \cap N_{i-1}/N_1 \cap \ldots \cap N_i \cong N_1 \times N_i \times N_1 \cap \ldots \cap N_i \cong N/N_1 \times N/N_1 \cap \ldots \cap N_i.$

□

**Prop. (2.1.9.12).** If a finite group $|G| = \prod p_i$, where $p_i$ are different primes that $\prod p_i$ and $\prod (p_i - 1)$ are coprime, then $G$ is cyclic.

**Proof:** We prove all the Sylow groups are normal. Choose the maximal Sylow group $A_n$, then it is normal by Sylow theorem, and other Sylow groups act by conjugation is trivial (consider the center (2.1.7.2), then the center of the quotient, and so on), hence $A_n$ is in the center. Now consider the quotient, by induction it is cyclic, hence this is a central extension of a cyclic group, hence $G$ is Abelian (2.1.8.1), so cyclic. □
Prop. (2.1.9.13). If $G$ is a finite group and $p$ is the minimal prime number of $|G|$, then all subgroups $N$ of $G$ of index $p$ is normal.

Proof: Consider the left action of $G$ on $G/H$, then the kernel is $\cap a^{-1}Ha$, which is the maximal normal subgroup contained in $H$. Now this is group homomorphism of $G$ into $S_p$, thus it has kernel at lest $|G|/p$, so the kernel equals $H$, showing $H$ is normal. □

Prop. (2.1.9.14) [Burnside’s Theorem]. If $p, q$ are primes, then any finite groups of order $p^aq^b$ is solvable.

Proof: Cf. [Serre Linear representations of finite groups, P65]. □

Prop. (2.1.9.15) [Thompson]. A finite group is not solvable iff there exist non-trivial elements $x, y, z$ of coprime orders $a, b, c$ that $xy = z$.

Prop. (2.1.9.16) [Feit-Thompson]. All finite groups that has odd order is solvable.

Proof: □

10 Commutators

Def. (2.1.10.1) [Notation].
- $[a, b] = a^{-1}b^{-1}ab$.
- $x^y = y^{-1}xy$.

Prop. (2.1.10.2) [Commutator relations].

Def. (2.1.10.3) [Metabelian Groups]. A metabelian group is a group $G$ that $G'$ is Abelian.

Prop. (2.1.10.4). If $G = AB$ where $A, B$ are Abelian, then $[G, G] = [A, B]$ and $G$ is metabelian.

Proof: The first one is easy to verify, the second because if we let $b^{a_1} = a_2b_2$, $a^{b_1} = b_3a_3$, then

$[a, b]^{a_1b_1} = [a, b^{a_1}]^{b_1} = [a, b]^{b_1} = [a^{b_1}, b_2] = [a_3, b_2]$

and similarly, $[a, b]^{b_1a_1} = [a_3, b_2]$, so we have $[a, b]$ commutes with $[b_1^{-1}, a_1^{-1}]$, which shows $[A, B]$ is Abelian. □

Prop. (2.1.10.5). If $G$ is a metabelian finite group, then the transfer of $Ver: G \rightarrow G'$ is trivial map.
13 Classification of Finite Groups

Thm.(2.1.13.1)[Classification of Finite Simple Groups]. Every finite simple group is one of the following:

- $\mathbb{Z}/(p)$.
- $A_n$.
- 16 infinite family of finite groups of Lie type.
- 26 exceptional groups, called sporadic simple groups.

Proof: A full list is in https://brauer.maths.qmul.ac.uk/Atlas/v3/? □

Prop.(2.1.13.2)[Monster Group]. The largest sporadic simple group is called the Monster group $M$.

$$\#M = 2^{46} \cdot 3^{20} \cdot 5^9 \cdot 7^6 \cdot 11^2 \cdot 13^3 \cdot 17 \cdot 19 \cdot 23 \cdot 29 \cdot 31 \cdot 41 \cdot 47 \cdot 59 \cdot 71.$$  □

Prop.(2.1.13.3)[Happy Family]. There are 20 sporadic groups appearing as a subquotient of $M$, and they form a set called the happy family. The remaining 6 groups are known as the pariah groups, including the Lyons group, Janko groups $J_1, J_3, J_4$, Rudvalis group and the O’Nan group $ON$.

Prop.(2.1.13.4)[Baby Monster Group]. The second largest sporadic simple group is called the baby Monster group $B$.

Def.(2.1.13.5)[O’Nan Group].

Prop.(2.1.13.6). The O’Nan group has size

$$\#ON = 2^9 \cdot 3^4 \cdot 5 \cdot 7^3 \cdot 11 \cdot 19 \cdot 31.$$  □

Prop.(2.1.13.7)[Classification of Small Groups].

1. A group $G$ of prime order $p$ or order $p^2$ is Abelian.
2. A group $G$ of order $p^a q^b$ that it has $q^b$ $p$-Sylow subgroups, then its $q$-Sylow subgroup is normal thus it is not simple.
3. A non-Abelian group $G$ of order 6 is isomorphic to $S_3$.
4. Any non-Abelian group of order 8 is isomorphic to $D_4$ or quadratic numbers $Q$.
5. A group of order smaller than 60 is solvable.
6. Any simple group $G$ of order 60 is isomorphic to $A_5$.
7. A group of order 148 is not simple, by (2.1.7.6) applied to the 37-Sylow subgroup.
8. A group of order 150 is not simple, by (2.1.7.6) applied to the 5-Sylow subgroup.

Proof:  
1. Because $G$ has non-trivial center $Z$ by (2.1.7.2), if $Z = G$, then it is Abelian, otherwise the $|Z| = p$, and the quotient $G/Z$ is cyclic, thus $G$ is Abelian by (2.1.8.1).
2. Calculating elements.

3. Consider its normal 3-Sylow group, then the quotient is cyclic thus $G$ is semi-product which must by $S_3$ when non-Abelian.

4.

5.

6. Consider $G$ has 6 5-Sylow groups, thus there are 24 elements of order 5.
$G$ has 4 or 10 3-Sylow subgroups, if it have 4 3-Sylow subgroups, then the normalizer contains a 5-Sylow subgroup, so we have a subgroup of order 15, which must by $\mathbb{Z}/15$, so it contains a normal 5-Sylow subgroup, which shows there are at most $60/15 = 4$ 5-Sylow subgroups, contradiction.
So we have 10 3-Sylow subgroups, which shows there are at most 15 elements of order 2 or 4. So we have 3 or 5 2-Sylow subgroups. If it is 3, then we can do the same as that for 3-Sylow to construct a 20-order group and reach contradiction.
So now it have 5 2-Sylow subgroups, and then we consider the conjugate action on Sylow subgroups, which is transitive, so it has trivial kernel, and $G \hookrightarrow S_5$. Now $G = [G, G] \subset [S_5, S_5] = A_5$.

Prop.(2.1.13.8). There is a group that is group that $a^3 = 1$ for any $a \in G$, but is not Abelian. It is the uni-upper-triangular matrices in $M_3(\mathbb{F}_3)$.

14 Profinite Groups

Basic references are [Neukirch Cohomology of Number Fields], [Serre Galois Cohomology] [Profinite Groups Zalesskii] and [Shatz Profinite Groups, Arithmetic and Geometry].

Def.(2.1.14.1) [Profinite Groups]. A profinite group is a topological group that is an inverse limit of finite discrete groups.

Lemma(2.1.14.2). For a compact totally disconnected group $G$, any nbhd $U$ of $e$ contains a normal open subgroup.

Proof: $U$ contains a precompact nbhd of $e$, then by(3.8.1.24), $U$ contains an open subgroup $V$, so by(3.8.1.6), there is a nbhd $V'$ of $e$ that $xV'x^{-1} \subset V$ for all $x \in G$, this says $\bigcap x^{-1}Vx$ is open, so it is an open normal subgroup.

Prop.(2.1.14.3)[Profinite Compact and Totally Disconnected]. A profinite group is the same thing as a totally disconnected, compact Hausdorff topological group. In particular, $G \cong \varprojlim G/U$ where $U$ runs over all open normal subgroups of $G$.

Proof: One way is because $\lim G_i$ is a closed subgroup of $\prod G_i$ which by Tychonoff’s theorem is compact.

Conversely, by(2.1.14.2), $G$ has a basis of $e$ consisting of normal open subgroups, and by(3.8.1.23), the intersection of open normal subgroups is $\{e\}$. For any open normal subgroup $N$ of $G$, $G/N$ is compact discrete hence finite, the map $G \rightarrow \varprojlim G/N$ is continuous and has dense image, but $G$ is compact and the right is Hausdorff, so the image is closed, hence it is surjective. It is injective because $\cap N = \{e\}$. Hence $G \cong \varprojlim G/N$. □
Cor. (2.1.14.4). A closed subgroup of a profinite group is profinite, and a quotient group is profinite.

A direct product of profinite groups are profinite, and so the inverse limit profinite groups are profinite, as it is a closed subgroup of a direct product.

Proof: The closed subgroup is totally disconnected by (3.6.1.26).

To show the quotient group is totally disconnected, by (3.8.1.23), it suffice to prove $H$ is intersection of compact open nbhds in $G/H$. If $x \notin H$, then there is an open subgroup $U$ disjoint from $xH$ by (3.8.1.7), so it is closed hence compact. So $UH$ is a compact nbhd of $H$ in $G/H$ that doesn’t contains $xH$, hence the result. □

Cor. (2.1.14.5). A closed subgroup of a profinite group is a intersection of open normal subgroups of $G$ containing it, as $G/H$ is profinite and as in the proof of (2.1.14.3), $H$ is the intersection of open normal subgroups of $G/H$.

Prop. (2.1.14.6). For $G \in \text{Prof}$, if $U_\alpha$ is the system of open normal subgroups of $G$, and $H$ is a closed subgroup of $G$, then there is a natural isomorphism of topological groups

$$H \cong \lim_{\leftarrow} H/H \cap U_\alpha,$$

and if $H$ is normal, then there is a natural isomorphism of topological groups

$$G/H \cong \lim_{\leftarrow} G/HU_\alpha.$$


Prop. (2.1.14.7). Any infinite profinite groups is uncountable.

Proof: [Profinite Groups Zalesskii] Prop2.3.1. □

Prop. (2.1.14.8). The category of profinite Abelian groups is Pontryagin dual to the category of torsion abelian group. (not that hard to verify).

Proof: □

Pro-$p$-Groups

Def. (2.1.14.9) [Surnatural Number]. To consider indexes of closed subgroups of a profinite group, the notion of surnatural numbers are needed. A surnatural number is a formal product $\prod_p p^{n_p}$, $n_p \in \mathbb{N} \cup \{0, \infty\}$.

For a closed subgroup $H$ of a profinite group $G$, $[G : H]$ is defined to be the least common multiple of $[G/U : H/H \cap U]$ where $U$ goes over all open normal subgroups of $G$. This also equals the least common multiple of $[G : V]$ for $V$ open containing $H$ (because for any such $V$, there is an open normal subgroup $U$ that $HU \subset V$ (3.8.1.6)).


Proof: $[G/U : K/K \cap U] = [G/U : H/H \cap U][H/H \cap U : K/K \cap U][G : H][H : K]$, giving one way of inequality. For the converse, Cf.[Etale Cohomology Fulei P150]. The quotient case is trivial. If $[G : H]$ is finite, then For the final assertion, notice for a open subgroup $V$, $G - V$ is compact, so $H_i \subset V$ if $\cap H_i \subset V$ for some $i$.\hfill\Box

Def. (2.1.14.11) [Pro-$p$-Group]. A profinite group $G$ is called a pro-$p$-group iff $[G : 1]$ is a power of $p$.

Given a profinite group, a closed subgroup $H$ is called Sylow pro-$p$-subgroup of $G$ if $H$ is pro-$p$ and $[G : H]$ is prime to $p$.\hfill\Box

Prop. (2.1.14.12). A profinite group $G$ is a pro-$p$-group iff it is an inverse limit of finite $p$-groups. In particular, any finite quotient of a pro-$p$-group is a $p$-group.\hfill\Box

Prop. (2.1.14.13) [Sylow Pro-$p$-Group Exists].\hfill\Box

Prop. (2.1.14.14). Any pro-$p$ subgroup $H$ of $G$ is contained in a Sylow $p$-subgroup of $G$, and any two Sylow $p$-subgroups are conjugate. And a surjective morphism of profinite groups maps a pro-$p$ group to a pro-$p$ group.\hfill\Box

Prop. (2.1.14.15). For a pro-$p$ group $G$, any nonzero simple $p$-torsion $G$-module is isomorphic to $\mathbb{Z}/p\mathbb{Z}$ with trivial $G$-action.\hfill\Box
2.2 Abstract Algebra

References are [Lan05], [Rom07] and [Finite Groups Issac].

This section differs from sections on Commutative Algebras because it contains more basic, but maybe non-commutative properties. This section differs from sections on Group Theory because it concerns objects with more structure than a group.

Notations (2.2.0.1).
- Use notations defined in Group Theory.

1 Rings

Basics

Def. (2.2.1.1) [Rings]. A ring is an Abelian group \((R, +)\) together with a multiplication map 
\[ \times : R \times R \to R \]
s.t.
- \((R, \times)\) is a monoid.
- For any \(x, y, z \in R\),
  \[ x(y + z) = xy + xz, \quad z(x + y) = zx + zy \]

A commutative ring is a ring that the multiplication is commutative. The category of rings is denoted by \(\mathcal{R}\)ing, the category of commutative rings is denoted by \(\mathcal{C}\)Ring.

Def. (2.2.1.2). \(R \in \mathcal{R}\)ing is called
- a simple ring if it has no non-trivial two-sided ideals.
- a domain or an integral ring if whenever \(ab = 0\), \(a = 0\) or \(b = 0\).
- reduced if it has no non-zero nilpotent element.
- Dedekind-finite if for any \(a, b \in R\), \(ab = 1 \Rightarrow ba = 1\).

Def. (2.2.1.3) [Fields]. A field is a commutative ring that every non-zero element has an inverse. The category of fields is denoted by \(\mathcal{F}\)ield.

Prop. (2.2.1.4) [Characteristic]. For \(R \neq 0 \in \mathcal{R}\)ing, there exists at most one \(p \in \mathbb{P}\) s.t. \(p \cdot 1 = 0 \in k\).
If such a \(p\) exists, denote char \(k = p\), otherwise denote char \(k = 0\).

Prop. (2.2.1.5). If \(1 - ab\) is left(right) invertible in a unital ring \(R\), then so is \(1 - ba\), and
\[ (1 - ba)^{-1} = 1 + b(1 - ab)^{-1}a. \]

Proof: Direct Calculation. \(\square\)

Prop. (2.2.1.6) [Kaplansky]. If \(a\) has a right inverse by no left inverse in a ring, then \(a\) has infinitely many right inverses.

Proof: If \(ab = 1\), then in fact \(b + (1 - ba)a^n\) are right inverses for \(a\) for any \(n \geq 0\), and they are distinct, because if \(b + (1 - ba)a^n = b + (1 - ba)a^m\), then \((1 - ba)a^n = (1 - ba)a^m\). And by multiplying \(b\) on the right, we get \((1 - ba)a^{n - m} = 1 - ba\), so \((1 - ba)a^{n - m - 1} + b)a = 1. \(\square\)
2.2. ABSTRACT ALGEBRA

Division Rings

Def. (2.2.1.7)[Division Rings]. A skew field (or division ring) is a unital ring that every non-zero element is invertible (but may not be commutative).

Prop. (2.2.1.8)[Wedderburn]. A finite division ring $D$ is a field.

Proof: Use the class equation for the invertible elements of $D$, if it is not isomorphic, consider the center $Z(D)$ of $D$, let $|Z(D)| = z$, then it is a field, and any other centralizer can be seen as a vector space over $Z(D)$, let it of dimension $k$, then $z^n - 1 = z - 1 + \sum \frac{z^n - 1}{z_k - 1}$. But then let $\Psi_n$ be the cyclotomic polynomial of degree $n$, then $\Psi_n(z)$ divides $z - 1$. But this is not true, as it is bigger. □

Prop. (2.2.1.9). If $D$ is a f.d. division algebra over $\mathbb{R}$, then it is isomorphic to $\mathbb{R}$, $\mathbb{C}$ or $\mathbb{H}$.

Proof: Cf. [Advanced Linear Algebra P466]. □

Prop. (2.2.1.10). Let $k \in \text{Field}, k = \mathbb{F}$, then any division ring $A$ over $k$ with dimension $< \#k$ is isomorphic to $k$.

In particular, a division ring $A$ of at most countable dimension over $\mathbb{C}$ is isomorphic to $\mathbb{C}$.

Proof: Notice it suffices to find an eigenvalue of $\varphi: A \to A$ for each $\varphi \in A$. But $\{(\varphi - a)^{-1}\}$ is a uncountable set of elements of $A$, so some $\sum a_i(\varphi - c_i)^{-1} = 0$, spanning the expression, we see $\prod_k(\varphi - \mu_k) = 0$, so some $\varphi - \mu_k = 0$, contradiction. □

Prop. (2.2.1.11)[Hua Equation]. In a division ring $D$, if $a, b \neq 0$ and $ab \neq 1$, then

$$a - (a^{-1} + (b^{-1} - a)^{-1})^{-1} = aba$$

Proof: suffices to show

$$1 = (1 - ab)a(a^{-1} + (b^{-1} - a)^{-1}) = (1 - ab)(1 + a(b^{-1} - a)^{-1}).$$

But this is equal to

$$(1 - ab)(1 - (b^{-1} - a)(b^{-1} - a)^{-1} + b^{-1}(b^{-1} - a)^{-1}) = (1 - ab)(1 - ab)^{-1} = 1.$$ □

Others

Prop. (2.2.1.12). If $R \in \text{Ring}, \#R = p^2$, then $R$ is commutative.

Proof: Consider the center of $R$, it is non-trivial because □

Prop. (2.2.1.13). Let $A, A'$ be $k$-algebras and $B, B'$ subalgebras of $A, A'$ with centralizers $C, C'$, then the centralizer of $B \otimes_k B' \subset A \otimes_k A'$ is $C \otimes_k C'$.

Proof: It suffices to show that $C \otimes_k A' \cap A \otimes_k C' = C \otimes_k C'$, which is clear because they are flat over $k$. □
2 Polynomials

**Prop.(2.2.2.1) [Descartes’s Rule of Sign]**. Let \( p(x) = a_0 x^b_0 + a_1 x^b_1 + \cdots + a_n x^b_n \) be a real polynomial with nonzero \( a_i \), where \( A_0 < B_1 < \cdots < b_n \), then the number of positive roots of \( p(x) \) has the same parity with the number of consecutive changes of signs of \( (a_k)_{k=0,\ldots,n} \).

**Proof**: Lemma: when \( a_0 a_n > 0 \), the number of positive roots are even and when \( a_0 a_n < 0 \), it is odd. This is seen by consider \( p(0) \) and \( p(\infty) \).

Then we consider the derivative \( p' \) and use induction. Denote the number of changing sign by \( v(p) \) and the number of positive roots by \( z(p) \), then if \( z_0 a_1 > 0 \), then \( v(p) = v(p') \) and \( z(p) = \equiv z(p') \mod 2 \).

Then we have \( z(p) = v(p) \mod 2 \) and middle value theorem shows that \( z(p') \leq z(p) - 1 \), hence by induction and parity argument, we have \( v(p) \geq z(p) \).

If \( a_0 a_1 < 0 \), then the same method shows that \( v(p) = v(p') + 1 \geq z(p') + 1 \geq z(p') \) and the have the same parity by the lemma.

**□**

**Cor.(2.2.2.3)**. If \( f(x) = a_n x^n + \cdots + a_0 \), then for any \( n + 1 \) different integers \( a_0, \ldots, a_n \), there exists some \( |f(a_i)| \geq \frac{n!}{2^n}|a_n| \).

**Proof**: Use Lagrange interpolation and consider the leading coefficient.

**□**

**Prop.(2.2.2.4)**. If a degree \( n \) polynomial \( p \) satisfies \( p(n) = 2^n \) for \( n = 0, 1, \ldots, n \), then \( p(n+1) = 2^{n+1} - 1 \).

**Proof**: The polynomial in search is \( p(x) = \sum_{k=0}^{n} \binom{n}{k} \).

**□**

**Prop.(2.2.2.5) [Combinatorial Nullstellensatz]**. If \( F \) is a field, \( a_i \) are \( n + 1 \) elements of \( K \), \( b_i \) are \( n + 1 \) elements of \( K \), then there is a unique polynomial \( f \) of degree no greater than \( n \) that \( f(a_i) = b_i \).

**Proof**: The polynomial in search is \( f(x) = \sum \prod_{j \neq i} b_j - a_j \).

It is a polynomial of degree smaller than \( n + 1 \), and it satisfies the hypothesis. And clearly there is at most one such polynomial, otherwise their difference has \( n + 1 \) zeros.

**□**

**Cor.(2.2.2.6) [Combinatorial Nullstellensatz]**. If \( F \) is a field and \( f \in F[X_1, \ldots, X_n] \) is a polynomial. Let \( S_1, \ldots, S_n \) be nonempty finite subsets of \( F \) and \( g_i = \prod_{s \in S_i} (x_i - s) \), then if \( f \) vanishes at the common zeros of \( g_i \), then there are polynomials \( h_i \in F[X_1, \ldots, X_n] \) that \( \deg h_i \leq \deg F - \deg g_i \) and \( g = \sum g \).

**Proof**: The proof is very simple, just replace terms of \( f \) by lower degree terms, using equation of \( g_i \), then we get a polynomial that has degree in \( x_i \) smaller than \( |S_i| \) and vanish on \( S_1 \times \ldots \times S_n \), so it must be 0, as easily checked.

**□**

**Remark (2.2.2.7)**. For many combinatorial applications of the combinatorial nullstellensatz, Cf.[Combinatorial Nullstellensatz].
Irreducibility

**Prop. (2.2.2.8).** If \( f = a_n x^n + \ldots + a_1 x + p \in \mathbb{Z}[X] \) satisfies \( p \) is a prime and \( \sum |a_i| < p \), then \( f \) is irreducible in \( p \).

**Proof:** The ideal is that all of its roots has norm bigger than 1, because otherwise \( p = |\sum a_k x^k| \leq \sum |a_k| < p \), contradiction. So if now \( f = gh \), then \( g, h \) all have roots with norm greater than 1, in particular it has constant coefficients norm greater than 1, which is a contradiction because \( p \) is a prime. \( \square \)

**Prop. (2.2.2.9).** The cyclotomic polynomial \( \Psi_n(x) \) is irreducible over \( \mathbb{Z} \).

**Proof:** It suffices to show that for any irreducible factor \( f \mid \Psi_n(x) \), if \( \xi \) is a root of \( f \) and \( (p, n) = 1 \), then \( \xi^p \) is also a root of \( f \). Cf.[Lan05]. \( \square \)

Diophantine Equations

**Prop. (2.2.2.10) [Fermat’s Equation in Function Case].** If \( n \geq 2 \), then the only non-trivial solution to the equation in \( \mathbb{C}[t] \) of

\[
X^n + Y^n = Z^n
\]

is \( n = 2, X = (a^2 - b^2)/2, Y = ab, Z = (a^2 + b^2)/2 \).

**Proof:** The \( n = 2 \) case is easy. If \( n > 2 \), we show there are no non-trivial solutions: Differentiate it to get:

\[
X^{n-1}X' + Y^{n-1}Y' = Z^{n-1}Z',
\]

And cancelling \( X^{n-1} \), we get

\[
Y^{n-1}(X'Y - Y'X) = Z^{n-1}(X'Z - Z'X).
\]

Now \( X'Z - Z'X \neq 0 \) because \( X, Z \) are not linearly equivalent, and \( Y, Z \) is coprime, so \( Y^{n-1}|X'Z - Z'X \). But then if we assume \( \dim Y \geq \dim X \), then \( (n-1) \dim Y \leq 2 \dim Y - 1 \), which means \( n < 2 \). \( \square \)

**Resultants**

**Def. (2.2.2.11)[Resultants].** Over a commutative ring \( R \), the **resultant** \( \text{res}(A, B) \) of two polynomials \( A, B \) of degree \( d, e \) respectively is the determinant of the linear map

\[
W_e \times W_d \to W_{d+e} : (X, Y) \mapsto AX + BY,
\]

where \( W_t \) is the free module of polynomials of degree \( < t \).

**Prop. (2.2.2.12).** The resultant can be seen as the determinant of the matrix with values the coefficient of \( A \) or \( B \) in different places, multiplying \( X^s \)s with different degree and add to the last row, we can get \( A \cdot X^s \)s and \( B \cdot X^s \)s, so: \( \text{res}(A, B) = AC + BD \) for some \( C, D \).

Now if \( R \subset S \) and \( A, B \) has common roots in \( S \), then \( \text{res}(A, B) = 0 \).

**Cor. (2.2.2.13).** Resultant is stable under Euclidean division, so it can be seen as a suitable division remainder of the two polynomial.
Prop. (2.2.2.14). When $R \subset L$ a field and $A, B$ decompose into linear factors in $L$, let $t_i$ be roots of $A$ and $u_j$ be roots of $B$, then

\[
\text{res}(A, B) = v_0^d w_0^e \prod_{i=1}^{d} \prod_{j=0}^{e} (t_i - u_j)
\]

Proof: See the resultant as polynomials of the roots of $A$ and $B$, then we proved that if they has the same root, then $\text{res} = 0$, so it is divisible by $(t_i - u_j)$ for all $i, j$. Then notice the RHS is homogenous of degree $d$ in $u_j$ and homogenous of degree $e$ in $t_i$, so does res. So they are equal. □

Invariant Theory

Prop. (2.2.2.15) [Elementary Symmetric Polynomial]. For $n$ indeterminants $x_i$, define the elementary polynomials

\[
\sigma_k = \sum_{1 \leq i_1 < \ldots < i_k \leq n} x_{i_1} x_{i_2} \ldots x_{i_k} \in \mathbb{Z}[x_1, \ldots, x_n]
\]

where for $k > n$ this expression means 0. Then any symmetric polynomial is a polynomial of the fundamental symmetric polynomials.

Proof: Set the first coordinate to 0, then the rest is a polynomial of the fundamental symmetric polynomials by induction, $f(0, x) = h(\sigma_1, \ldots, \sigma_n)$, then consider $f - h$, with $h$ the same expression but $x_n$ is included, we get it is a symmetric polynomial, and it is divisible by $x_1$, thus also divisible by $\prod x_i$, thus divide it by $\prod x_i$ and use induction, we get $f$ is a polynomial of elementary symmetric polynomials. □

Prop. (2.2.2.16) [Newton Identities]. For $n$ indeterminants $x_i$, define

\[
s_k = \begin{cases} 
\sum x_i^k, & k \geq 0 \\
0, & k < 0
\end{cases} \in \mathbb{Z}[x_1, \ldots, x_n],
\]

then there are Newton Identities:

\[
s_k - \sigma_1 s_{k-1} + \ldots + (-1)^n \sigma_n s_{k-n} = 0.
\]

Proof: The case of $k \geq n$ is simple. Now if $k < n$, then we prove by induction on $n$: If $n$ is already proven, then the term is 0 if one of them is 0, but this implies that this equation is divisible by $\prod_{i=1}^{k+1} x_i$, but is has degree $k \leq n$, so it must by 0. □

Prop. (2.2.2.17) [Chern Polynomials]. By (2.2.2.16) and induction there are polynomials $P_k \in \mathbb{Z}[x_1, \ldots, x_k]$ s.t. $P_k(\sigma_1, \ldots, \sigma_k) = s_k, k \geq 0$, called the Chern polynomials. Then they satisfy:

\[
\log(1 + c_1 + c_2 + \ldots + c_n + \ldots) = \sum_{p \geq 1} (-1)^{p-1} \frac{pP_p}{p} \in \mathbb{Q}[c_1, \ldots, c_n, \ldots]
\]

In particular, we can easily calculate via homogeneity that

\[
P_1 = c_1, \quad P_2 = c_1^2 - 2c_2, \quad P_3 = c_1^3 - 3c_1c_2 + 3c_3, \quad P_4 = c_1^4 - 4c_1^2c_2 + 4c_1c_3 + 2c_2^2 - 4c_4.
\]
Proof: We can define elementary power series
\[ \sigma_k = \sum_{1 \leq i_1 < \cdots < i_k} x_{i_1} x_{i_2} \cdots x_{i_k} \in \mathbb{Z}[[x_1, \ldots, x_n, \ldots]], \]
and also
\[ s_k = \begin{cases} \sum x_i^k, & k \geq 0 \\ 0, & k < 0 \end{cases} \in \mathbb{Z}[[x_1, \ldots, x_n, \ldots]]. \]
Then the Newton identities also holds by taking limits. There is an injection
\[ Q[[c_1, \ldots, c_n, \ldots]] \rightarrow Q[[x_1, \ldots, x_n, \ldots]] : c_i \mapsto \sigma_i, \]
and the LHS is mapped to
\[ \log \left( \prod_i (1 + x_i) \right) = \prod_i \log (1 + x_i) = \sum_{p \geq 1} (-1)^p \frac{s_p}{p} \]
is the image of the RHS. \( \square \)

Prop. (2.2.2.18)[Todd Polynomials]. There are Todd polynomials \( Q_p \in \mathbb{Z}[\sigma_1, \ldots, \sigma_p], p \geq 1 \) s.t.
\[ \text{Todd}(x_1, \ldots, x_n, \ldots) = \prod_{i=1}^{n} \frac{x_i}{1 - e^{-x_i}} = 1 + \sum_{p \geq 1} \frac{Q_p}{p!} \in \mathbb{Q}[[x_1, x_2, \ldots]] \]
for any \( n \in \mathbb{Z}_+, \) and
\[ Q_1 = c_1, \quad Q_2 = c_1^2 + c_2, \quad Q_3 = c_1 c_2, \quad Q_4 = -c_1^4 + 4 c_1^2 c_2 + 3 c_2^2 + c - 1 c_3 - c_4. \]

Proof: \( ? \) \( \square \)

Prop. (2.2.2.19)[Conjugate Invariant Polynomials]. Any polynomial on the entries of matrixes \( M_n(k) \) that is invariant under conjugation is generated by coefficients of \( \det(\lambda I + X) \) and can also be generated by \( \text{tr}(X^k) \).

Proof: We notice that the matrixes having disjoint eigenvalues is dense in \( M_n(k) \), thus the restriction of the polynomial on these matrixes is a symmetric polynomial(2.2.2.15) thus identical to a polynomial described above. Hence they are equal. \( \square \)

Prop. (2.2.2.20). For any polynomial on the entries of matrixes \( M_n(k) \) that \( f(BA) = f(A) \) for \( B \in O(n) \), there is a polynomial \( F \) that \( f(A) = F(A^*A) \). Cf.[Heat Equation and the Index Theorem Atiyah P323].

Prop. (2.2.2.21)[Weyl]. Any linear map \( f \) from \( (\mathbb{R}^m)^\otimes n \) to \( R \) that is \( O(m, \mathbb{R}) \)-equivariant is a linear combinations of maps of the form:
\[ v_1 \otimes v_2 \otimes \cdots \otimes v_n \mapsto \langle v_{i_1}, v_{i_2} \rangle \langle v_{i_3}, v_{i_4} \rangle \cdots \langle v_{i_{n-1}}, v_{i_n} \rangle. \]
Where \( i_1, \ldots, i_n \) is a permutation of \( 1, 2, \cdots, n \) when \( n \) is even and when \( n \) is odd, \( f \) must be 0.

Proof: Cf.[Heat Equation and the Index Theorem]. \( \square \)
3 Commutative Rings

Bézout Domain

Def. (2.2.3.1) [Bézout Domains]. A Bézout domain is an integral domain that any sum of two principal domains is also principal.

Prop. (2.2.3.2). The localization of a Bézout domain is Bézout. A local ring is Bézout iff it is a valuation ring by (10.3.2.8).

UFDs

Def. (2.2.3.3) [UFDs]. A non-zero element $x$ in a domain $R$ is called irreducible iff for any $y, z \in R$ that $x = yz$, either $y$ or $z$ is a unit.

A non-zero element $x$ in a domain $R$ is called a prime iff $(x)$ is a prime ideal. Every prime is irreducible.

A domain $R$ is called a UFD iff every non-zero element $x \in R$ has a factorization into irreducibles, unique up to units.

Prop. (2.2.3.4). if $R$ is Noetherian domain, then each element has a decomposition into irreducible.

Proof: Trace the decomposition inductively, if it doesn’t stop, then it contradicts with Noetherian hypothesis. □

Prop. (2.2.3.5). An integral domain $R$ is a UFD iff each element $x$ factors into irreducibles, and every irreducible element is a prime. Also this is equivalent to every non-zero element factors into prime elements.

Proof: If $R$ is a UFD, then if $x$ is irreducible, if $ab \in (x)$, $ab = xc$, then $x$ is one irreducible in the decomposition of $a$ and $b$, by UFD, so $a \in (x)$ or $b \in (x)$, and $(x)$ is a prime ideal.

Conversely, if there are two decompositions $\prod a_i = \prod b_j$, then some $b_j \in (a_i)$ by primeness of $(a_i)$, so $b_j = a_iu$, so $u$ must by units, so by induction, this two decompositions are the same.

If every element factors into prime elements, then an irreducible element is a prime because it factors as a product of primes, and notice every prime is irreducible (2.2.3.3). □

Prop. (2.2.3.6) [Kaplansky]. An integral domain $R$ is UFD iff every non-zero prime ideal contains a non-zero principle prime ideal. In particular, any prime of height 1 is principal.

Proof: If $R$ is a UFD, let $p$ be a non-zero prime ideal, choose $a \neq 0 \in p$, and write $a = \pi_1 \ldots \pi_n$ as a product of irreducibles. Then $\pi_i \in p$ for some $i$, so $p$ contains the prime ideal $(\pi_i)(2.2.3.5)$.

Conversely, let $S$ be the set of all finite products of prime ideals of $R$, then $S$ is a multiplicative set of $R$. For any non-zero element $a \in R$, if $(a) \cap S = \emptyset$, then there is a prime ideal $P$ containing $(a)$ and is maximal among those avoiding elements of $S$. Then $P$ contains a non-zero prime $\pi$, contradiction. So $(a) \cap S \neq \emptyset$. Let $b \in R$ that $ab = \pi_1 \ldots \pi_n$, then we show $a \in S$ by induction on $n$.

If $n = 1$, then $a$ is a unit or a prime, so we are done. For general $n$, if $\pi_k | b$ for some $k$, then $b = \pi_kc$, and $ac = \pi_1 \ldots \pi_{k-1}\pi_{k+1} \ldots \pi_n$, then $a \in S$ by induction hypothesis. Otherwise $\pi_k | a$ for all $k$, thus $a = \pi_1 \ldots \pi_n c$ and $1 = bc$, thus $c$ is a unit and $a \in S$.

Thus we proved that every non-zero element is a product of prime elements, so $R$ is a UFD by (2.2.3.5). □
Prop. (2.2.3.7). A polynomial ring over a UFD is a UFD.

Proof: □

Prop. (2.2.3.8). Let \( k \) be a field, then the power series \( k[[X_1, \ldots, X_n]] \) is a UFD.

Proof: Cf.[Algebra Lang P209]. □

Remark (2.2.3.9). WARNING: if \( A \) is a UFD, \( A[[X]] \) may not be a UFD. Cf.[Matsumura, Commutative Ring Theory, P165].

Prop. (2.2.3.10)[Gauss Lemma].

Prop. (2.2.3.11)[Nagata]. If \( A \) is a Noetherian domain and \( x \in A \) is a prime element s.t. \( A[\frac{1}{x}] \) is a UFD, then \( A \) is a UFD.

Proof: \( A[\frac{1}{x}] \) is normal by (4.3.5.2), and \( A \) is also normal: If \( a \in \text{Frac}(A) \) is integral over \( A \), then \( a = r/x^m \) for some \( m \in \mathbb{Z}, r \in A \setminus \{x\} \). If \( a \notin A \), then \( r \in x \), contradiction.

Then we can use (6.1.2.25) to show that \( \text{Cl(Spec A)} \) = 0, and then \( A \) is a UFD by (6.1.5.6). □

Prop. (2.2.3.12). For a field \( k \) of characteristic \( \neq 2 \) and \( n \geq m \geq 5 \), \( A = k[x_1, \ldots, x_n]/(-x_1^2 + x_2^2 + \ldots + x_m^2) \) is a UFD.

Proof: \( A \cong k[x_1, \ldots, x_n]/(x_1x_2 + x_3^2 + \ldots + x_m^2) \), and \( (x_2) \) is a prime ideal of \( A \) s.t. \( A[\frac{1}{x_2}] \) is a UFD by (2.2.3.7), so \( A \) is a UFD by Nagata’s lemma (2.2.3.11). □

Prop. (2.2.3.13)[Quadratic Extension of UFDs]. If \( A \in \mathbb{C}\text{Alg} \) is an integral domain and \( Z^2 - gZ + f \) doesn’t have a root in \( \text{Frac}(A) \), then \( A[Z]/(Z^2 - gZ - f) \) is integral and normal.

Proof: If \( (a + bZ)(c + dZ) = 0 \), then by hypothesis \( ad + bc + bdf = 0 \). Then \( b(fd^2 - c^2 - cdg) = 0 \), so \( b = 0 \) or \( c = d \) by hypothesis. If \( (c, d) \neq (0, 0) \), then \( ac = ad = 0 \), so \( a = b = 0 \). □

PID

Def. (2.2.3.14)[Euclidean Domain].

Prop. (2.2.3.15)[Euclidean Domain is PID]. An euclidean domain is a PID.

Proof: □

Cor. (2.2.3.16). If \( K \) is a field, then \( K[X] \) is a PID.

Prop. (2.2.3.17)[Chinese Remainder Theorem].

Prop. (2.2.3.18)[PID Structures]. In a PID,
- An element \( t \) is irreducible iff \( (t) \) is maximal.
- A PID is UFD hence Noetherian.
- An element \( t \) is irreducible iff it is a prime.

Proof: 1: By (2.2.3.6).
2: By (2.2.3.6).
3: By item 2 and (2.2.3.4). □
4 Module Theory

Def. (2.2.4.1) [Modules]. For \( R \in \mathcal{R} \), a (left)\( R \)-module is defined to be \( \mathbb{?} \). The category of \( R \)-modules is denoted by \( \mathbf{Mod}_R \).

Left modules are preferred. There are several proposition that is written in favor of right modules, they should be rectified.

Def. (2.2.4.2) [Finite Modules]. For \( R \in \mathcal{R} \), a finite \( R \)-module is an \( R \)-module \( M \) that there is a surjection \( R^n \to M \) for some \( n \geq 0 \).

Prop. (2.2.4.3). Let \( R \) be a nonzero commutative ring and \( M \) be an \( R \)-module generated by \( n - 1 \) elements, then any \( R \)-module map \( R^n \to M \) has a nonzero kernel.

Proof: Choose a surjection \( R^{n-1} \to M \), then the map \( R^n \to M \) can be extended to a map \( R^n \to R^{n-1} \). It suffices to assume \( M = R^n \). This map is represented by a matrix. If some entry \( a_{ij} = a \) is nilpotent, then we can localize \( R \) to \( \mathcal{R}_a \) that \( a \) is a unit. We can assume \( a_{11} = a \), and apply elementary row and column transformation to make \( A = \text{diag}(1, B) \), then we finish by induction. Now if all \( a_{ij} \) are nilpotent, then \( I = (a_{ij}) \) is nilpotent, and if \( m \) is the maximal integer that \( I^m \neq 0 \), then \( (I^m)^{\leq n} \) is contained in the kernel of this morphism.

Cor. (2.2.4.4) [Rank of Free Modules]. If \( M \) is a free module over a nonzero commutative ring \( R \), then any basis of \( M \) of the same cardinality, called the rank of \( M \), and any spanning subset of \( M \) has greater cardinalities. In particular, \( R^m \neq R^n \) as \( R \)-modules.

Prop. (2.2.4.5) [Fitting Lemma]. For an endomorphism \( T \) of a \( R \)-module \( M \), if we denote \( p \) the minimal integer that \( R(T^p) = R(T^{p+1}) \) and \( q \) the minimal integer that \( N(T^q) = N(T^{q+1}) \). Then the morphisms are stable afterward. Then if there is a \( m, n \) that \( R(T^m) \oplus N(T^n) = X \) for a \( R \)-module endomorphism \( T \in \text{End}(M) \), then \( p, q < \infty \) and they are equal. Moreover, if we know \( p, q < \infty \), then we have \( R(T^p) \oplus N(T^q) = M \).

Proof: We notice that

\[
T^i : N(T^{i+j})/N(T^i) \to R(T^i) \cap N(T^i), \quad T^i : M/(R(T^i) + N(T^i)) \to R(T^i)/R(T^{i+j})
\]

are isomorphisms. Thus \( R(T^m) \oplus N(T^n) = X \) shows \( q \leq m \) and \( p \leq n \), thus we have \( R(T^p) \oplus N(T^q) = M \), which implies \( p \geq q \) and \( q \geq p \). Thus the result. The rest also follows easily from these isomorphisms.

Prop. (2.2.4.6) [Nakayama]. If \( M \) is a finite \( A \)-module, and \( I \subset A \) is an ideal that \( IM = M \), then there is an \( a \in 1 + I \) that \( aM = 0 \).

In particular, if \( I \subset \text{rad}(A) \), then \( a \) is a unit (4.2.6.2), so \( M = 0 \).

Proof: Because \( M = IM \), choose a set of generators \( \{x_i\} \) of \( M \), then \( x_i = \sum a_{ij}x_j \), where \( a_{ij} \in I \). Then if the matrix \( M = (\delta_{ij} - a_{ij}) \), then \( Mx_i = 0 \). So taking the adjoint matrix, then \( \text{det}(M)x_i = 0 \). Notice \( \text{det}(M) \) is a morphism. But the determinant must be element like \( 1 + k, k \in I \), so we are done.

Cor. (2.2.4.7). If \( M \) is a finite \( A \)-module, \( N \) a submodule and \( M = \text{rad}(A)M + N \), then \( M = N \).

Cor. (2.2.4.8). If a finite \( R \)-module \( M \) satisfies \( M \otimes_R k(p) = 0 \), then there is a \( f \notin p \) that \( M_f = 0 \).
Proof: Because $M_p = 0$, and the support of $M$ is closed (finiteness used).

Cor. (2.2.4.9). If an endomorphism $\varphi$ of a finite module $M$ over $R$ is surjective, then it is injective.

Proof: This endomorphism makes $M$ a finite module over $R[X]$ by letting $X$ act by $\varphi$. So the hypothesis shows $IM = M$ where $I = (x) \subset R[x]$. Then Nakayama (2.2.4.6) shows there are some $(1 + f(X)X)M = 0$. Thus for any $m \in M$ that $X(m) = 0$, $m = 0$, so $\varphi$ is injective.

Prop. (2.2.4.10). If $A \in \text{Ring }/\mathbb{C}$ and $\alpha \in A$ is not nilpotent, then there exists a simple $A$-module $M$ that $\alpha|_M \neq 0$.

Proof: First we claim that there is some $\lambda \neq 0 \in \mathbb{C}$ that $\alpha - \lambda$ is not invertible in $A$, this is nearly the same as the proof of (2.2.1.10), noticing that $\alpha$ is not nilpotent. Now we can take $M = A/(\alpha - \lambda)A$, then $\alpha 1 = \lambda \neq 0$.

Prop. (2.2.4.11) [Jordan-Horder]. Cf. (2.1.9.10).

Tensor Module and Hom Module

Def. (2.2.4.12) [Hom Module]. If $B$ is an $R$-$S$-bimodule and $C$ is a $T$-$S$-bimodule, then $\text{Hom}_S(B, C)$ is naturally a $T-R$-module given by the action $(tfr)(b) = tf(rb)$.

Dually, if $B$ is an $S-R$-bimodule and $C$ is a $T$-$S$-bimodule, then $\text{Hom}_S(B, C)$ is naturally an $R-T$-bimodule given by the action $(rft)(b) = f(br)t$.

Def. (2.2.4.13) [Tensor Product]. Given a ring $R$, a $T-R$-bimodule $A$ and an $R$-$S$-bimodule $B$, their tensor product is a $T-S$-bimodule defined by universal properties: $A \times B \to A \otimes_R B$ is a $T$-$S$-bimodule map, and any $T$-$S$-bimodule map $A \times B \to C$ to a $T$-$S$-bimodule $C$ factors uniquely through $A \otimes_R B \to C$.

The tensor product can be constructed as:

There is an adjoint:

$$- \otimes_R B : T \text{Mod}_R \leftrightarrow T \text{Mod}_S : \text{Hom}_S(B, -) .$$

In particular, tensoring commutes with colimits.

Similarly, there is an adjoint:

$$A \otimes_R - : R \text{Mod}_S \leftrightarrow T \text{Mod}_R : \text{Hom}_T(A, -) .$$

Proof: We need to give an isomorphism

$$\tau : \text{Hom}_S(A \otimes_R B, C) \cong \text{Hom}_R(A, \text{Hom}_S(B, C)).$$

Given $f \in \text{Hom}_S(A \otimes_R B, C)$, we define

$$\tau(f) : A \to \text{Hom}_S(B, C) : (\tau(f)a)(b) = f(a \otimes b).$$

and conversely, for $g \in \text{Hom}_R(A, \text{Hom}_S(B, C))$,

$$\tau^{-1}(g)(a \otimes b) = (g(a))(b).$$

The verifications is routine and the isomorphism for left modules is dual.
Prop. (2.2.4.14)[(Co)Induced Modules]. Given a ring homomorphism $S \to R$, then $R$ is a $S - R$-bimodule as well as a $R-S$-bimodule, then we define:

- $f^* : R\text{Mod} \to S\text{Mod} : f^* M = S M = \text{Hom}_R(R, M) = R \otimes_R M$ (2.2.4.12)(2.2.4.13), the restriction.

- $f_1 : S\text{Mod} \to R\text{Mod} : f_1 M = R \otimes_S M$ is the induced module, it is left adjoint to restriction, by (2.2.4.13).

- $f_* : S\text{Mod} \to R\text{Mod} : f_* M = \text{Hom}_S(R, M)$ is the coinduced module, it is right adjoint to restriction, by (2.2.4.13).

Dually for left modules, we define:

- $f^* : \text{Mod}_R \to \text{Mod}_S : f^* M = M_S = \text{Hom}_R(R, M) = M \otimes_R R$ (2.2.4.12)(2.2.4.13), the restriction.

- $f_1 : \text{Mod}_S \to \text{Mod}_R : f_1 M = M \otimes_S R$ is the induced module, it is left adjoint to restriction, by (2.2.4.13).

- $f_* : \text{Mod}_S \to \text{Mod}_R : f_* M = \text{Hom}_S(R, M)$ is the coinduced module, it is right adjoint to restriction, by (2.2.4.13).

Def. (2.2.4.15)[Algebras]. For $R \in \mathbb{C}\text{Ring}$, a(n) (commutative/unital/associative) algebra over $R$ is a (commutative/unital/associative)magma object in the monoidal category $\text{(Mod}_R, \otimes)$.

The category of $R$-algebras is denoted by $\text{Alg}_R$. The category of commutative $R$-algebras is denoted by $\mathbb{C}\text{Alg}_R$, the category of commutative unital associative algebra over $R$ is denoted by $\mathbb{C}\text{Ring}_R$. Notice $\mathbb{C}\text{Ring}_R \cong \mathbb{C}\text{Ring}/R$.

Torsion-Free Modules

Def. (2.2.4.16)[Torsion-Free Modules]. Let $R$ be a ring, an $R$-module $M$ is called torsion-free iff there are no non-zero divisor $x \in R, 0 \neq f \in M$ that $xf = 0$.

Prop. (2.2.4.17). If $0 \to M_1 \to M_2 \to M_3$ and $M_1, M_3$ are torsion-free, then $M_2$ is torsion-free. Torsion-free is a stalk-wise property (4.1.4.2).

Proof: Trivial. □

Prop. (2.2.4.18). Let $M$ be a finite $R$-module, then $M$ is torsion-free if it is a submodule of a finite free module.

Proof: One direction is trivial, for the other, if $M$ is torsion-free, then $M \subset M \otimes_R K$, and $M \otimes_R K$ is a finite $K$-vector space, with basis $e_i$. Now let $x_i$ be a basis of $M$, let $x_i = \sum a_{ij}b_{ij}e_j$, then let $e = \prod_{ij} b_{ij}$, then $M \subset Re_1/b \oplus \ldots \oplus Re_n/b$. □

Prop. (2.2.4.19). If $M, N$ are $R$-modules that $M$ is torsion-free, then $\text{Hom}(N, M)$ is torsion free.

Proof: Choose a surjection $\bigoplus_I R \to N \to 0$, then $\text{Hom}(N, M) \hookrightarrow \prod_I M$ is torsion free. □

Modules over PID or Bézout Domains

Prop. (2.2.4.20)[Modules over a Bézout domain]. Let $R$ be a Bézout domain, then

- any finite submodule of a free module over $R$ is finite free.
any f.p. \( R \)-module \( M \) is a summand of a free \( R \)-module and \( M_{\text{tor}} \), where \( M_{\text{tor}} = \oplus R/(f_i) \) where \( f_i \in R^* \).

**Proof:** Cf.[Sta]0ASU. \( \square \)

**Prop. (2.2.4.21) [Classification of Modules over PID].**
1. Every submodule of a free module over a PID is free of smaller rank. Thus a projective module over a PID is free.
2. Every finite torsion-free module over a PID is free.
3. Every finite module over a PID has a primary decomposition \( M = \oplus_i R/(q_i) \), where \( (q_i) \) is primary ideals.

So projective \( \iff \) free \( \iff \) torsion-free (when f.g.).

**Proof:**
1: Choose a well ordering on the basis of \( F \), let \( F_i \) is the submodule generated by \( e_j, j \leq i \). Then \( \pi_j(P \cap F_i) \subset R \) is a module of the form \( (a_i) \), thus choose \( u_i \in P \) that \( p_i(u_i) = a_i \). Then \( u_i \) is a basis for \( P \): they are linearly independent, because for any finite linear combination that are 0, the maximal coordinate are 0. It also spans \( P \), because we can choose an element in \( P - \{u_i\} \) whose maximal nonzero coordinate \( \alpha \) is minimal among them, by well-orderedness. But we can subtract a multiple of \( u_\alpha \), thus producing a smaller element, contradiction.

2: If it is finite torsion-free, then it is a submodule of a finite free module(2.2.4.18), so it is free by item 1.

3: Follows immediately from(4.2.5.34) and(2.2.3.18).

**Prop. (2.2.4.22) [Primary Cyclic Decomposition].** There is a primary cyclic decomposition theorem for a torsion module \( M \) over a PID \( R \). Thus the multisets of elementary divisors of \( M \) is a complete set of invariants for \( M \).

**Proof:** Cf.[Advanced Linear Algebra P153]. \( \square \)

**Cor. (2.2.4.23) [Invariant Factor Decomposition].** By reordering the cyclic decomposition, we can get the invariant factor decomposition of \( M \), there are scalars \( d_m | d_{m-1} | \ldots | d_1 \) that are called the invariant factors of \( M \).

**Proof:** Cf.[Advanced Linear Algebra P157]. \( \square \)

**Cor. (2.2.4.24) [Elementary Factor Theorem].** Let \( F \) be a free module over a PID \( R \), and let \( M \) be a f.g. submodule\( \neq 0 \), then there exists a basis \( B \) of \( F \), elements \( e_1, \ldots, e_m \) in this basis, and non-zero elements \( a_1, \ldots, a_m \in R \) that

- the elements \( a_1 e_1, \ldots, a_m e_m \) forms a basis of \( M \).
- \( a_i | a_{i+1} \).

And these \( a_i \) are uniquely determined up to units.

**Transfinite Direct Sum Dévissage of Modules**

**Def. (2.2.4.25) [Direct Sum Dévissage of Modules].** Let \( M \) be a module over a ring \( R \), then a direct sum dévissage is a family of submodules \( M_\alpha \) indexed by an ordinal \( S \) such that

- \( M_0 = 0 \).
- if \( \alpha + 1 \in S \), then \( M_\alpha \) is a direct sum of \( M_{\alpha + 1} \).
• if $\alpha$ is a limit ordinal, then $M_\alpha = \bigcup_{\beta < \alpha} M_\beta$.

• $\bigcup_{\alpha \in S} M_\alpha = M$.

If moreover, for any $\alpha \in S, \alpha + 1 \in S$, $M_{\alpha + 1}/M_\alpha$ is countably generated, then $M_\alpha$ is called a Kaplansky dévissage of $M$.

**Prop.(2.2.4.26).** Let $M_\alpha$ be a direct sum dévissage of $M$, then $M \cong \bigoplus_{\alpha \in S, \alpha + 1 \in S} M_{\alpha + 1}/M_\alpha$.

**Proof:** Cf. [Sta]058V.

**Cor.(2.2.4.27).** $M$ is a direct sum of countably generated modules iff $M$ admits a Kaplansky dévissage.

**Prop.(2.2.4.28).** Suppose $M$ is a direct sum of countably generated modules and $P$ is a direct sum of $M$, then $P$ is also a direct sum of countably generated modules.

**Proof:** Cf.[Sta]058X.

**Prop.(2.2.4.29)[Direct Summand Criterion of Free Modules].** Let $M$ be a countably generated $R$-module that for any direct summand $N$ of $M$ and an element $x \in N$, $x$ is contained in a free direct summand of $N$, then $M$ is free.

**Proof:** Let $x_1, x_2, \ldots$ be a countable set of generators for $M$, then we can use inductions to find free submodules $F_1, F_2, \ldots$ of $M$ s.t. $\bigoplus_{i=1}^n F_i$ are direct summands of $M$ and contains $x_1, \ldots, x_n$ for any $n$, thus $M = \bigoplus F_i$ is free.

## 5 Field Extensions

**Prop.(2.2.5.1) [Artin].** If $G$ is a monoid and $K$ is a field, any distinct characters of $G$ in $K$ are linearly independent over $K$.

**Proof:** Consider the minimal length of linear combination that is 0, then we multiply a suitable $z$ in it, then we can can cancel a character, contradicting the minimality.

**Cor.(2.2.5.2).** If $\alpha_i$ are different elements in $K$ and there are element $a_i$ that $\sum a_i \alpha_i^v = 0$ for every $v \geq 0$, then $a_i = 0$ for all $n$. (Seen as characters from $\mathbb{Z}_{\geq 0} \to K$).

**Def.(2.2.5.3)[Composition of Fields Extensions].**

**Field Extensions**

**Def.(2.2.5.4) [Distinguished Class of Extensions].** A family $L$ of extensions are called distinguished iff

- It is closed under base change.
- $E/F/K \in L$ iff $F/K \in L$ and $E/F \in L$.

**Def.(2.2.5.5) [Algebraic Extensions].** An algebraic extension is a field extension $L/K$ s.t. for any element $\alpha \in L$, there exists a nonzero polynomial $f(X) \in K[X]$ s.t. $f(\alpha) = 0$.

**Prop.(2.2.5.6).** The family of finite extensions form a distinguished class.

The family of algebraic extensions form a distinguished class.

The family of f.g. extensions form a distinguished class.
Proof: Finite case is trivial. For the alg. extensions, for \( k \subset F \subset E \), for any \( \alpha \in E \), \( \alpha \) satisfies an polynomial function with f.m coefficients in \( F \), the coefficients form a subfield \( F_0 \) of \( F \) which is finite over \( k \), so \( k \subset F_0 \subset F_0(\alpha) \) is a finite tower, so it is finite, hence algebraic. The base change is easy to check.

For f.g. extensions, it suffice to check composition:?

Prop. (2.2.5.7). For an alg.extension \( k \subset E \), any injective field map \( E \to E \) over \( k \) is an automorphism. (This is because it induce a permutation of any \( \alpha \) with its conjugates in \( E \), so it is surjective).

Lemma (2.2.5.8). Let \( f \in k[X] \) be a polynomial of degree \( \geq 1 \), then there is a field \( K \) that \( f \) has a root in \( K \). Hence for any finite set of polynomials, there is a field \( K \) that all of them have roots in \( K \).

Proof: Cf. [Algebra Lang P231].

Lemma (2.2.5.9). For any \( k \in \text{Field} \), there exists \( K \in \text{Field} \) s.t. \( k \subset K, K = K \).

Proof: Firstly, we construct a field that every polynomial in \( k[X] \) of degree \( \geq 1 \) has a root. Consider the polynomial ring \( k[X_f] \), where there is a indeterminant \( X_f \) for each \( f \in k[X] \) of deg \( \geq 1 \). Then the ideal generated by \( f(X_f) \) is not a unit ideal, which can be seen by constructing a finite field extension that \( f_i \) all have a root in it (2.2.5.8).

So if \( \mathfrak{m} \) is a maximal ideal containing all \( f(X_f) \), then the quotient field is a field that all \( f \) have a root(\( X_f \)).

So now if we construct inductively like this, and consider their union, then it is clearly a field and any polynomial of degree \( \geq 1 \) have a root in it.

Prop. (2.2.5.10) [Algebraic Closure]. For any field \( K \). There exists uniquely an alg.closed field \( K/k \) that is algebraic over \( K \), up to isomorphism over \( k \), called the algebraic closure of \( k \), denoted by \( \overline{k} \).

Proof: Let \( E \) be a field that is alg.closed and contains \( k \) by (2.2.5.9). Let \( k^a \) be the union of subextensions that are algebraic over \( k \). \( k^a \) is a field, by (2.2.5.6), and \( k^a \) is alg.closed, because if \( f(X) \) is a polynomial of degree \( \geq 1 \) in \( k^a[X] \), then it has a root \( \alpha \in E \), and \( \alpha \) is algebraic over \( k^a \), so \( \alpha \in k^a \).

Prop. (2.2.5.11) [Finite Algebraic Extensions]. Let \( L/K \) be a field extension and \( F/L \) be a finite extension, then there is a finite extension \( F'/K \) s.t. \( F = LF' \).

Proof: Take a generator \( x_i \) of \( F/L \), then \( x_i \) are algebraic over \( L \), thus there are polynomials \( f_i \in L[X] \) s.t. \( f_i(x_i) = 0 \). Let \( F' \) be the fields over \( K \) generated by all the coefficients of \( f_i \)'s, then \( F = LF' \).

Prop. (2.2.5.12). If \( E/F \) is an algebraic field extension, then for any \( R \) that \( E \subset R \subset F \), \( R \) is a field.

Proof: If \( \alpha \in R \), then \( \alpha \) is algebraic over \( E \), so there is a relation \( \alpha^n + \ldots + a_0 = 0 \), so \( \alpha^{-1} = -a_0^{-1}(a_1 + \ldots \alpha^{n-1}) \in R \).
Normal & Separable Extensions

Def. (2.2.5.13) [Normal Extensions]. A field extension $K/k$ in $\bar{k}$ is called normal extension iff it satisfied the following equivalent conditions:

- Any embedding of $K$ into $\bar{k}$ induce an automorphism on $K$.
- $K$ is the splitting field of a family of polynomials in $k[X]$.
- Every irreducible polynomial in $k[X]$ that has a root in $K$ splits in $K$.

Proof: Cf. [Algebra Lang P237].

Prop. (2.2.5.14). Normal extension are stable under base change and composition, by the first definition of (2.2.5.13).

Def. (2.2.5.15) [Normal Closure]. For any field extension $F/K$, there is a field extension $E/F$ that $E/K$ is normal, called the normal closure of $F/K$. It is the composite of conjugates of $F/K$.

Def. (2.2.5.16) [Separable Degree]. Define the separable degree $[E : k]_s$ of an extension $E/k$ as the cardinality of embedding of $E$ into $\bar{k}$. Separable degree commutes with composition, and when $E/k$ is finite, $[E : k]_s \leq [E : k]$.

Def. (2.2.5.17) [Separable Polynomials]. A finite extension is called a separable extension iff $[E : k]_s = [E : k]$, an algebraic number $\alpha$ over $k$ is called separable over $K$ iff $k(\alpha)/k$ is separable. A polynomial $f \in k[X]$ is called a separable polynomial iff it has no multiple roots in $\bar{k}$.

Def. (2.2.5.18) [Separable Extensions]. An algebraic extension $E/k$ is called a separable extension iff it satisfies the following equivalent conditions:

- every f.g. subfield is separable over $k$, (this is compatible because subfield of a finite separable extension is separable, by the compatibility of separable degree).
- Every element of $E$ is separable.
- It is generated by a family of separable elements.

Proof: If $E/k$ is separable and $k \subset k(\alpha) \subset E$, then by (2.2.5.17), $k(\alpha)$ is separable. And if it is generated by a family of separable elements $\{\alpha_i\}$, then any f.g. subfield can are f.g. by elements $\{\alpha_i\}$. Now it is a tower of separable extensions, hence separable by the compatibility of separable degree.

Prop. (2.2.5.19). Separable extensions form a distinguished class.

Proof: Cf. [Algebra Lang P241].

Prop. (2.2.5.20) [Primitive element Theorem]. A finite extension $E/k$ is primitive iff there are only f.m. middle fields. And if $E/k$ is separable, this is satisfied.

Proof: If $k$ is finite, this is simple. Assume $k$ infinite, for any two elements $\alpha, \beta$, consider $k(\alpha + c, \beta)$, if there is only finitely many middle fields, there exists two that is equal, so $k(\alpha, \beta) = k(\gamma)$. Proceeding inductively, $E$ is primitive.

Conversely, if $k(\alpha) = E$, every middle field corresponds to a divisor of the irreducible polynomial of $\alpha$. This map is injective, because for any $g_F$, degree of $\alpha$ over $F$ is the same over the degree over the coefficient field of $g_F$, so it must be equal to $F$. 

If \( E/k \) is separable, Let

\[
P(X) = \prod_{i \neq j} (\sigma_i \alpha + X \sigma_i \beta - \sigma_j \alpha - X \sigma_j \beta)
\]

for different embedding \( \sigma_i, \sigma_j \) of \( E(\alpha, \beta) \) into \( k^{\text{alg}} \). Then it is not identically zero, thus there exists \( c \) that \( \sigma_i(\alpha + c \beta) \) is all distinct, thus generate \( K(\alpha, \beta) \). \( \square \)

**Inseparable Extensions**

**Prop. (2.2.5.21).** Any irreducible polynomial of fields of characteristic 0 is separable and if \( \text{char} = p \), then all roots have the same multiplicity and thus \( [k(\alpha) : k] = p^n [k(\alpha) : k] \) for some \( n \).

**Proof:** All roots have the same multiplicity because there are Galois actions. If the multiplicity is not 1, the derivative \( f' \) is zero, otherwise \( f \) is not irreducible. Then \( f(X) = g(X^p) \). We can choose \( f(X) = h(X^{p^n}) \) with \( h \) separable, then \( [k(\alpha) : k(\alpha^p^n)] = p^n \), thus the result. \( \square \)

**Def. (2.2.5.22).** The **inseparable degree** \( [E : k]_s \) is defined as the quotient \( [E : k]/[E : k]_s \). An algebraic element \( \alpha \) is called **purely inseparable** over \( k \) iff there is a \( n \) that \( \alpha^{p^n} \in k \).

**Def. (2.2.5.23).** An extension is called **purely inseparable** if it satisfies the following equivalent conditions:

- \( [E : k]_s = 1 \).
- Every element \( \alpha \) of \( E \) is purely inseparable over \( k \).
- For every \( \alpha \in E \), the irreducible equation of \( \alpha \) over \( k \) is of type \( X^{p^n} - a \).
- It is generated by a family of purely inseparable elements.

**Proof:** Cf. [Algebra Lang P249]. \( \square \)

**Cor. (2.2.5.24).** A field over \( \mathbb{F}_p \) is perfect iff there are no purely inseparable extensions of it.

**Cor. (2.2.5.25) [Perfect Closure].** For any field \( k \) of char \( p \), there is a unique purely inseparable field extension \( k^{\text{perf}}/k \) that \( k^{\text{perf}} \) is perfect, called the **perfect closure** of \( k \). It is generated by adding all the \( p^n \)-th roots to \( k \).

**Prop. (2.2.5.26).** Purely inseparably extensions form a distinguished class.

**Proof:** Cf. [Algebra Lang P250]. \( \square \)

**Prop. (2.2.5.27).** If \( E/k \) is algebraic and \( E_0 \) be the maximal separable extension contained in \( E \), then \( E/E_0 \) is purely inseparable. And if \( E/k \) is normal, then \( E_0/k \) is normal, too.

**Proof:** By the proof of (2.2.5.21), any \( \alpha \) has a \( p^n \) that \( \alpha^{p^n} \) that \( \alpha^{p^n} \) is separable, hence it is purely inseparable over \( E_0 \) by (2.2.5.23). \( E_0/k \) is normal because any \( \sigma \) maps \( E \) to itself, and \( E_0 \) to \( \sigma(E_0) \in E \) separable, hence \( \sigma(E_0) \subset E_0 \). \( \square \)
Trace and Norm

Prop. (2.2.5.28) [Trace and Norm]. Let \( L/K \) be a finite field extension and \( \Sigma \) be the set of embeddings \( \sigma : L \to \overline{K} \), then define the **trace map** \( \text{tr}_{L/K} : L \to K : x \mapsto [L : K] \sum_{\sigma \in \Sigma} \sigma(x) \) and the **norm map** \( N_{L/K} : L \to K : x \mapsto (\prod_{\sigma \in \Sigma} \sigma(x))^{[L : K]} \).

Prop. (2.2.5.29). Let \( L/K \) be a field extension,

- The norm induces a multiplicative homomorphism \( L^* \to K^* \), and the trace induces an additive homomorphism \( L \to K \).
- If \( E/F/K \) are field extensions, then \( N_{E/K} = N_{F/K} \circ N_{E/F} \), and \( \text{tr}_{E/K} = \text{tr}_{F/K} \circ \text{tr}_{E/F} \).
- If \( L = K(\alpha) \) and \( F = \text{Irr}(\alpha, k; X) = X^n - a_{n-1}X^{n-1} + \ldots + (-1)^n a_0 \), then
  \[
  N_{L/K}(\alpha) = a_0, \quad \text{tr}_{L/K}(\alpha) = a_{n-1}.
  \]


Prop. (2.2.5.30) [Calculating Dual Basis]. Let \( L = K(\alpha) \) be a finite separable extension, let \( f(X) = \text{Irr}(\alpha, k; X) \), and

\[
\frac{f(X)}{X - \alpha} = \beta_0 + \beta_1 X + \ldots + \beta_{n-1} X^{n-1},
\]

then the dual basis of \((1, \alpha, \ldots, \alpha^{n-1})\) w.r.t. the trace form (2.2.5.32) is

\[
\frac{\beta_0}{f'(\alpha)}, \ldots, \frac{\beta_{n-1}}{f'(\alpha)}.
\]

Proof: Denote the roots of \( f \) be \( \alpha_i \), then they are pairwise different, and

\[
\sum_i \frac{f(X)}{X - \alpha_i} \frac{\alpha_i^r}{f'(\alpha_i)} = X^r
\]

for all \( r \) by Lagrange interpolation (2.2.2.2). But this is equivalent to

\[
\text{tr}
\left(\frac{\alpha_i^r \beta_j}{f'(\alpha)}\right) = \delta_{ij}
\]

Prop. (2.2.5.31). Let \( L/K \) be a field extension, then \( x \in L \) acts on \( L \) via multiplication \( T_x \). Then

\[
\det(T_x) = N_{L/K}(x), \quad \text{tr}(T_x) = \text{tr}_{L/K}(x).
\]

Proof: Let \( F = K(x) \subset L \), and \( p(X) \) be the minimal monic polynomial of \( x \), then \( \text{char}(T_x; X) = \text{char}(T_x|K; X)^{[L:K(x)]} \), thus we are done by (2.2.5.29).

Prop. (2.2.5.32) [Trace Form]. If \( L/K \) is a finite extension, consider the pairing

\[
Q_{L/K} : L \times L \to K : (x, y) \mapsto \text{tr}(xy)
\]

called the **trace form**. Then the following are equivalent:
Prop. (2.2.6.2).

Def. (2.2.6.1) [Transcendental Basis].

Prop. (2.2.5.34).

Def. (2.2.5.33) [Discriminant of a Basis].

We define $x$ self algebraically independent. So

If $L/K$ is inseparable, then by (2.2.5.29), if we consider $L/K'/K$ that $L/K'$ is purely inseparable of degree $p$, then it is generated by some equation $x^p - a$, and the root is $\alpha$. Then $L = K'(\alpha)$ and the minimal polynomial of $\alpha^i, 0 \leq i \leq p - 1$ is $x^p - a^i$, so $\text{tr}(\alpha^i) = 0$, and $\text{tr} L/K = 0$.

If $L/K$ is separable, $\text{tr}_{L/K} \neq 0$ by the linear independence of characters (2.2.7.3). □

Def. (2.2.5.33) [Discriminant of a Basis]. Let $\alpha_i$ be a basis of a separable extension $L/K$, then the discriminant of the basis $d(\alpha_1, \ldots, \alpha_n)$ is defined to be $\det(\sigma_i(\alpha_j))^2$. Clearly, $d(\alpha_1, \ldots, \alpha_n)$ is invariant under the Galois action of $L/K$, thus it is an element of $K$.

Prop. (2.2.5.34). Notice $\text{tr}_{L/K}(\alpha_i \alpha_j) = \sum_k \sigma_k(\alpha_i) \sigma_i(\alpha_j)$, thus $(\text{tr}_{L/K}(\alpha_i \alpha_j))$ is the product of the matrices $(\sigma_k \alpha_i)^t$ and $(\sigma_k \alpha_j)$, thus

$$d(\alpha_1, \ldots, \alpha_n) = \det(\text{tr}_{L/K}(\alpha_i \alpha_j)).$$

So the discriminant of $\{\alpha_1, \ldots, \alpha_n\}$ is the Gram matrix of the trace norm w.r.t. this basis (2.3.8.24). In particular, by (2.2.5.32),

$$d(\alpha_1, \ldots, \alpha_n) \neq 0.$$ 

6 Transcendental extension

Def. (2.2.6.1) [Transcendental Basis]. Let $K$ be an extension of a field $k$, a transcendental base is an algebraically independent set that any element is algebraic over it.

Given any algebraically independent set $S \subset T$ a set over which $K$ is algebraic, $S$ can be extended to a transcendental base contained in $T$, by Zorn’s lemma. In particular, a transcendental basis exists.

Prop. (2.2.6.2). Any two transcendental bases have the same cardinality, called the transcendental degree of $K/k$, denoted by $\text{tr deg}_k(K)$.

Proof: If $K/k$ has a finite transcendental basis, then let $X = \{x_1, \ldots, x_m\}$ transcendental base of minimal number, $S = \{w_1, \ldots, w_n\}$ an algebraically independent set. If $n > m$, we proceed by changing one element in $X$ a time using induction and prove that $K$ is algebraic over $\{w_1, \ldots, w_r, x_{r+1}, \ldots, x_m\}$, contradiction.

Because $w_{r+1}$ is algebraic over $\{w_1, \ldots, w_r, x_{r+1}, \ldots, x_n\}$, we have a minimal polynomial

$$f = \sum g_j(w_{r+1}, w_1, \ldots, w_r, x_{r+2}, \ldots, x_m)x_j^{r+1}$$

s.t. $f(w_{r+1}, w_1, \ldots, x_m) = 0$ (after possibly renumbering $x_i$, this $x$ must exists because $S$ is itself algebraically independent). So $x_r$ is algebraic over $\{w_1, \ldots, w_r, x_{r+1}, \ldots, x_n\}$, hence $K$ is independent over it, too.

If $K/k$ has an infinite basis $B$, let $B'$ be another basis, then for any $\alpha \in B^*$, there is a finite set $B_\alpha \subset B$ that $\alpha$ is algebraic over $k(B_\alpha)$, because algebraic equation involves f.m. generators. Then we define $B^* = \cup_{\alpha \in B^*}$, then it has cardinality smaller than $B'$. But $B^* = B$, because for any $\beta \in B$, $\beta$ is algebraic over $B'$ which is algebraic over $k(B^*)$, thus $\beta$ is algebraic over $k(B^*)$, thus $\beta \in B^*$. □
Prop. (2.2.6.3). If $K$ is of finite transcendental degree over $k$, then $|K| = |k|$.

Proof: We find a purely transcendental $L/k$ that $K/L$ is algebraic, then the element of $L$ are all polynomials of finite indeterminants of elements of $k$, so $|L| = |k|$ by (1.1.5.4), and similarly $|K| = |L|$.

Prop. (2.2.6.4). Two alg.closed field of the same transcendental degree over base field is isomorphic.

Proof: We define a bijection of the transcendental basis, and then extend it to an isomorphism of fields, by adjunction of algebraic numbers using Zorn's lemma.

Prop. (2.2.6.5) [Lüroth]. The automorphism group of $K(T)$ is $PGL_2(K)$.

Proof: Consider $\theta = \sigma(x) = \frac{f(x)}{g(x)}$, then $x$ is algebraic over $K(\theta): \theta g(x) - f(x) = 0$. Now $x$ is transcendental over $K$, thus $\theta$ is transcendental over $K$ as well. Now the minimal polynomial of $x$ over $K(\theta)$ is just $\theta g(x) - f(x)$, because it is irreducible, as it is linear over $\theta$. But $K(x) = K(\theta)$, thus the polynomial must have degree 1, so $f(x), g(x)$ is of degree 1. Now the rest is clear.

Prop. (2.2.6.6) [Lüroth]. Any subfield $K \nsubseteq L \subset K(T)$ is of the form $K(u)$ where $u \in K(X)$ is transcendental over $K$.

Proof: It is clearly transcendental over $K$, so this follows from (5.11.1.17) and Riemann-Hurwitz (5.11.1.32), notice that the field extension is separable by (4.3.9.4): The non-singular complete curve corresponding to $L$ has genus 0, and it has a rational point, so isomorphic to $\mathbb{P}^1_k$ (5.11.8.2).

7 Galois Theory

Def. (2.2.7.1) [Galois Extension]. A Galois field extension is a field extension that is both normal and separable.

Def. (2.2.7.2) [Galois Closures]. Let $F/K$ be a separable extension, then the normal closure $E/K$ is also separable, called the Galois closure of $F/K$.

In particular, the maximal separable extension $k^{\text{sep}}/k$, called the separable closure of $k$, is Galois over $k$, and $\text{Gal}(k^{\text{sep}}/k)$ is denoted by $\text{Gal}_k$.

Prop. (2.2.7.3) [Algebraic Independence, Artin]. Let $L$ be a field, $G$ be a monoid and $\chi_i: G \to L$ be multiplicative maps, then $\chi_i$ are linearly independent over $L$.

Proof: Let $\sum_{i=1}^n a_i \chi_i = 0$ and $a_i \neq 0$ for any $i$, we use induction to derive contradictions: for all $i$, $n = 1$ is trivial, and for general $n$, assume $a_1, a_2 \neq 0$, then the two equations $\chi_1(h) \neq \chi_2(h)$, then $\sum_{i=1}^n a_i \chi_i(hg) = 0$ and $\sum_{i=1}^n a_i \chi_i(g) = 0$ gives us a equation with smaller $n$, thus we are done.

Prop. (2.2.7.4) [Galois Main Theorem, Artin]. Let $G$ be a finite group of automorphisms of $K$. Then $K/K^G$ is Galois of Galois group $G$.

Proof: For every element $x$, set $\{\sigma_1 x, \ldots, \sigma_r x\}$ be distinct conjugates, then $f(X) = \prod_{i=1}^r (X - \sigma_i x)$ shows that $K$ is separable and normal over $K^G$. And primitive element theorem shows that $[K : K^G] \leq |G|$, so it must equals $G$. 

Prop. (2.2.7.5). If \( L/K \) is a finite Galois extension, then there is an isomorphism:

\[
L \otimes_K L \cong L \times L \times \ldots \times L : (a, b) \mapsto (ab, a\sigma_1(b), \ldots, a\sigma_{n-1}(b))
\]

where \( \sigma_i \) are Galois elements.

Proof: Choose a primitive element \( x \) and its minimal polynomial \( f(x) \), then \( L \cong K[X]/(f) \), and \( L \otimes_K L \cong L[X]/(f) \), but \( f \) decomposes completely in \( L[X] \), thus by Chinese remainder theorem (2.2.3.17), the given map is an isomorphism of rings.

Prop. (2.2.7.6) [Infinite Galois Theorem]. The middle fields correspond to the closed subgp of \( G(L/K) \).

Proof: The highlight is that \( G(L/L^n) = H \) for a closed subgp \( H \) of \( G(L/K) \). If \( \sigma \) fixes \( L^n \) but is not in \( H \), because for every finite field \( M \), \( H \cdot G(L/M) \) corresponds to \( M/(M \cap L^n) \), so \( \sigma G(L/M) \cap H \neq \emptyset \). So \( \sigma \) is in the closure of \( H \) thus in \( H \).

Prop. (2.2.7.7) [Normal Basis Theorem]. For a finite Galois extension, normal basis exists.

Proof: Finite case: The Galois group is cyclic, and the linear independent of characters shows that the minimal polynomial of \( \sigma \) is \( n \)-dimensional thus equals \( X^n - 1 \). Regard \( L \) as a \( K[X] \) module thus by (2.2.4.21) is a direct sum of modules of the form \( K[X]/(f(x)) \), \( f(x)|X^n - 1 \) and the minimal polynomial for the action of \( X \) is \( X^n - 1 \). So it must be isomorphic to \( K(X)/(X^n - 1) \).

Infinite Case: Let

\[
f([X_\sigma]) = \det(t_{\sigma_i, \sigma_j}), \quad t_{\sigma, \tau} = X_{\sigma^{-1}\tau}
\]

We see \( f \neq 0 \) by substituting 1 for \( X_{id} \) and 0 otherwise. So it won’t vanish for all \( x \) if we substitute \( X_\sigma = \sigma(x) \) because \( [\sigma(x)] \) is pairwisely different. Thus there exists \( w \) s.t.

\[
\det(\sigma^{-1}\tau(w)) \neq 0.
\]

Now if

\[
\sum a_{\tau}(w) = 0, \quad a_{\sigma} \in K,
\]

act by \( \sigma \) for all \( \sigma \), we get \( [\sigma^{-1}\tau(w)][a_{\sigma}] = 0 \), thus \( [a_{\sigma}] = 0 \).

Prop. (2.2.7.8) [Kummer Theory]. Let \( K \) be a field and containing the set \( n \)-th roots of unity \( \mu_n \) where \( n \in \mathbb{Z} \cap K^* \), a Kummer extension \( L/K \) of exponent \( n \) is a Galois extension that the Galois group is Abelian of exponent \( n \).

Then there is an inclusion preserving isomorphism between the lattice of Kummer extensions \( L \) over \( K \) and the lattice of subgroups of \( K^\times \) containing \( (K^\times)^n \):

\[
L \mapsto \Delta = (L^\times)^n \cap K^\times, \quad \Delta \mapsto K(\sqrt[n]{\Delta}).
\]

And \( \Delta/(K^\times)^n \) is isomorphic to \( \text{Gal}(L/K)^\vee = \text{Hom}(\text{Gal}(L/K), \mathbb{Q}/\mathbb{Z}) \).

Proof: The Galois cohomology of the Kummer sequence \( 1 \to \mu_n \to L^\times \xrightarrow{n} (L^\times)^n \to 0 \) says

\[
1 \to K^\times \xrightarrow{n} (L^\times)^n \cap K^\times \xrightarrow{\delta} H^1(\text{Gal}(L/K), \mu_n) \to H^1(\text{Gal}(L/K), L^\times) = 1 (10.1.3.2)
\]

And \( \text{Gal}(L/K) \) acts trivially on \( \mu_n \subset K^* \), so

\[
H^1(\text{Gal}(L/K), \mu_n) = \text{Hom}(\text{Gal}(L/K), \mathbb{Q}/\mathbb{Z})
\]
and
\[ \delta : a \mapsto \chi_a(\sigma) = \sigma(\sqrt[n]{a})/\sqrt[n]{a} \in \mu_n. \]

Now let \( L/K \) be the maximal Kummer extension of exponent \( n \), then \((L^\times)^n = K^\times\). So the assertion follows from Galois theory on applied to \( L/K \).

\[ \square \]

**Prop. (2.2.7.9) [Finite Fields].** \( \text{Gal}(\mathbb{F}_{p^n}/\mathbb{F}_p) = \mathbb{Z}/(n) \) and is generated by the Frobenius.

**Proof:**

**Prop. (2.2.7.10) [Artin-Schreier Theory].** Let \( K \) be a field of characteristic \( p > 0 \) containing \( \mathbb{F}_q \), where \( q = p^k \), an Artin-Schreier extension \( L/K \) of exponent \( q \) is a Galois extension that the Galois group is Abelian of exponent \( q \).

Then there is an inclusion preserving isomorphism between the lattice of Artin-Schreier extensions \( L \) over \( K \) of exponent \( q \) and the lattice of subgroups of \( W_{p,k}^+(K) \) containing \((W_{p,k}^+(\text{Frob}_p^k) - \text{id})(W_{p,k}^+(K)):\)

\[ L \mapsto \Delta = (W_{p,k}^+(\text{Frob}_p^k) - \text{id})(W_{p,k}^+(L)) \cap W_{p,k}^+(K), \]
\[ \Delta \mapsto K\{b_{i_1}, \ldots, b_{i_k}| b_i = (b_{i_1}, \ldots, b_{i_k}), W_{p,k}^+(\text{Frob}_p^k)(b) - b \in \Delta\}. \]

And \( \Delta/(W_{p,k}^+(\text{Frob}_p^k) - \text{id})(W_{p,k}^+(K)) \) is isomorphic to \( \text{Gal}(L/K)^\vee = \text{Hom}(\text{Gal}(L/K), \mathbb{Q}/\mathbb{Z}) \).

**Proof:** The Galois cohomology of this exact sequence

\[ 0 \to W_{p,k}^+(\mathbb{F}_q) \to W_{p,k}^+(L) \xrightarrow{W_{p,k}^+(\text{Frob}_p^k) - \text{id}} (W_{p,k}^+(\text{Frob}_p^k) - \text{id})(W_{p,k}^+(L)) \to 0, \]

says

\[ 1 \to W_{p,k}^+(K) \xrightarrow{W_{p,k}^+(\text{Frob}_p^k) - \text{id}} (W_{p,k}^+(\text{Frob}_p^k) - \text{id})(W_{p,k}^+(L)) \cap W_{p,k}^+(K) \]
\[ \xrightarrow{\delta} H^1(\text{Gal}(L/K), W_{p,k}^+(\mathbb{F}_q)) \to H^1(\text{Gal}(L/K), W_{p,k}^+(L)) = 0(10.1.3.3) \]

And \( \text{Gal}(L/K) \) acts trivially on \( W_{p,k}^+(\mathbb{F}_q) \), so by (4.5.3.22),

\[ H^1(\text{Gal}(L/K), W_{p,k}^+(\mathbb{F}_q)) = \text{Hom}(\text{Gal}(L/K), \mathbb{Q}/\mathbb{Z}) \]

and

\[ \delta : a \mapsto \chi_a(\sigma) = \sigma(b) - b \in W_{p,k}^+(\mathbb{F}_q), \quad W_{p,k}^+(\text{Frob}_p^k)(b) - b = a. \]

Next we prove for any \( b = (b_1, \ldots, b_k), W_{p,k}^+(\text{Frob}_p^k)(b) - b \in W_{p,k}^+(K), K\{b_1, \ldots, b_k\}/K \) is Abelian of exponent \( q \). Let \( K_i = K(\{b_1, \ldots, b_i\}) \). By (4.5.3.4),

\[ (b_1^q, \ldots, b_k^q) - (b_1, \ldots, b_k) \in W_{p,k}^+(K) \]

implies \( b_i^q - b_i \in K_{i-1} \). Thus \( K_i/K_{i-1} \) is an Artin-Schreier extension of exponent \( p \). As the Galois action is always of the form \( \sigma(s) - s \in \mathbb{F}_q \) for any \( \sigma \in \text{Gal}(K_k/K) \) and \( s \in K_k \), we see \( K_k/K \) is also Artin-Schreier of exponent \( q = p^k \).

Now let \( L/K \) be the maximal Artin-Schreier extension of exponent \( q \), then \((W_{p,k}^+(\text{Frob}_p^k) - \text{id})(W_{p,k}^+(L)) = W_{p,k}^+(K) \). So the assertion follows from Galois theory on applied to \( L/K \).

\[ \square \]
Cor. (2.2.7.11) [Artin-Schreier of Exponent $p$]. Let $K$ be a field of characteristic $p > 0$, then there is an inclusion preserving isomorphism between the lattice of Artin-Schreier extensions $L$ over $K$ of exponent $p$ and the lattice of subgroups of $K^+$ containing $\{x^p - x| x \in K\}$:

$$L \mapsto \Delta = \{x^p - x| x \in L\} \cap K,$$

$$\Delta \mapsto K(\{b| b^p - b \in \Delta\}).$$

And $\Delta/\{x^p - x| x \in K\}$ is isomorphic to $\text{Gal}(L/K)^\vee = \text{Hom}(\text{Gal}(L/K), \mathbb{Q}/\mathbb{Z})$.

8 Ordered Rings

Def. (2.2.8.1) [Ordered Rings]. An ordered ring is a ring $R$ together with a subset $P \subset R$ that $R$ is a disjoint union $P \bigcup \{0\} \bigcup (-P)$, and if $x, y \in P$, then $x + y, xy \in P$. Elements in $P$ are called positive elements.

An ordered field is an ordered ring that is also a field. An orderable ring/field is a ring/field that can be given an ordered structure.

Prop. (2.2.8.2). An orderable field has char0, because $0 \notin P \cup (-P)$.

A square $> 0$ in an ordered field (trivial).

Def. (2.2.8.3) [Convex Subgroup]. Let $\Gamma$ be an ordered Abelian group (2.2.8.1), then a convex subgroup of $\Gamma$ is a subgroup $\Delta$ that if $a < b < c$ and $a, c \in \Delta$, then $b \in \Delta$. Notice this is in fact equivalent to if $0 < c \in \Delta$, then $0 < b < c$ are also in $\Delta$.

Prop. (2.2.8.4) [Height]. The set of all convex subgroups of $\Gamma$ is well-ordered, and its ordinal is called the height of $\Gamma$.

Proof: If $\Delta_1, \Delta_2$ don’t contains each other, let $a \in \Delta_1 - \Delta_2$ and $b \in \Delta_2 - \Delta_1$, then changing $\pm a, \pm b$, we may assume $0 < a < b$, so $a \in \Delta_2$, contradiction. \qed

Prop. (2.2.8.5) [Height 1 Case]. Let $\Gamma$ be an ordered Abelian group, then the following are equivalent:

1. $\text{ht}(\Gamma) = 1$.
2. for all $a, b \in \Gamma$ that $a > 0$ and $b \geq 0$, there is an integer $n$ that $b \leq na$.
3. there exists an injection from $\Gamma$ to $\mathbb{R}$.

Proof: $3 \rightarrow 1$ is easy.

1 $\rightarrow$ 2: Consider the convex subgroup generated by $a$, then it is $\Delta$ by height condition, so $b$ must by in it, i.e. $b \leq na$ for some $n$.

2 $\rightarrow$ 3: Choose an $a > 0$, let the injection $\varphi$ given by $\varphi(b) = \sup\{\frac{b}{k}| na \leq kb\}$ for $b > 0$ and extends to negative elements.

It is easily verified that $\varphi(c) + \varphi(b) \leq \varphi(c + b)$, and if $\varphi(c) + \varphi(b) < \varphi(c + b)$, choose a rational approximation of them, and multiply to get integers, then if $k(c+b) \leq \varphi(c+b)ka > \varphi(b)a + \varphi(c)a + a$, then either $kc \geq \varphi(c)ka + a$ or $kb \geq \varphi(b)ka + a$, contradiction.

So this map is truly a morphism of ordered Abelian groups, and it is injective because if $b > 0$, then by 2, there must be an $n$ that $a \leq nb$, so $\varphi(b) \geq 1/n$. \qed
9 Real Fields

Def.(2.2.9.1)[Real Fields]. A field \( K \) is called real if \(-1\) is not a sum of squares in \( K \). A field \( K \) is called real closed iff it is real, and any alg.extension that is real must be itself. An ordered field is clearly a real field by (2.2.8.2), the converse is in fact true, by (2.2.9.11). In particular, a real field is of characteristic 0.

Prop.(2.2.9.2). If \( K \) is real, \( a \in K \), and \( -a \) cannot both be sum of squares. If \( -a \) is not a sum of squares in \( K \), then \( K(\sqrt{a}) \) is real. Hence either \( K(\sqrt{a}) \) or \( K(\sqrt{-a}) \) is real.

Proof: Suppose \( K(\sqrt{a}) \) is not real. If \( a \) is a square, then \( K(\sqrt{a}) = K \) is real. So \( a \) is not a square,

\[
-1 = \sum (b_i + c_i \sqrt{a})^2 = \sum (b_i^2 + c_i^2 + 2b_i c_i \sqrt{a})
\]

Since \( \sqrt{a} \notin K \), \( -1 = \sum (b_i^2 + c_i^2) \), so

\[
-a = \frac{1 + \sum b_i^2}{\sum c_i^2}
\]

This implies that \( -a \) is a sum of squares. \( \square \)

Prop.(2.2.9.3). If the minimal polynomial \( f \) of an \( \alpha \) algebraic over a real field \( K \) is of odd degree, then \( K(\alpha) \) is real.

Proof: If \( K(\alpha) \) is not real, then \( -1 = \sum g_i(X)^2 + h(X)f(X) \), where \( g_i \) has degree smaller than \( n \).

This can happen if \( h(X) \) has degree odd and \( \leq n - 2 \). Then if \( \beta \) is a root of \( h \), then \( K(\beta) \) is also not real. So the proof is finished if we use induction. \( \square \)

Def.(2.2.9.4)[Real Closure Exists]. For any real field \( K \), there exists a real closure \( K^a \) of \( K \).

That is, it is real closed and algebraic over \( K \).

Proof: This is an easy consequence of Zorn’s lemma. \( \square \)

Cor.(2.2.9.5)[Real Closed Fields Unique Ordering]. There exists a unique ordering on a real closed field \( R \). The elements \( > 0 \) are just the squares in \( R \). Now every real closed field is assumed to have this ordering tacitly. In particular, any real closed field has char0, so does any real field.

Proof: The set of finite sum of squares in \( R \) is closed under addition and multiplication, and all of them are squares, by (2.2.9.2) and maximality of \( R \). Also by (2.2.9.2) either \( a \) is a square or \( -a \) is a square, but not simultaneously. So it is truly an order on \( R \). \( \square \)

Prop.(2.2.9.6)[Fundamental Theorem of Algebra]. For a field \( R \), \( R \) is real closed iff \( R \neq R[i] \) and \( \overline{R} = R(i) \).

Proof: One direction is trivial, the other follows from the lemma below (2.2.9.7), it satisfies the condition by (2.2.9.2) and maximality. \( \square \)

Lemma(2.2.9.7)[Equivalent Definition of Real Closed Fields]. If \( R \) is a real field that: for all \( a \in R, \sqrt{a} \in R \) or \( \sqrt{-a} \in R \), and any polynomial of odd degree has a root in \( R \), then \( K = R(i) \) is alg.closed.
Proof: For any order of $R$, the first condition in fact says that any $a > 0$ in $R$ is a square. Now $rac{a + \sqrt{a^2 + b^2}}{2}$ is non-negative, so there is a $c^2 = \frac{a + \sqrt{a^2 + b^2}}{2}$, that is $(c + \frac{b}{2c})^2 = a + bi$, so $K$ has all squares.

As $R$ is of char0(2.2.9.5)(2.2.8.2), so it suffices to show any Galois extension $L/K$ is trivial. Let $G = G(L/R)$, and $H$ be its 2-Sylow subgroup, then $G = H$ by condition. Now if $G_1 = G(L/K)$, then $G_1$ is nontrivial, because otherwise there is a subgroup of index 2, then its fixed field is a square extension of $K$, which is impossible by what we have proved. So $G = G_1$, that is $L = K$. □

Cor. (2.2.9.8) [Complex Numbers is Alg.Closed]. $\mathbb{C} = \mathbb{R}[i]$ is alg.closed.

Prop. (2.2.9.9) [Intermediate Property]. An ordered field is real closed iff it has the intermediate property.

Proof: If $R$ is real closed, as $R[i]$ is alg.closed(2.2.9.6), $f$ can be decomposed into factors of degree 1 or 2. For a factor $X^2 + \alpha X + \beta$, 4$\beta > \alpha^2$, otherwise it has a root hence not irreducible. So the change of sign is because of a linear factor, the rest is easy.

Conversely, if it has the intermediate property, then for $a > 0$, consider $p(X) = X^2 - a$, then $p(0) < 0, p(a + 1) > 0$, so $p$ has a root, that is, $a$ is a square. For a polynomial of odd degree, for $M$ large enough, $f(M) > 0, f(-M) < 0$, so $f$ has a root. So by(2.2.9.7) $R$ is real closed. □

Prop. (2.2.9.10) [Artin-Schreier]. If $K$ is separably closed and $F$ is a subfield of finite index in $K$, then $F = K$ or $F$ is real closed and $K = F(i)$.

Proof: Cf.[Lan05]P299.

Real Fields and Order

Prop. (2.2.9.11) [Real Field and Order]. If $R$ is a real field, then it is orderable, in fact, if $-a$ is not a sum of squares in $F$, then there is an ordering that $a > 0$. So a real field is equivalent to an orderable field.

Proof: By(2.2.9.2), $F(\sqrt{a})$ is real, so it has a real closure(2.2.9.4) and has the induced order(2.2.9.5), and $a > 0$ because it is a square(2.2.8.2). □

Prop. (2.2.9.12) [Existence and Uniqueness of Real Closure]. For any ordered field $F$, there is a unique real closure $R$ of $F$ that every positive element of $F$ is a square in $R$, thus the ordering is compatible.

Proof: The existence is by adding all the square roots of elements> 0 to $F$, the resulting field is real closed because of(2.2.9.2) and the fact a union of real fields(2.2.9.2) is real.

The uniqueness: because an ordered field is of char0(2.2.8.2), so the primitive element theorem(2.2.5.20) applies that each finite subextension of $R_0$ is of the form $F(\alpha)$, where $\alpha$ is a root of an irreducible separable polynomial $f$. Then the roots of $f$ are different so can be ordered $\alpha_1 < \ldots < \alpha_n$. Similarly, $f$ has the same number of different roots in $R_1 \beta_1 < \ldots < \beta_n$ by(2.2.9.14), so there is a map $h: \alpha_i \to \beta_i$, and it is the unique map that a ordered map from $F(\alpha)$ to $R_1$ extending id on $F$ can be. it is this uniqueness that makes us able to use Zorn’s lemma to show that there is a maximal ordered map, must be a map from $R_0$ to $R_1$, which is an isomorphism, by primitive element theorem again. □

Prop. (2.2.9.13) [Sturm’s Algorithm]. Cf.[Model Theory Marker P327].
Cor. (2.2.9.14). If $F$ is an ordered field and $R_0, R_1$ be two real closure of $F$ that is compatible with the ordering, then any irreducible polynomial has the same number of roots in $R_0$ and $R_1$.

Proof: Cf.[Model Theory Marker P328].

Prop. (2.2.9.15)[Hilbert’s 17th Problem]. If $f$ is a positive semidefinite rational function over a real closed field $F$, then $f$ is a sum of squares of rational functions.

Proof: Let $f(X_1, \ldots, X_n)$ be a positive semidefinite rational function, if $f$ is not a sum of squares of rational functions, then by (2.2.9.11), there is an ordering on $F(X)$ that $f < 0$. Let $R$ be a real closure of $F(X)$, then $R \models \exists \bar{v} F(\bar{v}) < 0$, as $F(X) < 0$. But $RCR$ is complete, by (1.2.7.6), thus $F \models \exists \bar{v} F(\bar{v}) < 0$ also, contradiction.
2.3 Linear Algebra

Main references are [H-K71], [线性代数 谢启鸿], [Rom07] and [Determinant, 高等代数 notes, 安金鹏].

In this section, the category of vector spaces over a field $k$ is studied, without considering any topology on $K$ or $V$. More generally, the category of free modules over a commutative unital ring $R$ is studied.

Def. (2.3.0.1) [Notations]. Throughout this section, $k$ denote a field.

1 Basics

Def. (2.3.1.1) [Vector Spaces].

Def. (2.3.1.2) [Linear Operators]. A linear operator on a $R$-module $V$ is an element of the endomorphism ring $\text{End}_R(V)$

Def. (2.3.1.3) [Basis]. Let $R$ be a field, then the sets $S$ that are linearly independent over $R$ has maximal objects by Zorn’s lemma, and such a maximal object must span $M$, called a basis of $M$.

Prop. (2.3.1.4) [Dimension]. All basis of a linear $k$-vector space $V$ have the same cardinality, this cardinality is called the dimension $\dim_k(V)$ of $V$. This follows immediately from (2.2.4.4).

Prop. (2.3.1.5) [Canonical way of Writing a Basis]. After so many years, I still find it confusing to write a basis and observing change of basis, so I will write it here:

A vector should always be written vertically, and so a basis should be $\overrightarrow{e} = (e_1, \ldots, e_n)(\text{horizontal})$, and a vector with basis $\overrightarrow{d}$ (vertical) is in fact $\overrightarrow{e} \overrightarrow{d}$.

A change of basis should be written $\overrightarrow{e}' = ea$, with $a \in GL_n$, and then if an operator has matrix $A$ w.r.t. the basis $\overrightarrow{e}$, it then map in the basis $\overrightarrow{e}' v = \overrightarrow{e}' x = \overrightarrow{e} a x \mapsto \overrightarrow{e} Aax = \overrightarrow{e} a^{-1} Aax$, so it has matrix $a^{-1} Aa$ w.r.t the basis $\overrightarrow{e}'$.

Prop. (2.3.1.6) [Extension of Basis].

Proof: \hfill \Box

Prop. (2.3.1.7). Let $F$ is a subfield of $K$ and $U$ is a $K$-vector space with a $F$-subspace $U'$. Then if every finite $F$-linearly independent subset of $U'$ is $K$-linearly independent, then $\dim_F(U') \leq \dim_K(U)$.

Proof: If the converse is true, there is a $F$-basis $u_j'$ of $U'$, then some of $u_j'$ is $K$-linearly dependent, contradiction. \hfill \Box

Def. (2.3.1.8) [Matrices]. Let $R$ be a commutative ring, the set of matrices of size $m \times n$ over $R$ is an (non-commutative) algebra $M_{m \times n}(R)$ over $R$ whose underlying module is $R^\otimes_{n2} = \oplus_{1 \leq i \leq m, 1 \leq j \leq n} e_{ij} R$, and the algebra structure is given by

$e_{ij} e_{ij} = e_{ik}$.

An element $A = \sum_{1 \leq i \leq m, 1 \leq j \leq n} a_{ij} e_{ij} \in M_{m \times n}(R)$ is denoted by $A = (a_{ij})$. 
Prop. (2.3.1.9). $A, B$ are two $n \times n$-matrices, if $1 - AB$ is invertible, then so does $1 - BA$, and
\[(1 - BA)^{-1} = 1 + B(1 - AB)^{-1}A.\]

Proof: Immediate from (2.2.1.5) or (2.3.10.12).

Cor. (2.3.1.10). $AB$ and $BA$ has the same characteristic polynomials.

Prop. (2.3.1.11). For a ring $R$, there is an isomorphism of rings
\[M_n(R) \cong M_n(R^{op}).\]

The isomorphism is given by $A \mapsto A^t$.

Def. (2.3.1.12) [Notation for Matrix Group]. Let $R$ be a ring, denote
- $GL(n, R)$ be the subgroup of $\text{End}_R(\oplus R^\oplus n)$ consisting of invertible matrices.
- $SL(n, R)$ be the subgroup of $GL(n, R)$ consisting of matrices of determinant 1 (2.3.10.1).
- $U_n(R)$ be the subgroup of $GL(n, R)$ consisting of upper-triangular matrices.
- $P_n(R)$ be the subgroup of $GL(n, R)$ consisting of matrices $A = (a_{ij})$ that $a_{ni} = 0$ for $i < n$.
- $Q_n(R)$ be the subgroup of $GL(n, R)$ consisting of matrices $A = (a_{ij})$ that $a_{ni} = 0$ for $i < n$ and $a_{nn} = 1$.

Prop. (2.3.1.13). Let $K$ be a topological field, there is a decomposition of spaces
\[U_n(K) \setminus GL(n, K) \cong GL(1, K) \times U_2(K) \setminus GL(2, K) \times \ldots \times Q_n(K) \setminus GL(n, K)\]
where $GL(n - 1, K)$ embeds $GL(n, K)$ obviously.

Remark (2.3.1.14). This is wrong.

Proof: By induction, it suffices to show
\[U_n(K) \setminus GL(n, K) \times U_{n-1}(K) \setminus GL(n-1, K) \times Q_n(K) \times GL(n, K).\]
Consider the map $GL(n - 1, K) \times GL(n, K) \to U_n(K) \setminus GL(n, K) : (x, y) \mapsto xy$, then $x_1y_1 = x_2y_2$ iff $x_1y_1 = ux_2y_2$ for some $u \in U_n(K)$, iff $y_1y_2^{-1} = x_1^{-1}ux_2$. This is possible iff $y_1y_2^{-1} \in Q_n$, and for all $(y_1, y_2)$ that $y_1y_2^{-1} \in Q_n$, $x_1y_1 = ux_2y_2$ iff $x_1 = ux_2y_2y_2^{-1}$. □

2 Rank

Prop. (2.3.2.1) [Rank Nullity Theorem]. Let $T : V \to W$ be a linear map between vector spaces, then rank$(T) + \dim \text{Nul}(T) = V$.

Proof: This follows from the exact sequence $0 \to \ker(T) \to V \to \text{Im}(T) \to 0$. □

Prop. (2.3.2.2) [Row Rank equals Column Rank]. The row rank of a $m \times n$ matrix $A$ is the same as the column rank.

Proof: Let $A$ be the matrix of a linear map $T : V \to W$, then column rank equals the range of $T$, and the row rank equals the range of $T^t$, so they are equal by (2.3.3.7). □
Prop. (2.3.2.3) [Sylvester’s Inequality]. For $U$ a $m \times n$ matrix and $V$ a $n \times k$ matrix,

$$\text{Rank}(UV) \geq \text{Rank}(U) + \text{Rank}(V) - n$$

Proof: This comes from $\dim \ker fg \leq \dim \ker f + \dim \ker g$, which is because $\ker fg = g^{-1}(\ker f)$.

Prop. (2.3.2.4) [Finite Field General Linear Group]. Over finite field $\mathbb{F}_p$, $|GL_n(\mathbb{F}_p)| = (p^n - 1)(p^n - p)\ldots(p^n - p^{n-1})$.

Proof: This is because choose the rows are equivalent to choosing a basis for $V = \oplus_{i=1}^n \mathbb{F}_p$, and when choosing $n$-th row, it suffices to avoid an element in the span of the first $n - 1$ rows.

Prop. (2.3.2.5) [Wedge and Rank]. Let $T : V \to V'$ be a linear map, then $\wedge^k(T) = 0$ iff $\text{rank}(T) < k$.

Proof: If $\text{rank}(T) < k$, then $\text{Im}(\wedge^k(T)) \subset \wedge^k \text{Im}(T) = 0$. Conversely, if $\text{rank}(T) \geq k$, choose $\{Te_1, \ldots, Te_k\}$ linearly independent, then $T(e_1 \wedge \ldots \wedge e_k) = Te_1 \wedge \ldots \wedge Te_k \neq 0$.

3 Dual spaces

Def. (2.3.3.1) [Dual Spaces]. Let $V$ be a vector space over a field $k$, the set of linear functionals on $V$ with value in $k$ form another vector space, which is denoted by $V^*$, called the dual space of $V$.

Def. (2.3.3.2) [Annihilator]. Let $V$ be a vector space and $W \subset V$ a subspace, then the annihilator $W^\perp$ is the subspace of $W^*$ consisting of linear functionals $l$ on $V$ s.t. $l(W) = 0$.

Def. (2.3.3.3) [Dual Basis]. Let $V \in \text{Vect}_k$ and $(e_1, \ldots, e_n)$ is a basis of $V$, then there exists unique elements $\alpha_1, \ldots, \alpha_n$ of $V^*$ s.t. $(e_i, \alpha_j) = \delta_{ij}$. Any such elements $\alpha_1, \ldots, \alpha_n$ constitute a basis for $V^*$, and is called the dual basis of $(e_1, \ldots, e_n)$.

Prop. (2.3.3.4) [Dimension of the Annihilator]. Let $W \subset V$ be f.d. vector spaces, then $\dim W + \dim W^\perp = \dim V$.

Proof: Let $\{e_1, \ldots, e_k\}$ be a basis of $W$ and extend it to a basis $\{e_1, \ldots, e_k, e_{k+1}, \ldots, e_n\}$ of $V$ by (2.3.1.6). Consider the dual space $e_1^*, \ldots, e^*_n$, then the annihilator of $W$ is just span$\{e_{k+1}^*, \ldots, e^*_n\}$. Thus $k + (n - k) = n = \dim V$.

Def. (2.3.3.5) [Transpose]. Let $T : V \to W$ be a linear map of f.d. vector spaces, then $T$ induces a map $T^t : W^* \to V^*$ given by $T^t(l) = l \circ T$. This is a linear map, called the transpose of $T$.

Prop. (2.3.3.6) [Adjoint Map and Transpose]. Let $T : V \to W$ be a linear map of f.d. vector spaces, such that w.r.t. a basis $\{e_1, \ldots, e_n\}$ of $V$ and $\{f_1, \ldots, f_m\}$ of $W$, $T$ is given by matrix $A = (a_{ij})$. Then w.r.t. the dual basis $\{f_1^*, \ldots, f^*_m\}$ of $W^*$, $\{e_1^*, \ldots, e^*_n\}$ of $V^*$, the transpose map (2.3.3.5) $T^t : W^* \to V^*$ is given by the a matrix $A^t = (b_{ij})$, where $b_{ij} = a_{ji}$. $A^t$ is called the transpose matrix of $A$.

Proof: $(e_j, T^t(f^*_i)) = \langle Te_j, f^*_i \rangle = a_{ji}$, thus $b_{ij} = a_{ji}$.

Prop. (2.3.3.7) [Transpose Range Nullity Duality]. Let $f : V \to V'$ be a linear map between f.d. vector spaces over a field $k$, then

- $\text{rank}(T^t) = \text{rank}(T)$. 

• The range of $T^t$ is the annihilator of the null space of $T$.

Proof: 1: Notice that $T^t(g) = 0$ iff $\langle g, T(v) \rangle = 0$ for any $v \in V$, thus the null space of $T^t$ is just the annihilator of the range of $T$, which equals $\dim(V' - \text{rank}(T))$ by (2.3.3.4). But this space has dimension $\dim \ker(T^t) = \dim V' - \text{rank}(T')$, so $\text{rank}(T) = \text{rank}(T^t)$.

2: This follows from the fact that $(T^t)^t = T$ and the argument above. □

Cor. (2.3.3.8). A linear map between f.d. vector spaces is surjective iff its transpose is injective.

Prop. (2.3.3.9) [Infinite Dual space]. If $\dim_K V$ is not finite, then $\dim_K V < \dim_K V^*$.

Proof: Notice $\text{Hom}(\oplus_{i \in I} K e_i, K) = \prod K e_i^*$.

We prove first that if $|K|$ is at most countable, then $|V| = |I|$. Notice the set $S_n(I)$ of all $n$-element subsets of $I$ is of the same cardinality of $I(1.1.5.3)$. And the finite sums of $K$ and $e_i$ can be seen as a subset of $S_n(I) \times K^n$, so it has the same cardinality of $I$.

Now we can prove if $|K|$ is at most countable, then $\dim V < \dim V^*$. This is because $V^*$ equals the functions from $V$ to $K$, which is bigger than the functions from $V$ to $\{0, 1\}$, which is the power set of $V$, so having cardinality $2^{|V|}$ which is bigger than $|V|$, by Cantor theorem (1.1.2.12).

Now generally, $K$ is not countable, but it has a base field $F$, which is countable, so we consider the $F$-vector space $W = \oplus_{i \in I} F e_i$, then $\dim_F W = \dim_K V$, and $\dim_F W < \dim_F W^*$. If we can show $\dim_F W^* \leq \dim_K V^*$, then we are done.

For this, first consider the natural $F$-linear mapping $W^* \to V^*$, which is clearly an imbedding. Now we want to use (2.3.1.7), so we check the conditions, for $F$-linearly independent $\varphi_1, \ldots, \varphi_n$, if $\sum c_i \varphi_i = 0$, $c_i \in K$, then if we can find $w_k \in W$ that $\varphi_i(w_j) = \delta_{ij}$, then this is a contradiction. But this is true, by a simple argument, using the $F$-linearity of $F$. □

4 Rational Form and Jordan Form

Prop. (2.3.4.1) [Elementary and Invariant Factors]. A linear operator in $L(V)$ is equivalent to a $K[X]$-module structure on $V$, and two operators are similar iff the module structure are isomorphic.

As $K[X]$ is a PID, the elementary factors, invariant factors, cyclic and elementary decomposition theorems (2.2.4.22) can be applied to the case.

Proof: Cf. [Advanced Linear Algebra P168]. □

Cor. (2.3.4.2) [Jordan Forms].

• For a matrix over an alg.closed field, it is similar to a matrix of blocks $\lambda_i I + N, N x_i = x_i + 1$, called the Jordan form.

• For a real matrix, it is similar to a matrix of blocks of the above form together with $\begin{bmatrix} a & -b \\ b & a \end{bmatrix}$ on the diagonal and $I_{2 \times 2}$ on the lower side.

Proof: 1: Over an alg.closed field, the elementary factors are all of the form $(x - c_i)^{m_{ij}}$. Now in the basis $v, (T - c_i)v, \ldots, (T - c_i)^{m_i - 1}v$, the matrix is just the Jordan form.

2: Over $R$, the elementary factors are all of the form $(x - c_i)^{m_{ij}}$ and $((x - a)^2 + b^2)^{m_{ij}}$. Then complexify it and consider a cyclic vector $v$, for $(T - (a + bi)I)$, let $v_{n+1} = (T - (a + bi)I) v_n$, and let $v_n = X_n + iY_n$, then it can be verified that $T$ is of the Jordan form given in the basis $X_i, Y_i$. □
Def. (2.3.4.3) [Companion matrix]. The companion matrix for a monic polynomial \( p(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_0 \in F[X] \) is the matrix

\[
T_{p(x)} = \begin{bmatrix}
0 & 0 & \cdots & 0 & -a_0 \\
1 & 0 & \cdots & 0 & -a_1 \\
0 & 1 & \ddots & \vdots \\
\vdots & \vdots & \ddots & 0 \\
0 & 0 & \cdots & 1 & -a_{n-1}
\end{bmatrix}
\]

Prop. (2.3.4.4) [Companion Matrix is Nonderogatory]. An operator is cyclic iff it is similar to a companion matrix.

A companion matrix is nonderogatory (2.3.5.2). In fact, the minimal polynomial and the maximal polynomial of the companion matrix of \( p(X) \) are both \( p(X) \).

Proof: The operator of the companion matrix is an operator \( A \) with a basis \( \{ v, Av, A^2v, \ldots, A^{n-1}v \} \) and \( A^nv = -\sum_{i<n} a_i A^i v \), which just equivalent to the fact the action of \( A \) is cyclic.

The determinant of \( T_{p(X)} \) equals \( p(X) \) by (2.3.4.13), and for the minimal polynomial, in the basis of \( \{ v, Av, A^2v, \ldots, A^{n-1}v \} \), clearly for a polynomial \( f(X) \) of degree \( m < n \), \( f(A)v \neq 0 \), and \( p(A)v = \sum_{i<n} a_i A^i v + A^nv = 0 \). So the minimal polynomial of \( A \) is \( p(X) \). \( \square \)

Prop. (2.3.4.5) [Rational Canonical Form]. Every matrix is similar to splint of companion matrices (2.3.4.3) corresponding to its elementary divisors.

Prop. (2.3.4.6) [Invariant Factor Form]. Every matrix is similar to splint of companion matrices, corresponding to its invariant factors.

Computing the Invariant Factors

Def. (2.3.4.7) [Elementary Row Operation]. An elementary row operation for a matrix \( M \) over an algebra \( A \) is one of the following:

- Multiplying one row of \( M \) by a non-zero scalar in \( A \).
- plus the \( r \)-th row by \( c \)-times the \( s \)-th row, where \( c \) is invariant \( A \).

And an elementary matrix is a matrix obtained by the identity matrix by an elementary row operation.

Two matrix is called row equivalent iff they can be connected by f.m. elementary row operations, and this is equivalent to \( M = PN \), where \( P \) is a product of f.m. elementary matrices, because left multiplication by an elementary matrix is equivalent to an elementary row operation.

Similarly we can define elementary column operations.

Lemma (2.3.4.8). The elementary row operation change the determinant only by an invariant element in \( A \). (Clear).

Prop. (2.3.4.9). Let \( P \) be a matrix with entries in \( F[X] \), then the following are equivalent:

- \( P \) is invertible.
- The determinant is a nonzero scalar.
- \( P \) is row equivalent to identity matrix.
• $P$ is a product of elementary matrices.

Proof: The only hard part is $2 \rightarrow 3$: this is because it has determinant in $F^*$, thus the greatest common divisor of the first column is a scalar, thus we can use row operation to make it $(1, 0, \ldots, 0)'$, and then we can continue to make it a upper triangular matrix with 1 in the diagonal, and also kill the upper half part. So it is row equivalent to the identity matrix. □

Cor.(2.3.4.10). Let $M, N$ be two matrices with entries in $F[X]$, then they are equivalent iff $N = PM$ for some $P$ that has determinant in $F$.

Def.(2.3.4.11). We call $M, N$ equivalent iff $M, N$ are connected by a sequence of elementary row operations and column operations. This is equivalent to $M = PNQ$ for $P, Q$ invertible matrices in $M_n(F[X])$.

Prop.(2.3.4.12)[Normal Form of Companion Matrix]. For a monic polynomial $p(X)$, consider its companion matrix $T_p$, then the matrix $xI - T_p \in M_n(F[X])$ is equivalent to $\text{diag}(p(X), 1, \ldots, 1)$.

Proof: Clear, if one reduces the $x$ in the diagonal from the bottom row to the top row one by one. □

Cor.(2.3.4.13). For a companion matrix $A$ of $p$, $\det(xI - A) = p$.

Proof: This is from (2.3.4.8), and the fact both the side are monic polynomials. □

Def.(2.3.4.14)[Smith Normal Form]. A matrix in $M_n(F[X])$ is called a Smith normal form iff it is diagonal and diagonal entries $f_i \in F[X]$ is monic and satisfies $f_k$ divides $f_{k+1}$.

Prop.(2.3.4.15). Any matrix $M$ with entries in $F[X]$ is equivalent to a unique Smith normal form.

Proof: This is immediate from (11.6.6.7) applied to the PID $F[X]$ (2.2.3.16). □

Cor.(2.3.4.16)[Computing Invariant Factors]. The diagonal entries of the Smith form of the matrix $xI - M \in M_n(F[X])$ are just the invariant factors of $M$.

Proof: This is because of the uniqueness of Smith form (2.3.4.15) and the invariant factor (2.3.4.6) and (2.3.4.12). □

Applications

Prop.(2.3.4.17). For any two matrices $A, B \in M_{n \times n}(K)$, $(AB)^n$ and $(BA)^n$ are similar.

Proof: It suffices to show that they have the same elementary factors. Notice that for any irreducible polynomial $p$, if $p \neq x$, then if $p^k(AB)v = 0$, then $p^k(BA)Bv = 0$, if $p^k(NA)v = 0$, then $p^k(AB)Av = 0$. Thus there are maps $B : N(p^k(AB)) \rightarrow N(p^k(BA))$ and $A : N(p^k(BA)) \rightarrow N(p^k(AB))$. Now their composition are both injective, thus they have the same dimension.

And for $p = x$, these two both have nullity as the multiplicity of 0 in the charpoly of $AB, BA$ (2.3.10.13), thus the same. So they have the same elementary factors, thus similar. □

Prop.(2.3.4.18)[Matrix Similar to Transpose]. Any matrix is similar to its transpose.

Proof: This is because the invariant factors can be computed using the greatest common divisors of minors by (2.3.4.15) and (2.3.4.16), and they are clearly invariant under conjugation. □
5 Minimal and Characteristic Polynomials

Def. (2.3.5.1) [Minimal Polynomials]. The minimal polynomial of a matrix $A$ is the polynomial $p$ of minimal degree that $p(A) = 0$. It is equivalent to the maximal invariant factor of $A$, by (2.3.4.1).

Def. (2.3.5.2) [Non-derogatory Operator]. An operator is called nonderogatory iff it has only one invariant factor.

Prop. (2.3.5.3) [Generalized Cayley-Hamilton]. The characteristic polynomial of $A$ is the product of the elementary divisors of $A$, thus the characteristic polynomial and minimal polynomial (2.3.5.1) of $A$ have the same set of irreducible factors, but may not with the same multiplicity. In particular, the characteristic polynomial is divisible the minimal polynomial.

Proof: Because charpoly and minipoly are both invariant under similarity, assume $A$ is in rational form (2.3.4.5), so the result follows from (2.3.4.4). \qed

Prop. (2.3.5.4). The linear functor $X \to AX - XC$ is an isomorphism iff the minimal polynomial of $A$ and $C$ has not common factor.

Proof: Notice if $AX = XC$, then we have $P(A)X = XP(C)$ for every polynomial $P$, in, particular for the minimal polynomials of $A$ and $C$, thus $P(C)$ is non-invertible and $A, C$ has a characteristic value in common. Conversely, if they have a characteristic value, then we upper triangularize $A$ to see clearly that there is a $X$ that $AX = XC$ ($X$ has only the first row). \qed

Characteristic Polynomial Images

In this subsubsection, we consider the set of characteristic polynomials of elements in a subgroup of $GL(n, k)$ as a whole.

6 Diagonalization and Triangulation

Prop. (2.3.6.1). If a linear map has matrix form $T$ in a basis $(X_i)$ and there is another basis $(Y_i)$ that $(Y_i) = (X_i)P$, then it has matrix form $PTP^{-1}$ in the basis $(Y_i)$. In particular, if $T$ can be diagonalized, with eigenvectors $(X_i)$, then $T = (X_i)D(X_i)^{-1}$.

Prop. (2.3.6.2) [Relation with Minimal Polynomial].
- An $n \times n$-matrix $A$ is upper-triangular over a field $K$ iff its minimal polynomial is a product of linear factors.
- An $n \times n$-matrix $A$ is diagonalizable over a field $K$ iff its minimal polynomial is a product of linear factors with no multiple roots.

Proof: 1: If it is upper-triangular, its minimal polynomial is a product of factors because its characteristic polynomial does (2.3.5.3). Conversely, we can find an eigenvector for $A$, then we quotient this vector and use induction.

2: If it is diagonalizable, then the minimal polynomial is clearly polynomials. Conversely, its elementary factors are all linear factors, thus its Jordan form is just diagonal (2.3.4.2). \qed

Cor. (2.3.6.3) [Upper Triangulation Alg.Closed Field]. If $K$ is alg.closed, then any $n \times n$-matrix $A$ is upper-triangular over $K$. Similarly, it is lower-triangular.
Proof: It suffices to find a flag that is stabilized by $A$. And for this, it suffices to find an eigenvector of $A$. This is clear, as the characteristic polynomial of $A$ has a root in $K$.

Prop.(2.3.6.4) [Simultaneously Triangulable]. If $A_i$ is a commutating family of upper-triangulable $n \times n$-matrices, then they are simultaneously triangulable.

Proof: As in the proof of (2.3.6.3), by induction, it suffices to show there is a common eigenvector. Now assume there are f.m. matrices in $F$, we induct on the number of matrices to show there is an eigenvector. Let $\lambda$ be an eigenvalue of $A_1$ because it is upper-triangulable, then $N(A_1 - \lambda I)$ is invariant under $F$, and all the matrices are upper-triangulable on $N(A_1 - \lambda I)$, which is seen by intersecting the flag with $N(A_1 - \lambda I)$. So by induction, there is a common eigenvector for $F$.

Prop.(2.3.6.5) [Simultaneously Diagonalizable]. If $A_i$ is a commutating family of diagonalizable $n \times n$-matrices, then they are simultaneously diagonalizable.

If $A_i$ is a commutating family of real symmetric matrixes, then they are simultaneously orthogonally diagonalizable.

Proof: We may assume there are f.m. matrices and use induction. Consider the diagonal decomposition $V_i$ of $V$ for $A_1$, then each $V_i$ is invariant under $F$. Notice then each $A_i$ is diagonalizable on $V_i$, thus by induction, $F$ is simultaneously diagonalizable on each $V_i$, then $F$ is simultaneously diagonalizable.

For the second, induction on the numbers of matrices. If some matrix is $cI$, then clear, if some are not $cI$, then choose its eigenvalue decomposition, we conclude by induction hypothesis.

Prop.(2.3.6.6) [Invariance of Field Extension]. Let $A \in M_n(F)$, and $E$ be the subfield generated by the entries of $A$, then the invariant factors of $A$ are polynomials over $E$. In particular, two matrix are similar over the smallest field that they are defined.

Proof: Clear, because we know how an irreducible polynomial over $E$ factors through $\overline{E}$.

Prop.(2.3.6.7) [Jordan Decomposition]. Let $k$ be a perfect field and $A \in M_n(k)$, then there exists unique matrices $A_s, A_n$ that $A_s$ is semisimple, $A_n$ is nilpotent, $A = A_s + A_n$, and $A_s, A_n$ are polynomials of $A$ in particular, $A_s$ commutes with $A_n$.

Moreover, if $A$ is invertible, then there exists unique matrices $A_s, A_u$ that $A_s$ is semisimple, $A_u$ is unipotent, $A = A_s \cdot A_u$, and $A_s, A_u$ are polynomials of $A$, in particular, $A_s$ commutes with $A_u$.

Proof: If $k$ is alg.closed, then use (2.3.6.3). And Lagrange interpolation shows $A_s, A_n$ are polynomials in $A$. For the uniqueness, notice that because they are polynomials in $A$, if there are two sets of Jordan decompositions $A = A_s + A_n = A_s' + A_n'$, then $(A_s - A_{s}') = (A_n' - A_n)$, but the sum of commuting semisimple/nilpotent matrices is semisimple/nilpotent, so it is semisimple and nilpotent, so it can only be 0, so $A_s = A_{s}'$.

In general, because $k$ is perfect, taking a Galois field extension $k'/k$ containing all eigenvalues of $A$, then $A = A_s + A_n$ where $A_s, A_n$ has entries in $k'$. But then taking Galois action and using the uniqueness, $A_s, A_n$ has entries in $k$.

Finally, by the Galois action again, $A_s, A_n$ are polynomials in $A$.

If $A$ is invertible, then $A_s$ is also invertible, seen by base change to alg.closure. Then $A = A_s(1 + A_s^{-1}A_n)$, where $1 + A_s^{-1}A_n$ is unipotent.

Prop.(2.3.6.8). If $T$ is a diagonalizable operator on a subspace $V$, then for any invariant subspace $V'$, $T|_{V'}$ is also diagonalizable.

Proof: Use the eigenvalue decomposition $V = \oplus_i V_{\lambda_i}$, then $V' = \oplus_i (V_{\lambda_i} \cap V')$, which is because if $\sum v_i \in V'$, where $v_i$ are in different eigenspaces, then each $v_i \in V'$. 

\[\square\]
7 Positivity(Inner Spaces)

Def. (2.3.7.1) [Inner Spaces]. A real inner space is a f.d. real quadratic space that $B(v, v) > 0$ for $v \neq 0$. It is necessarily non-degenerate.

A complex inner space is a f.d. Hermitian space $V$ that $B(v, v) > 0$ for $v \neq 0$.

Prop. (2.3.7.2). An inner metric on a vector space will induce an inner metric on the dual space, that is, asserting the dual basis of an orthonormal basis to be orthonormal. On an arbitrary basis, the matrix on the dual basis is written as $A^{-1}$ because we can write $A = P^tP$, and the dual basis transformation is like $(P^t)^{-1}$, so the metric matrix is $A^{-1}$.

Prop. (2.3.7.3) [Positivity and Principal Minors]. A matrix is positive symmetric (Hermitian) iff it is symmetric, and all its upper principle minors has positive determinants.

A positive symmetric (Hermitian) matrix is equivalent to a real (complex) inner space.

Proof: Cf. [Hoffman P328].

Cor. (2.3.7.5) [Gordan’s Theorem]. exactly one of the following has a solution:

$\left\{\begin{array}{ll}
AX > 0 \\
Y^tA = 0, Y \geq 0, Y \neq 0
\end{array}\right.$

Proof: If both have a solution, then $0 = Y^tAX > 0$, contradiction. If the first has no solution, then $A'x = e, z \geq 0$, where $A' = [A, -A, -I]$ has no solution, by Farkas’ lemma, there is a solution of $Y^tA' \leq 0$ and $Y^tb = 0$. Which shows that $Y^tA = 0$ and $Y \neq 0$.

Cor. (2.3.7.6). For any subspace in $\mathbb{R}^m$, either it has an intersection with the open first quadrant, or its orthogonal complement has an intersection with the closed first quadrant minus 0. (Regard it has the image of a $AX$).

8 Bilinear & Hermitian Forms

Prop. (2.3.8.1) [Hermitian Forms]. A complex vector space $V$ is equivalent to a real vector space with an endomorphism $J$ that $J^2 = -1$, by $i$ acting by $J$.

A Hermitian form on $(V, J)$ is an $\mathbb{R}$-bilinear mapping $(-, -) : V \times V \to \mathbb{C}$ that satisfies

$(Ju, v) = i(u, v), \quad (u, v) = (v, u)$.

If we write $(u, v) = \varphi(u, v) - i\psi(u, v)$, then

- $\varphi$ is symmetric, $\varphi(Ju, Jv) = \varphi(u, v)$.
- $\psi$ is alternating, $\psi(Ju, Jv) = \psi(u, v)$. 
• \( \psi(u,v) = -\varphi(u,Jv), \varphi(u,v) = \psi(u,Jv) \).

Conversely, if \( \varphi \) satisfies this condition, then

\[
(u,v) = \varphi(u,v) + i\varphi(u,Jv).
\]

is a Hermitian form. Also \((-,-)\) is positive or non-singular iff \( \varphi \) is.

**Lemma (2.3.8.2).** Any eigenvalue of a Hermitian (e.g., real symmetric) matrix \( M \) is real.

**Proof:** Consider the bilinear form defined by the matrix \( M \), then if \( x \) is an eigenvector with eigenvalue \( \lambda \), then \( \lambda(x,x) = (Hx,x) = (x,Hx) = \overline{\lambda}(x,x) \), so if \( \lambda \) is not real, \( x = 0 \).

**Prop. (2.3.8.3) [Principal Axis Theorem].** A symmetric matrix \( A \) is orthogonally diagonalizable. Similarly, a Hermitian matrix is unitarily diagonalizable.

**Proof:** Firstly, we can find an eigenvector of \( A \): Only the real case needs proof, and this is because any eigenvalue of \( A \) is real (2.3.8.2).

Let \( v \) be an eigenvector of \( A \) of length 1, then the orthogonal complement of \( v \) is preserved by \( A \), so we can use induction to find an orthonormal basis consisting of eigenvectors of \( A \), then these together with \( v \) forms an orthonormal basis consisting of eigenvectors of \( A \).

**Prop. (2.3.8.4) [Complex Normal operators].** More generally, a normal operator over \( \mathbb{C} \) is unitarily diagonalizable using resolution of identity (10.8.4.3) because the spectrum are discrete thus the point projection is orthogonal.

**Prop. (2.3.8.5) [Gram-Schmidt].** Any symmetric matrix over fields of characteristic \( \neq 2 \) is congruent to a diagonal matrix.

**Proof:** Any symmetric matrix defines a bilinear form on \( V \). If \( B \) is not identically 0, then there is a \( x \) that \( x^tBx \neq 0 \), by polarization identity. Then \( W = \{Kx\} \) is non-degenerate, so we have \( W \oplus W^\perp = V \) by (12.3.1.8). And by induction, we are done.

**Prop. (2.3.8.6) [Antonne-Takagi].** For any complex symmetric matrix \( A \), there is unitarily matrix \( U \) that \( UAU^t \) is a real diagonal matrix with non-negative entries.

**Proof:** Consider \( B = A^*A \) is Hermitian and positive-semi-definite, thus there is a unitary matrix \( V \) that \( V^*BV \) is diagonal with non-negative real entries by (2.3.8.3). Now \( C = V^tAV \) is complex symmetric with \( C^*C \) real diagonal. If we let \( C = X + iY \), then \( XY = YX \). So by (2.3.6.5), there is a real orthogonal matrix \( W \) that \( WXW^t \) and \( WYW^t \) are diagonal. Now set \( U = VW^t \), which is unitary, \( UAU^t \) is complex diagonal. And easily we can modify the diagonal entries to be non-negative.

**Prop. (2.3.8.7) [Skew-Symmetric Forms].** For any f.d. skew-symmetric vector space \( V \) over a field \( k \) with \( \text{char} \ k \neq 2 \), then there exists a basis \( \{x_1, \ldots, x_r, y_1, \ldots, y_r, z_1, \ldots, z_k\} \) s.t. \( (x_i, y_i) = -(y_i, x_i) = 1 \), and the inner product of other pairs in this basis vanish. In particular, if \( V \) is non-degenerate, then \( \dim V \) is even.

**Proof:** Use induction on \( \dim V \). If \( \dim V = 0 \), this is clear. For \( \dim V > 0 \), if there exists a pair \( (x,y) \neq 0 \), then we can take \( (x,y) = 1 \), and we can look at the complement \( \{x,y\}^\perp \subset V \) and use induction.
Prop. (2.3.8.8). Given a bilinear form on a field, the relation of orthogonality is symmetric iff it is symmetric or alternating, i.e. $B(x, x) = 0$.

Proof: Let $w = B(x, z)y - B(x, y)z$, then $B(x, w) = 0$, hence we have $B(w, x) = 0$, that is

$$B(x, z)B(y, x) - B(x, y)B(z, x) = 0.$$  

Let $z = x$, then $B(x, x)[B(x, y) - B(y, x)] = 0$.

If some $B(u, v) \neq B(v, u)$ and $B(w, w) \neq 0$, then $B(u, u) = B(v, v) = 0, B(w, v) = B(v, w), B(w, u) = B(u, w)$. Let $x = u$ or $v$ se get $B(w, v) = B(v, w) = 0 = B(w, u) = B(u, w)$. Now $B(u, w + v) \neq B(w + v, u)$, hence $B(w + v, w + v) = 0 = B(w, w)$, contradiction. $\square$

Prop. (2.3.8.9). If $B$ is a non-degenerate bilinear form on an associative algebra $V$, choose a basis $x_i$ of $V$, then choose a dual basis $y_i$, then $\sum x_i \otimes y_i \in T(V)$ is independent of $x_i$ chosen.

Proof: Let $V^\vee$ be the dual of the vector space $V$. There is an isomorphism $V \otimes V^\vee \cong \text{End}(V)$ given by mapping $(v, f)$ to the operator $v' \mapsto f(v')v$. The non-degenerate bilinear form induces naturally an isomorphism $\beta : V \cong V^\vee : v \mapsto (., v)$. Then under the isomorphisms

$$\text{End}(V) \cong V \otimes V^\vee \cong V \otimes V,$$

where the second isomorphism is $(\text{id}_V, \beta^{-1})$. The identity map $\text{id}_V \in \text{End}(V)$ is send to $\sum x_i \otimes y_i \in T(V)$, so $\sum x_i \otimes y_i$ is independent of the basis chosen. $\square$

Symmetric Bilinear Forms

For symmetric bilinear forms and more about quadratic forms, see 12.3.

Real Spectral Theory

Remark (2.3.8.10). The general spectral theory applies to this case.

Prop. (2.3.8.11). For a normal operator $N$ on a real inner product space, $N\alpha = 0$ iff $N^t\alpha = 0$. In particular, $N$ and $N^t$ has the same number of eigenvalues and dimension of eigenspaces.

Proof: This is because

$$(N\alpha, N\alpha) = (N^tN\alpha, \alpha) = (NN^t\alpha, \alpha) = (N^t\alpha, N^t\alpha).$$  

$\square$

Cor. (2.3.8.12). For a normal operator $N$ on a real inner product space, $\text{Im}(N) = \ker(N)^\perp$.

Proof: $\text{Im}(N) = \ker(N^*) = \ker(N)$. $\square$

Cor. (2.3.8.13). For a normal operator $N$ on a real inner product space, if $N^2\alpha = 0$, then $N\alpha = 0$.

Proof: This is because $N\alpha \in \ker(N) \cap \text{Im}(N) = \emptyset$. $\square$

Lemma (2.3.8.14). If $f, g$ are relatively prime polynomials and $T$ is a normal operator, $f(T)\alpha = 0$ and $g(T)\beta = 0$, then $\alpha$ is orthogonal to $\beta$.  

$\square$
Proof: Choose polynomials $a, b$ that $af + bg = 1$, then $\alpha = b(T)g(T)\alpha$, and
\[(\alpha, \beta) = (b(T)g(T)\alpha, \beta) = (b(T)\alpha, g(T)^*\beta)\]
Notice $g(T)$ is also normal, and $g(T)\beta = 0$, thus by (2.3.8.11) $g(T)^*\beta = 0$. Thus $\alpha, \beta$ are orthogonal. $\square$

**Lemma (2.3.8.15).** Let $V$ be a real inner product space and $S$ an operator that $S^2 = -1$. Suppose $\alpha \in V$ and $S\alpha = -\beta$, then
\[
S^*\alpha = \beta, \quad S^*\beta = -\alpha,
\]
$\alpha, \beta$ are orthogonal, and $||\alpha|| = ||\beta||$.

**Proof:** Because $\alpha, \beta$ are orthogonal, and $\alpha \perp \beta$, and $S\alpha = -\beta$. Let $V = \ker(p_1(T))$, then $V$ is invariant under $T$, and $W = \sum V_j$ is orthogonal to $W_j$ by (2.3.8.14).

The restriction of $T$ on $W_i$ has minimal polynomial $p_i$. If $p_i$ has degree 1, then $T$ is a scalar on $W_i$. If $p_i$ has degree 2, then $p_i = (x - a)^2 + b^2$ for some $a, b \in \mathbb{R}, b \neq 0$. Then we choose a maximal $k$ that there exists subspaces $V_j \in W_i, j \leq k$ that
- $\dim V_j = 2$.
- $V_j$ are pairwise orthogonal.
- $V_j$ is invariant under $T, T^*$, and $T|_{V_j}$ is orthogonal congruent to $\begin{bmatrix} a_i & b_i \\ -b_i & a_i \end{bmatrix}$.

Then denote $W = \bigoplus_{j=1}^k V_j$, we prove that $W = V$: Suppose not, then $W^{\perp} \neq 0$ is invariant under $T$ and $T^*$. Denote $S = b^{-1}(T - a)$, then $S^2 + 1 = 0$. Let $\alpha \neq 0 \in W^{\perp}$, then $S\beta = -S\alpha$, then $S\alpha = \alpha, \alpha, \beta \in W^{\perp}$. Since $T = aI + bS$, we have
\[
T\alpha = a\alpha - b\beta, \quad T\beta = b\alpha + a\beta.
\]
Now lemma (2.3.8.15) implies $\{\alpha, \beta\}$ is invariant under $S, S^*$ thus also $T, T^*$, so this gives another $V_{k+1}$, contradiction. $\square$
Cor. (2.3.8.17) [Unitary Equivalence of Normal Operators]. Let $T, T'$ be real (complex) normal matrices, then $T$ is orthogonally (unitarily) congruent to $T'$ iff $T$ and $T'$ have the same characteristic polynomial.

Proof: This follows from (2.3.8.16) (or (2.3.8.4)). □

Cor. (2.3.8.18) [Complex Structure Form]. A real normal matrix $J$ s.t. $J^2 + 1 = 0$ is orthogonal congruent to $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}_n$.

In particular, as such $J$ is equivalent to a complex structure on $\mathbb{R}^n$, so the set of complex structures is bijective to $O(n)/U(\frac{n}{2})$ thus can be endowed with a structure of a homogenous space.

Proof: This is because $J$ and $\begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}_n$ are both normal and they have the same characteristic polynomial, by (2.3.5.3). □

Def. (2.3.8.19) [Cayley-transformation]. For a field $k$ of char $k \neq 2$ and a matrix $P \in M_n(k)$ that has no eigenvalue $-1$, there is a Cayley transformation $A = \frac{1 - P}{1 + P}$. $1 + A$ is invertible, and

$$P = \frac{1 - A}{1 + A}.$$

Then $A$ is skew-symmetric iff $P$ is orthogonal.

Proof: If $Av = -v$, then $v - Pv = -v - Pv$, so $2v = 0$, so $v = 0$. So $A + 1$ is invertible.

If $P$ is orthogonal, then $A^t = \frac{1 - P^t}{1 + P^t} = \frac{1 - P^{-1}}{1 + P^{-1}} = -A$. Conversely, if $A^t = -A$, then $P^t = \frac{1 + A}{1 - A} = P^{-1}$. □

Prop. (2.3.8.20). If char $k \neq 2$ and $P$ is an orthogonal matrix of odd dimension, then det $P$ is an eigenvalue of $P$.

Proof: multiplying by $-1$, we can assume det $P = -1$. Consider the Cayley transformation (2.3.8.19), then

$$\text{det } P = \text{det}(1 - A) \text{det}(1 + A)^{-1} = \text{det}(1 - A)^t \text{det}(1 + A)^{-1} = 1.$$

Contradiction. □

Hermitian Spaces

Def. (2.3.8.21) [Hermitian Space]. Let $E$ be a field, $F$ a Galois extension of $E$ of degree 2 with involution $x \mapsto \overline{x}$ or $E \oplus E$ with involution $(x, y) = (y, x)$.

Then a Hermitian space over $F/E$ is a free $F$-module $V$ with a $E$-map $(\cdot, \cdot) : V \times V \to F$ s.t.

- $(cx, y) = (x, cy) = c(x, y)$ for $c \in F$.
- $(x, y) = (y, x)$.
- the pairing is non-degenerate.

Def. (2.3.8.22) [Hermitian Transpose]. Let $L : V \to W$ be a map between Hermitian spaces, then there is a Hermitian transpose $F$-anti-linear map $L^* : W^* \to V^*$ that satisfies

$$(Lu, w) = (u, L^* w).$$

As the pairing on $V$ is non-degenerate, this is map is uniquely determined.
Def. (2.3.8.23) [Hermitian Matrix]. A Hermitian matrix is a matrix $A \in M_{n \times n}(F)$ that satisfies $A^t = \overline{A}$.

Prop. (2.3.8.24) [Gram Matrix]. Let $V$ be a $n$-dimensional vector space with a canonical basis $e_1, \ldots, e_n$, then a $n \times n$ symmetric (Hermitian) matrix $M$ defines a bilinear (sesqui-linear) form $B$ on $V$ by $(x, y) \mapsto x^t My(x^t My)$. Conversely, for any bilinear (sesqui-linear) form $B$ on $V$, let $M = (a_{ij})$ where $a_{ij} = (e_i, e_j)$, then $M$ is symmetric (Hermitian) matrix, called the Gram matrix of $B$.

so we will interchange freely between a symmetric (Hermitian) matrix and a bilinear (sesqui-linear) form on $V$.

Proof: Trivial. □

9 Tensor Algebras

Def. (2.3.9.1) [Tensor Algebras]. The tensor product and tensor algebras of modules are defined in (2.2.4.13) and (4.1.1.20). In this subsection, we focus on tensor algebras of vector spaces.

Def. (2.3.9.2) [Symmetrized Tensors]. Let $V$ be a vector field over a field of characteristic 0, for any $n$, we define a multilinear map

\[ V^n \rightarrow T^n(V) : (v_1, \ldots, v_n) \mapsto \frac{1}{n!} \sum_{\sigma \in S_n} v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(n)}. \]

and descends to a linear map $\sigma : S^n(V) \rightarrow T^n(V)$, called the symmetrizer. Elements in $\text{Im}(\sigma) = \tilde{S}^n(V)$ is called symmetrized tensors.

Then $\sigma^2 = \sigma$, and $\ker(\sigma) = I \cap T^n$, where $I = \ker(T(V) \rightarrow \text{Sym}(V))$. In particular,

\[ T^n(V) = \tilde{S}^n(V) \oplus (T^n(V) \cap I). \]

Proof: $\sigma^2 = \sigma$ is easy. So $V = \text{Im}(\sigma) \oplus \ker(\sigma)$. Now $T^n(V) \cap I \subset \ker(\sigma)$, and because $\text{Im}(\sigma) \rightarrow S^n(V)$ is surjective, $T^n(V) \cap I = \ker(\sigma)$. □

Def. (2.3.9.3) [Anti-Symmetrized Tensors]. Let $V$ be a vector field over a field of characteristic 0, for any $n$, we define a multilinear map

\[ V^n \rightarrow T^n(V) : (v_1, \ldots, v_n) \mapsto \frac{1}{n!} \sum_{\sigma \in S_n} \text{sgn}(\sigma)v_{\sigma(1)} \otimes \cdots \otimes v_{\sigma(n)}. \]

and descends to a linear map $\tau : \wedge^n(V) \rightarrow T^n(V)$, called the anti-symmetrizer. Elements in $\text{Im}(\tau) = \tilde{\wedge}^n(V)$ is called anti-symmetrized tensors.

Then $\tau^2 = \tau$, and $\ker(\tau) = I \cap T^n$, where $I = \ker(T(V) \rightarrow \wedge(V))$. In particular,

\[ T^n(V) = \tilde{\wedge}^n(V) \oplus (T^n(V) \cap I). \]

Proof: $\tau^2 = \tau$ is easy. So $V = \text{Im}(\sigma) \oplus \ker(\sigma)$. Now $T^n(V) \cap I \subset \ker(\sigma)$, and because $\text{Im}(\sigma) \rightarrow S^n(V)$ is surjective, $T^n(V) \cap I = \ker(\sigma)$. □
10 Determinant and Trace

Def. (2.3.10.1)[Determinant]. For a linear operator $T \in L(V)$, as $\dim \wedge^n V^* = 1$, the determinant $\det(T) \in R$ is defined by $\wedge^n (T^t) = \det(T) \cdot \text{id}_{\wedge^n V^*}$. That is: $L(T\alpha_1, \ldots, T\alpha_n) = \det TL(\alpha_1, \ldots, \alpha_n)$. And the determinant of a matrix is defined by the linear operator it associates in a canonical basis.

Prop. (2.3.10.2)[Properties of Determinants].
1. $\det(\text{id}_V) = 1$.
2. $\det(UV) = \det U \cdot \det V$.
3. $T$ is invertible iff $\det T$ is invertible, in which case $\det(T^{-1}) = (\det T)^{-1}$.
4. If $\{\alpha_1, \ldots, \alpha_n\}$ is a basis for $V$, and $f_i$ is its dual basis, then $\det T = f_1 \wedge \ldots \wedge f_n(T\alpha_1, \ldots T\alpha_n)$.

Proof: All these are not hard. □

Cor. (2.3.10.3). $\det(P^{-1}AP) = \det(A)$.

Prop. (2.3.10.4). $\det T = \det T^t$.

Proof: Use (2.3.10.2), if $\{\alpha_1, \ldots, \alpha_n\}$ is a basis for $V$, and $f_i$ is its dual basis, then $\det T^t = f_1 \wedge \ldots \wedge f_n(T^t f_1, \ldots, T^t f_n) = f_1 \wedge \ldots \wedge f_n(T \alpha_1, \ldots T \alpha_n) = \det T$ □

Prop. (2.3.10.5)[Expansion of Determinants]. If $A_i$ be the $i$-th column of $A$, then $\det A = f_1 \wedge \ldots \wedge f_n(A \varepsilon_1, \ldots, A \varepsilon_n) = f_1 \wedge \ldots \wedge f_n(A_1, \ldots, A_n) = \sum_{\sigma \in S_n} \text{sgn}(\sigma) \prod_{1 \leq i \leq n} A_{\sigma(i)} i$.

Prop. (2.3.10.6). For a matrix, the determinant satisfies the following properties:
1. adding a multiple of a column/row to another column/row, the determinant doesn’t change.
2. Multiplying a row or a column with a scalar, then the determinant multiplies with this scalar.
3. Changing two rows or two columns makes the determinant multiply by $-1$.

Proof: All this follows from 4 of (2.3.10.2). Notice the last one follows from the first two. □

Prop. (2.3.10.7)[Laplacian Expansion Formula]. Cf.[Determinant 安金鹏 P15].

Prop. (2.3.10.8). Adjunction matrix, Cf.[Determinant 安金鹏 P16].

Proof: □

Cor. (2.3.10.9). If $AB = 1$, then $BA = 1$.

Prop. (2.3.10.10)[Cramer’s Rule]. Cf.[Determinant 安金鹏 P16].

Prop. (2.3.10.11)[Binet’s Formula]. Let $F/E$ be a Hermitian pair, $A \in M_{n \times m}(F)$, then $\det(A^*A) = \sum_{I \in \{0, \ldots, n\}, \# I = m} |\det(A_I)|^2$. 

Proof: □
Proof: Let \( L : F^m \to F^n \) be the corresponding map, then \( \wedge^n(L^*) \circ \wedge^n(L) = \wedge^n(L^* \circ L) \). In the canonical basis, the matrices for \( \wedge^n(L^*)(\text{resp. } \wedge^n(L)) \) have only one column(\text{resp. one row}) with entries \( \det(A_I) \) by definition(2.3.10.1), thus the assertion follows by(2.3.10.1) again. □

Prop. (2.3.10.12)[Sylvester’s Determinant Identity]. If \( A \) and \( B \) are matrices of sizes \( m \times n \) and \( n \times m \), then

\[
\det(I_m + AB) = \det(I_n + BA)
\]

Proof: Notice

\[
\begin{pmatrix} 1 & A \\ B & 1 \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ B & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ 0 & 1 - BA \end{pmatrix} \begin{pmatrix} 1 & A \\ 0 & 1 \end{pmatrix}
\]

\[
= \begin{pmatrix} 1 & A \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 - BA & 0 \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 & 0 \\ B & 1 \end{pmatrix}
\]

and use(2.3.10.2). □

Cor. (2.3.10.13). Multiplying by \( x \), we see that the characteristic polynomial of \( AB \) and \( BA \) are the same.

Remark(2.3.10.14). There is another proof in case \( m = n \): It suffices to show

\[
\det(I + (A + xI)(B + xI)) = \det(I + (B + xI)(A + xI)).
\]

But notice \( A + xI \) and \( B + xI \) are invertible in \( M_{n \times n}(K(X)) \), thus

\[
\det(I + (A + xI)(B + xI)) = \det((A + xI)((A + xI)^{-1} + (B + xI))) = \det(I + (B + xI)(A + xI)).
\]

Prop. (2.3.10.15).

\[
\det \begin{bmatrix} A & B \\ C & D \end{bmatrix} = \det(A) \det(D - CA^{-1}B).
\]

Proof: As before, consider \( \det \begin{bmatrix} A + xI & B \\ C & D + xI \end{bmatrix} \), then \( A + xI \) is invertible, and this equals

\[
\det \begin{bmatrix} A + xI & B \\ C & D + xI - C(A + xI)^{-1}B \end{bmatrix} = \det(A + xI) \det(D + xI - C(A + xI)^{-1}B).
\]

Letting \( x = 0 \), we get the desired result. □

Prop. (2.3.10.16) [Symplectic Group Determinant]. The determinant of a symplectic matrix \( \in \text{Sp}(2n, \mathbb{R}) \) has determinant 1.

Proof: A symplectic matrix preserves the symplectic structure thus the symplectic form \( \omega \), hence preserves \( \omega^n \) which is \( n! \) times the volume form, so it has determinant 1 by definition(2.3.10.1). □

Prop. (2.3.10.17) [Vandermonde Matrix]. The \( n \times n \) Vandermonde matrix, with the \( k \)-th row \( (1, x_k, \ldots, x_k^n) \), has determinant \( \prod_{i<j}(x_i - x_j) \). So it is invertible when \( x_i \) are pairwisely different.

Proof: Eliminate the first row by adding columns. □
Prop. (2.3.10.18) [Pfaffian]. There is a polynomial $\text{Pf}$ called Pfaffian s.t. $\det M = \text{Pf}(M)^2$ for a skew-symmetric matrix. This is because a skew symmetric is equal to $A^t \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}^k A$ for $A$ an orthogonal matrix (2.3.8.3), so it has determinant $(\det A)^2$ and $A$ and depends polynomially on the entries of $M$.

Cor. (2.3.10.19).

$\text{Pf}(A^t MA) = \det A \cdot \text{Pf}(M)$.

Because we only need to consider the sign and it is determined by letting $A = \text{id}$.

Traces

Def. (2.3.10.20) [Trace]. For a $n \times n$-matrix $A$, define its trace $\text{tr}(A)$ to be the minus of the coefficient of $x^{n-1}$ in $\det(xI - A)$. It is clear that $\text{tr}(A) = \sum_{i=1}^n a_{ii}$, and by (2.3.10.3) that traces are invariant under conjugacy.

Prop. (2.3.10.21). $\text{tr}(AB) = \text{tr}(BA)$.

Proof: This is because $\det(x - AB) = \det(x - BA)$ by Sylvester determinant identity (2.3.10.12).

Prop. (2.3.10.22) [Trace Formula]. For $V \in \text{Vect}/k, F \in \text{End}(V), d \in \mathbb{Z}_+$,

$$t \frac{d}{dt} \log \det(1 - FT)^{d-1} = \sum_{i \geq 1} d \text{tr}(F^i|V)T^i + 1 + T k[[T]].$$

In particular, if char $k = 0$,

$$\det(1 - FT)^d|V|^{-1} = \exp\left(\sum_{i \geq 1} \text{tr}(F^i|V)\frac{T^d}{i}\right) + 1 + T k[[T]].$$

Proof: Pass to $\overline{k}$ and let $k_1, \ldots, k_r$ be the eigenvalues of $F$.

11 (Real) Quaternion Algebra

Remark (2.3.11.1). The argument below are largely true for any skew field.

Def. (2.3.11.2) [Real Quaternion Algebra]. The real quaternion algebra $\mathbb{H}$ is the space $\mathbb{R}\{1, i, j, k\}$ subjects to the relations

$$ij = -ji = k, jk = -kj = i, ki = -ik = j, i^2 = j^2 = k^2 = -1.$$

In fact, by (12.3.5.6), any quaternion algebra over $\mathbb{R}$ is isomorphic to $\mathbb{H}$.

Prop. (2.3.11.3) [Module of Quaternion Algebras]. There is an involution on $\mathbb{H}$ that $\overline{x} = \frac{a + bi + cj + dk}{a - bi - cj - dk} = a - bi - cj - dk$. Then we define a the module of $x \in \mathbb{H}$ as

$$|x|^2 = x\overline{x} = \overline{x}x = a^2 + b^2 + c^2 + d^2.$$

Then every non-zero element of $\mathbb{H}$ is invertible. In particular, it is a skew field.
Prop. (2.3.11.4). H is isomorphic to subalgebra of matrices in $M(2, \mathbb{C})$ consisting of elements of the form
\[
\left\{ \begin{bmatrix} \alpha & -\overline{\beta} \\ \beta & \overline{\alpha} \end{bmatrix} \right\} | \alpha, \beta \in \mathbb{C} \}
\]

Prop. (2.3.11.5). The center of H is $\mathbb{R}$, by (12.3.4.3).

Prop. (2.3.11.6) [Invertible Quaternion Matrices]. Denote $GL(n, \mathbb{H})$ the set of invertible matrices in $M_n(\mathbb{H})$. If $A \in M_n(\mathbb{H})$, $A$ acts on $\mathbb{H}^n$, and determines a complex matrix $A'$ in $M_{2n}(\mathbb{C})$.

- If $A, B \in M_n(\mathbb{H})$ satisfies $AB = 1$, then $BA = 1$.
- $A \in M = GL(n, \mathbb{H})$ iff $A' \in GL(2n, \mathbb{C})$. In particular if we define the determinant of $A \in M_n(\mathbb{H})$ as the determinant of $A'$, then $\det(A) \neq 0$ iff $A$ is invertible.

Proof: 1: $(AB)' = A'B'$, thus $M_n(\mathbb{H})$ is a subalgebra of $M_{2n}(\mathbb{C})$. Thus $B'A' = 1$ by (2.3.10.9).

2: If $A'$ is invertible, then $A$ is a bijection, thus there are vectors $v_1, \ldots, v_n$ that $Av_i = e_i$. This means
\[
(v_1, \ldots, v_n)A = 1.
\]
Thus by item 1 $A$ is invertible. \(\square\)

Def. (2.3.11.7) [Sesquilinear Form on $\mathbb{H}^n$]. Let $V = \mathbb{H}^n$, then a sesquilinear form on $\mathbb{H}^n$ is a bi-additive function $(\cdot, \cdot) : V \times V \rightarrow \mathbb{H}$ such that
\[
(x\alpha, y\beta) = \overline{\pi}(x, y)\beta, \quad \alpha, \beta \in \mathbb{H}.
\]

Moreover if it is called a Hermitian form iff $(x, y) = \overline{(y, x)}$, and skew-Hermitian iff $(x, y) = -(y, x)$.

Prop. (2.3.11.8) [Quaternion Hermitian Forms].

- Every non-degenerate Hermitian quaternion form is of the form
\[
(x, y) = \overline{x}_1y_1 + \ldots + \overline{x}_py_p - \overline{x}_{p+1}y_{p+1} - \ldots - \overline{x}_ny_n
\]
in some basis. And $p$ is uniquely determined.

- Every non-degenerate skew-Hermitian quaternion form is of the form
\[
(x, y) = \overline{x}_1y_1 + \ldots + \overline{x}_ny_n
\]
in some basis.

Proof: Firstly, there are some $v$ that $(v, v) \neq 0$: If $(v, v) = 0$ for all $v$, then $(x, y) + (y, x) = 0$ for all $x, y$. If it is skew-Hermitian, this means $(x, y)$ is real, which is impossible, unless $(x, y) = 0$. If it is Hermitian, this means $(x, y)$ is imaginary, but $(x, y\overline{i}), (x, y\overline{j}), (x, y\overline{k})$ are all imaginary, thus $(x, y) = 0$.

Then choose this $v$, and take the orthogonal complement of $v$, then by induction we can find $v_1, \ldots, v_n$ that is mutually orthogonal.

If it is Hermitian, then $(v_i, v_i) \in \mathbb{R}$, thus we can find some $t_i \in \mathbb{R}$ that $(tv_i, tv_i) = \pm 1$. $2p$ is the multiplicity of the eigenvalue 1 of the eigenspace of to the matrix corresponding to the form, so $p$ is uniquely defined.

If it is skew-Hermitian, then $(v_i, v_i)$ is imaginary, thus by (11.6.4.3), there are $u_i \in \mathbb{H}$ that $(u_i, v_i, u_i, v_i) = \overline{u}_i(v_i, v_i)u_i = j$. \(\square\)
Cor. (2.3.11.9).
- Every non-degenerate Hermitian quaternion form is of the form
  \[(x, y) = B_1(x, y) + jB_2(x, y)\]
in some basis, where \(B_1(x, y)\) is the usual canonical Hermitian form of signature \((2p, 2q)\), and \(B_2\) is the usual canonical skew-symmetric bilinear form. Also \(B_2(x, y) = B_1(xj, y)\).

- Every non-degenerate skew-Hermitian quaternion form is of the form
  \[(x, y) = B_1(x, y) + jB_2(x, y)\]
in some basis, where \(B_1(x, y)\) is the usual canonical skew-Hermitian form that \(iB_1\) is Hermitian of signature \((n, -n)\), and \(B_2\) is the usual canonical symmetric bilinear form. Also \(B_2(x, y) = B_1(xj, y)\) in some basis.

12 Others

Prop. (2.3.12.1). Let \(H^* = \bigoplus_{i=0}^{2d} H^i\) be a graded algebra over a field s.t. \(\dim H^i < \infty\) for each \(i\). Assume that for each \(0 \leq i \leq 2d\), there is a perfect pairing
\[H^i \times H^{2d-i} \to K\]
induced from an isomorphism \(\text{tr} : H^{2d} \cong K\), Let \(\varphi\) be a ring endomorphism of \(H^*\) that satisfies
- \(\varphi(H^i) \subset H^i\),
- \(\varphi_{2d} = \text{id}\)

Then each \(\varphi_i\) is invertible, and \(\varphi_i^{-1} = \varphi_{2d-i}^t\), where \(\varphi_{2d-i}^t\) is the transpose of \(\varphi_{2d-i}\) w.r.t. the perfect pairing \(H^i \times H^{2d-i} \to K\).

Proof: Let \(a \in H^i\) be any element, if \(a \neq 0\), then because the pairing \(H^i \times H^{2d-i} \to K\) is perfect, there exists some \(b \in H^{2d-i}\) s.t. \(ab \neq 0\). Thus \(\varphi_i(a)\varphi_{2d-i}(b) \neq 0\), thus \(\varphi_i\) is injective. Now \(\text{tr}(\varphi_i^{-1}(a)b) = \text{tr}(\varphi_{2d}(\varphi_i^{-1}(a)b)) = \text{tr}(a\varphi_{2d-i}(b))\), thus \(\varphi_i^{-1} = \varphi_{2d-i}^t\). \(\Box\)
2.4 More on (Non-Commutative) Algebras

Main references are [Noncommutative Rings, T.Y.Lam], [Lan05]Chap17 and [Sta]Chap11.

Notations (2.4.0.1).

- Use notations defined in Abstract Algebra.

1 Semisimplicity

Def. (2.4.1.1). For \( R \in \mathfrak{Ring} \), a simple \( R \)-module is a \( E \in \Mod_R \) that no submodules other than 0 and \( E \). It is called faithful iff there is no nonzero element \( a \in R \) that \( ax = 0 \) for any \( x \in E \).

- It is called non-degenerate if \( RE = E \).

Prop. (2.4.1.2) [Shur’s lemma]. For \( R \in \mathfrak{Ring} \) and \( E \) a simple \( R \)-module, \( \text{End}_R(E) \) is a division ring, this is because the kernel and image are all 0 or \( E \).

Cor. (2.4.1.3) [Uniqueness of Decomposition of Modules]. If an \( R \)-module \( E \) can be written as a finite direct sum of simple \( R \)-modules in multiple ways, then the multiplicity of the irreducible modules appearing in it is uniquely determined.

Proof: Cf. [Lang, Algebra, P643]

Def. (2.4.1.4) [Semisimple Modules]. For \( R \in \mathfrak{Ring} \), a semisimple \( R \)-module is a \( E \in \Mod_R \) iff it satisfies the following equivalent conditions:

- It is a sum of simple modules.
- It is a direct sum of simple modules.
- Any submodule \( F \) of \( E \) has a complement in \( E \).

Proof: 3 \( \rightarrow \) 2: By Zorn’s lemma, it suffices to show any non-zero semisimple module contains a simple submodule: Take a \( m \neq 0 \in M \), then we may assume \( M = Rm \), and by Zorn’s lemma there is a maximal submodule \( N \) that \( m \notin N \), and let \( N \oplus N' = M \), then we show \( N' \) is simple. because any submodule \( N'' \) satisfies \( m \in N \oplus N'' \) thus \( N'' = N' \).

2 \( \rightarrow \) 1 is immediate, it suffices to show 1 \( \rightarrow \) 3: for any submodule \( N \subset M \), consider all the simple modules that intersect \( N \) trivially, denote their sum by \( V \), I claim \( N \oplus V = M \), otherwise, let \( S \) be a simple submodule that contained in \( N + V \), then \( S \cap (N + V) = 0 \), so \( N \cap (S + V) = 0 \), contradicting the maximality.

Cor. (2.4.1.5). For \( R \in \mathfrak{Ring} \), any submodule and quotient module of a semisimple \( R \)-module is semisimple.

Proof: The quotient is clearly a sum of simple modules, and for a submodule, its submodule has a complement.

Density Theorems

Def. (2.4.1.6). If \( E \) be a semisimple \( R \)-module, let \( R' = \text{End}_R(E) \), then \( E \) is also a \( R' \)-module, where the action is given by \( (\varphi, x) \rightarrow \varphi(x) \). Then any element of \( R \) defines an element of \( \text{End}_{R'}(E) \) by left multiplication. If we called \( \text{End}_{R'}(E) \) the bicommutant of \( E \) over \( R \), then
Lemma (2.4.1.7). For a module $E$ over $R$, let $\text{End}_{R'}(E)$ be the bicommutant. If $f \in \text{End}_{R'}(E)$ and $x \in E$, then there is an element $\alpha \in R$ that $\alpha x = f(x)$.

Proof: Since $E$ is semisimple, write $E = Rx \oplus F$, and let $\pi$ be the projection unto $Rx$, then $\pi \in \text{End}_R(E)$, and $f(x) = f(\pi(x)) = \pi f(x) \in Rx$. □

Prop. (2.4.1.8) [Jacobson Density Theorem]. Let $E$ be semisimple over $R$ and let $R' = \text{End}_R(E)$. If $f \in \text{End}_{R'}(E)$ and $x_1, \ldots, x_n \in E$, then there is an element $\alpha \in R$ that $\alpha x_i = f(x_i)$ for all $i$.

In particular, if $E$ is f.g. over $R'$, the natural map $R \to \text{End}_{R'}(E)$ is surjective.

Proof: Consider $f^n \in \text{End}_R(E^n)$, then it is just a $n \times n$ matrix with entries in $R'$.

Consider the lemma (2.4.1.7) shows there is an $\alpha \in R$ that

$$(\alpha x_1, \ldots, \alpha x_n) = (f(x_1), \ldots, f(x_n))$$

which is the result. □

Cor. (2.4.1.9) [Wedderburn Theorem]. Let $R \in \mathfrak{Ring}$ and $E$ is a faithful simple $R$-module. Let $D = \text{End}_R(E)$. If $E$ is of f.g. over $D$, then $R = \text{End}_k(E)$.

Proof: The density theorem (2.4.1.8) and the fact $E$ is f.g. over $D$ shows that $R \to \text{End}_k(E)$ is surjective, and also injective because it is faithful, thus $R = \text{End}_k(E)$. □

Cor. (2.4.1.10) [Burnside’s Theorem]. Let $E$ is an $R$-module that is f.d over an alg.closed field $k$ and $R$ is a subalgebra of $\text{End}_k(E)$. If $E$ is simple as an $R$-module, then $R = \text{End}_k(E)$.

Proof: It follows from Shur’s lemma (2.4.1.12) and (2.2.1.10) $R' = \text{End}_R(E)$ is just $k$, so we can use Wedderburn’s theorem (2.4.1.9). □

Cor. (2.4.1.11) [F.d. Simple Module over Commutative Algebra]. If $R$ is commutative and $E$ is a simple $R$-module of f.d. over an alg.closed field $k$, then $E$ is of 1-dimensional.

Proof: The theorem shows the image of $R$ in $\text{End}_k(E)$ is all of $\text{End}_k(E)$, but Shur’s lemma (2.4.1.12) and (2.2.1.10) that the image of $R$ consists of scalars, thus $\dim_k E = 1$. □

Prop. (2.4.1.12) [Projection Operators]. Let $k$ be a field and $R$ is a $k$-algebra. If $V_1, \ldots, V_n$ are pairwise non-isomorphic simple $R$-modules of f.d. over $k$, then there exists elements $e_i$ in $R$ that acts as identity on $V_i$ and 0 on other $V_j$.

Proof: This is an immediate consequence of Jacobson density theorem (2.4.1.8) applied to the projection operator on $\oplus_i V_i$. □

Prop. (2.4.1.13) [Characters Determine F.D. Representations (Bourbaki)]. Let $R$ be an algebra over a field $k$ of char0, $E_1, E_2$ be two f.d. semisimple $R$-module over $k$, then if the character $\chi_1 = \chi_2$, then the $R$-modules $E_1, E_2$ are isomorphic.

Proof: $E, F$ are isomorphic to direct sums of simple $R$-modules, so it suffices to show the multiplicities $m, n$ of any simple module $V$ is the same. We can find an element $e$ that is identity on $E$ and 0 on other simple modules $V_i$ by (2.4.1.12), thus the trace of $e$ on $E, F$ are $m \dim_k(V), n \dim_k(V)$ respectively, thus $m = n$ because $k$ is of char0. □
Def. (2.4.1.14) [Matrix Coefficients]. For an algebra $R$ and an $R$-module $M$ over a field $k$, then a matrix coefficient of $M$ is a function $c : R \to k$ of the form $c(r) = L(rx)$, where $L$ is a linear functional on $M$ and $x \in M$.

Cor. (2.4.1.15). If $R$ is an algebra over a field $k$ and two simple $R$-modules that is f.d. over $k$ have a nonzero matrix coefficient in common, then they are isomorphic.

Proof: Let $c(r) = L_1(rx_1) = L_2(rx_2)$. If they are non-isomorphic, then we can find a $e \in R$ that is identity on $M_1$ and $0$ on $M_2$ by (2.4.12). Let $c(u) \neq 0$, then
\[
    c(ue) = L_1(ue x_1) = L_1(u x_1) = c(u) \neq 0, \quad c(ue) = L_2(ue x_2) = L_2(0) = 0
\]
contradiction.

Prop. (2.4.1.16) [Simple Modules of Tensor Product]. Let $A, B$ be algebras over a field $\Omega$, $R = A \otimes B$, then:

- If $P$ be a simple $R$-module of f.d. over $\Omega$, then there is a simple $A$-module $M$ and a simple $B$-module $N$ that $P$ is isomorphic to a quotient of $M \otimes N$. Also the isomorphism classes of $M, N$ are uniquely determined.

- If $\Omega$ is alg.closed and $M, N$ are simple modules of $A, B$ of f.d. over $\Omega$, then $M \otimes N$ is a simple module over $A \otimes B$.

Proof: 1: because $P$ is f.d., it contains a simple $A$-module $M$. Let $N_1 = \text{Hom}_A(M, P)$, then it is a $B$-module as $A, B$ commutes in $A \otimes B$. Then we can define a map $\lambda : M \otimes N_1 \to P$, which is a $A \otimes B$-module morphism. Now $N_1$ is also of f.d., so it contains a simple $B$-module $N$, and $\lambda$ is clearly non-zero on $M \otimes N$, thus its image is all of $P$, as $P$ is simple.

For the uniqueness, let $d = \dim N$, then $P$ is isomorphic to $k \leq d$ copies of $M$ as an $A$-module, so the isomorphism class of $M$ is determined, so does that of $N$.

2: Consider the map of $A, B$ to $\text{End}_\Omega(M), \text{End}_\Omega(N)$ are surjective by (2.4.10). Then it suffices to show that $M \otimes N$ are simple over $\text{End}_\Omega(M) \otimes \text{End}_\Omega(N)$, but this is just $\text{End}_\Omega(M \otimes N)$, over which $M \otimes N$ is clearly simple.

Semisimple Rings and Simple Rings

Def. (2.4.1.17) [Semisimple Ring]. A (left) semisimple ring is a ring $R$ s.t. it is a (left)semisimple module over itself. In (2.4.1.23), we will see a semisimple ring is semisimple in both sides.

Prop. (2.4.1.18). Any semisimple ring is left Artinian and Noetherian.

Proof: Consider the decomposition $R = \bigoplus_{\alpha} \mathcal{A}_\alpha$, where $\mathcal{A}_\alpha$ are simple left $R$-ideals. Then by considering the decomposition of $1 \in R$, clearly this is a finite sum. The rest is easy.

Prop. (2.4.1.19). If $R$ is a semisimple ring, then any $R$-module is semisimple.

Proof: Any $R$-module is a quotient of a free $R$-module, thus semisimple, by (2.4.15).

Prop. (2.4.1.20). $R$ is semisimple iff all $R$-modules are projective.

Proof: If $R$ is left-semisimple, for any $R$-module $P$ and an exact sequence
\[
    0 \to N \to M \to P \to 0
\]
by (2.4.1.19), there is a complement of $N$ in $M$, thus this sequence splits and $P$ is projective. The converse is also clear that any submodule of any $R$-module has a complement.
Lemma (2.4.1.21). Let $D$ be a division ring and $R = M_n(D)$, then
- $R$ is simple, left semisimple and left Noetherian.
- $R$ has a unique left simple module $V$, and $R$ acts faithfully on $V$, with $R \cong nV$.
- $\text{End}_R(V) \cong D$.

Proof: Cf. [Lam, P31].

Prop. (2.4.1.22) [Wedderburn-Artin]. Any left semisimple ring is of the form $R \cong \text{Mat}(n_1, D_1) \times \cdots \times \text{Mat}(n_r, D_r)$, and $D_i$ are uniquely determined division rings. There are exactly $r$ different left simple $R$-modules and $D_i$ are uniquely determined.

Proof: Consider the decomposition $R \cong n_1V_1 \oplus \cdots \oplus n_rV_r$ where $V_i$ are simple left $R$-modules. Then we can use Schur’s lemma (2.4.1.2) and (2.4.1.21) to calculate the endomorphism ring, so:

$$R \cong \text{End}(n_1V) \times \cdots \times \text{End}(n_rV_r) \cong \text{Mat}(n_1, D_1) \times \cdots \times \text{Mat}(n_r, D_r).$$

For the uniqueness, we use (2.4.1.21), which shows $D_i$ and $V_i$ both can be recovered.

Cor. (2.4.1.23). $R \in \text{Ring}$ is left semisimple iff it is right semisimple. ((2.3.1.11) is used).

Cor. (2.4.1.24). A semisimple commutative ring is a finite direct product of fields.

Def. (2.4.1.25) [Semisimple Categories]. Let $k \in \text{Field}$ and $\mathcal{A}$ a $k$-linear Abelian category that End$(X)$ are all finite $k$-modules for $X \in \mathcal{A}$, then $\mathcal{A}$ is semisimple iff End$(X)$ is a semisimple $k$-algebra for any $X$.

Proof: If $\mathcal{A}$ is semisimple, then any $X \in \mathcal{A}$ is a direct sum of simple objects, so End$(X)$ is semisimple.

Conversely, if End$(X)$ is semisimple thus a product of matrix algebras over division algebras, so $X$ can be indecomposable only if End$(X)$ is a division algebra. Now if $f : M \to N$ is a morphism of indecomposable objects, if there is a map $g : N \to M$ that $g \circ f \neq 0$, then $g \circ f$ is an automorphism of $M$, and $(g \circ f)^{-1} \circ g$ is a right inverse to $f$, so $N$ is a direct sum of $M$, and thus $f$ is an isomorphism because $M$ is indecomposable.

Now it suffices to show any indecomposable object is simple. If $M$ is an indecomposable object properly contained in another indecomposable object, then

$$\begin{bmatrix} 0 & 0 \\ \text{Hom}(M, N) & 0 \end{bmatrix} \subset \begin{bmatrix} \text{End}(M) & \text{Hom}(N, N) \\ \text{Hom}(M, N) & \text{End}(N) \end{bmatrix} = \text{End}(M \oplus N)$$

is a two sided nilpotent nonzero ideal, contradicting the fact End$(M \oplus N)$ is semisimple.

Prop. (2.4.1.26) [Semisimplicity and Base Change]. If $A \in \text{Alg}_k$ and $A \otimes_k K$ is semisimple for some field extension $K/k$, then $A$ is semisimple. Conversely, if $A$ is semisimple, then $A \otimes_k K$ is semisimple for every separable field extension $K/k$.

Prop. (2.4.1.27) [Characters Determine F.D. Representations]. If \( R \) is a semisimple ring over a field \( k \) of characteristic 0, then its f.d. representations are determined by their characters, by (2.4.1.13).

Prop. (2.4.1.28) [Simple Artinian Algebras]. For a simple ring \( R(2.2.1.2) \), the following are equivalent:

- \( R \) is left semisimple.
- \( R \) is left Artinian.
- \( R \) has a minimal left ideal.
- \( R \cong \text{Mat}(n,D) \) for some division ring \( D \).

Proof: The equivalence of 1, 4 is by Wedderburn theorem (2.4.1.22) and (2.4.1.21). 2 \( \rightarrow \) 3 is easy, and for 1 \( \rightarrow \) 2, \( R \) is a finite direct sum of minimal ideals by Wedderburn theorem (2.4.1.22), so it is Artinian.

For 3 \( \rightarrow \) 1, consider all the ideals in \( R \) that is isomorphic to the minimal ideal \( \mathfrak{A} \), then it is also a right ideal of \( R \), so equals \( R \), hence \( R \) is semisimple. \( \square \)

Cor. (2.4.1.29). And finite simple \( k \)-algebra \( A \) is of the form \( M_n(D) \) where \( D \) is a finite division ring over \( k \). This is because \( A \) is clearly left Artinian.

Prop. (2.4.1.30) [Double Centralizer Property]. Let \( R \) be a simple ring and \( \mathfrak{A} \) a nonzero left ideal. Let \( D = \text{End}_R(\mathfrak{A}) \), then the natural map \( f : R \rightarrow \text{End}(\mathfrak{A}_D) \) is an isomorphism.

Proof: since \( R \) is simple, \( f \) is injective. To show it is surjective, let \( E = \text{End}(\mathfrak{A}_D) \), then for any \( a, r \in \mathfrak{A} \) and \( h \in E \), we have \( h(ra) = h(r)a \), thus

\[(h \cdot f(r))a = h(ra) = h(r)a = f(h(r))a\]

which shows \( f(R) \) is a left ideal in \( E \). And because \( \mathfrak{A}R = R \), we have \( f(R) = f(\mathfrak{A})f(R) \), then

\[Ef(R) = Ef(\mathfrak{A})f(R) \subset f(\mathfrak{A})f(R) = f(R)\]

which shows \( f(R) \) is a left ideal in \( E \), and it contains 1, so \( f(R) = E \). \( \square \)

2 Jacobson Radical Theory

Def. (2.4.2.1) [Jacobson Radical]. For \( R \in \mathfrak{Ring} \), the Jacobson radical is defined to be the intersection of all maximal left ideals in \( R \).

- \( R \) is called Jacobson semisimple if \( \text{rad } R = 0 \).
- \( R \) is called semi-local if \( \overline{R} = R/\text{rad } R \) is semisimple.
- \( R \) is called semi-primary if \( R \) is semi-local and \( \text{rad } R \) is nilpotent.

Prop. (2.4.2.2) [Characterizing Jacobson Radicals]. For \( y \in R \), the following are equivalent:

- \( y \in \text{rad } R \).
- \( 1 - xy \) is left-invertible for any \( x \in R \).
- \( yM = 0 \) for any simple left \( R \)-module \( M \).
- \( 1 - xyz \) is invertible for any \( x, z \in R \).
Prop. (2.4.2.6) [Artinian Radical Nilpotent].

In a left Artinian ring, rad $R$ is the largest nilpotent left ideal, and it is also the largest nilpotent right ideal.

Proof: By the above lemma, it suffices to show $J = \text{rad } R$ is nilpotent. By Artinian property, the descending chain $J \supset J^2 \supset J^3 \supset \ldots$ is stabilizing, so there exists $k$ s.t. $J^k = J^{k+1} = I$. Then $I = 0$, because otherwise we can choose a minimal non-left ideal $\mathfrak{A}$ s.t. $IA = 0$. Then if $a \neq 0 \in \mathfrak{A}$,

$$I(Ia) = I^2a = Ia = 0,$$

so $\mathfrak{A} = Ia$, and $a = ya$ for some $y \in J$, so $(1-y)a = 0$. But $1-y$ is a unit by (2.4.2.2), contradiction. □

Cor. (2.4.2.7). In a left Artinian ring, any 1-sided locally nilpotent ideal is nilpotent. By left Artinian, there is a $k$ that $(\text{rad } R)^k = (\text{rad } R)^{k+1} = I$. Now if $I \neq 0$, then we can choose a minimal left ideal $\mathfrak{A}$ that $I\mathfrak{A} \neq 0$ by Artinian property. Now there is an $a \in \mathfrak{A}$ that $Ia \neq 0$, so $I(Ia) = Ia \neq 0$, so $Ia = \mathfrak{A}$ and $a = ya$ for some $y \in I$. But $1-y$ is invertible, so $a = 0$, contradiction.

Prop. (2.4.2.8) [Semisimplicity and Jacobson Semisimplicity]. For $R \in \text{Ring}$, the following are equivalent:

- $R$ is semisimple.
- $R$ is Jacobson semisimple and left Artinian.
- $R$ is Jacobson semisimple and satisfies DCC on principal left ideals.

Proof: 1 → 2: $R$ is left Artinian by (2.4.1.18), and consider $R = \text{rad } R \oplus \mathfrak{B}$, then $\mathfrak{B}$ is contained in a maximal left ideal $\mathfrak{m}$, which cannot contain $\text{rad } R$, unless $\text{rad } R = 0$.

3 → 1: 3 implies that any left ideal $\mathfrak{A}$ contains a minimal left ideal $I$ (the minimal principal one), and every minimal left ideal $I$ is a direct summand of $R$ (by choosing the maximal left ideal $\mathfrak{m}$ not containing $I$, because $I \oplus \mathfrak{m} = R$).

Then we can deduce 1: If $R$ is not semisimple, then take a minimal left ideal $\mathfrak{B}_1$, then $R = \mathfrak{B}_1 \oplus \mathfrak{A}_1$, and $\mathfrak{A}_1 \neq 0$ otherwise $R$ is semisimple, and we can choose a minimal left ideal $\mathfrak{B}_2 \subset \mathfrak{A}_1$, then $\mathfrak{A}_1 = \mathfrak{B}_2 \oplus \mathfrak{A}_2$. Continuing this way, we get a chain of left ideals $\mathfrak{A}_1 \supset \mathfrak{A}_2 \supset \ldots$, and they are both principal because they are direct summands of $R$, contradicting item 3. □
Prop. (2.4.2.9) [Hokins-Levitzki Theorem]. Let $R$ be a semi-primary ring (2.4.2.1), then for any $R$-module $M$, the following are equivalent:

- $M$ is Noetherian.
- $M$ is Artinian.
- $M$ has a composition series.

In particular, a ring is left Artinian iff it is left Noetherian and semi-primary.

Proof: It suffices to prove if $M$ is Noetherian or Artinian, $M$ has a composition series. Denote $J = \sqrt{R}$, then $J^n$ for some $n > 0$. We consider

$$0 \subset J^{n-1}M \subset \cdots \subset JM \subset M,$$

and the quotient $J^{k-1}M/J^kM$ is Artinian or Noetherian over $\overline{R} = R/\sqrt{R}$ which is semisimple, so it is a direct sum of simple modules, and the sum is finite, so there is a composition series.

The last assertion: A left Artinian ring is semi-primary, by (2.4.2.6) and (2.4.2.8). So the assertion follows from the equivalence of item 1 and 2. □

Lemma (2.4.2.10). Let $x \in \sqrt{R}$ where $R$ is a $k$-algebra, then $x$ is algebraic over $k$ iff $x$ is nilpotent.

Proof: One direction is trivial. For the other, if $x^r + a_1x^{r+1} + \cdots + a_nx^{r+n} = 0$, then because $1 + a_1x^1 + \cdots + a_nx^n$ is invertible, we have $x^r = 0$. □

Prop. (2.4.2.11) [Amitsur]. Suppose $k$ is a field and $R$ is a $k$-algebra that $\dim_k R < |k|$, then $\sqrt{R}$ is the largest locally nilpotent ideal of $R$.

Proof: If $|k| < \infty$, then $R$ is Artinian, so $\sqrt{R}$ is nilpotent by (2.4.2.6), and it is the largest by (2.4.2.6) again. Suppose now $k$ is infinite. By the lemma above, it suffices to show every $r \in \sqrt{R}$ is algebraic over $k$. Notice that $a - r$ is invertible for $a \in k^*$, and $\{(a - r)^{-1}\}$ cannot be $k$-linearly independent because $\dim_k R < |k|$, so there is a dependence relation

$$\sum_{i=1}^n b_i(a_i - r)^{-1} = 0.$$

Hence $r$ is algebraic over $k$. □

Prop. (2.4.2.12) [Amitsur]. Let $R$ be a ring and $S = R[T]$. Let $J = \sqrt{S}$ and $N = R \cap J$, then $N$ is a locally nilpotent ideal in $R$, and $J = N[T]$. In particular, if $R$ is Jacobson semisimple, then $S$ is also Jacobson semisimple (2.4.2.5).

Proof: Cf. [Lam, P71]. □

Lemma (2.4.2.13). Let $R$ be a $k$-algebra and $K/k$ is a separable algebraic field extension, then if $R$ is Jacobson semisimple, so is $R \otimes_k K$.

Proof: Cf. [Lam, P76]. □

Prop. (2.4.2.14) [Jacobson Radical Under Base Change of Fields]. Let $R$ be a $k$-algebra and $K/k$ a separable algebraic extension, then $\sqrt{R \otimes_k K} = (\sqrt{R}) \otimes_k K$.

Proof: Cf. [Lam, P76]. □
3 Finite Semisimple \( k \)-Algebras

Reference for this subsection is [Sta] Chap 11.

**Def. (2.4.3.1) [Azumaya Algebras].** A central \( k \)-algebra is an algebra \( A \) that the center of \( A \) is the image of \( k \rightarrow A \).

**Def. (2.4.3.2) [Azumaya Algebras].** An Azumaya algebra over \( k \) is defined to be a finite central \( k \)-algebra. The category of Azumaya algebras over \( k \) is denoted by \( \text{Az} k \).

**Lemma (2.4.3.3).** Let \( D \) be a division ring with central field \( k \) and \( A \in \text{Ring} / k \), then any two-sided ideal \( I \) of \( A \otimes k D \) is of the form \( J \otimes k D \) for some two-sided ideal \( J \) of \( A \). In particular, if \( A \) is simple, then \( A \otimes k D \) is also simple.

*Proof:* Cf. [Sta] 074C.

**Lemma (2.4.3.4).** Let \( R \in \text{Ring} \) and \( n \in \mathbb{Z}_+ \), then
- The functors \( M \mapsto M \oplus n, N \mapsto e_{11} n \) defines an equivalence of categories between \( \text{Mod}_R \) and \( \text{Mod}_{\text{Mat}(n,R)} \).
- Any two-sided ideal of \( \text{Mat}(n,R) \) is of the form \( \text{Mat}(n,I) \) for some two-sided ideal \( I \) of \( R \).
- Then center of \( \text{Mat}(n,R) \) is the equal to the center of \( R \).

**Prop. (2.4.3.5).** if \( A, A' \) are two simple \( k \)-algebras that \( A \) is finite central over \( k \), then \( A \otimes_k A' \) is simple.

*Proof:* Let \( A' \) be finite central over \( k \), then by (2.4.1.28), \( A' \cong \text{Mat}(n,D) \) for some finite central division algebra over \( k \). Then
\[
A \otimes_k A' \cong \text{Mat}(n,A \otimes D),
\]
which is simple by (2.4.3.3) and (2.4.3.4).

**Cor. (2.4.3.6).** The tensor product of two Azumaya \( k \)-algebras is an Azumaya \( k \)-algebra.

*Proof:* Combine the proposition with (2.2.1.13).

**Cor. (2.4.3.7) [Base Change].** If \( k \in \text{Field} \) and \( A \in \text{Ring} / k \), then for any field extension \( k'/k \), \( A \otimes_k k' \in \text{Az} k' \) iff \( A \in \text{Az} k \).

*Proof:* Combine (2.2.1.13) with (2.4.3.5).

**Prop. (2.4.3.8) [Skolem-Noether].** Let \( A \) be a finite central simple \( k \)-algebra and \( B \) is a simple \( k \)-algebra that \( f, g : B \rightarrow A \) are two \( k \)-algebra homomorphisms. Then there exists an invertible element \( x \in A \) that \( f = x^{-1} g x \).

*Proof:* Choose a simple \( A \)-module \( M \), then \( L = \text{End}_A(M) \) is a skew field, and \( M \) has two \( B \otimes_k L^{\text{op}} \) structures by \( f \) and \( g \). The \( k \)-algebra \( B \otimes_k L^{\text{op}} \) is simple by (2.4.3.5), and also \( B \) is finite simple because there is a \( k \)-homomorphism \( B \rightarrow A \), so \( B \otimes_k L^{\text{op}} \) is finite simple, thus the two \( B \otimes_k L^{\text{op}} \) structures on \( M \) are isomorphic, which means there is a \( \varphi : M \rightarrow M \) intertwining these two structures. But \( \varphi \) commutes with \( L \), meaning that \( \varphi \) is just multiplying by some \( x \in A \), so \( x \) is what we want.

**Cor. (2.4.3.9).** Let \( A \) be a finite simple \( k \)-algebra, then any automorphism of \( A \) is inner.

*Proof:* Because the center of \( A \) is a finite field extension \( k' \) of \( k \) that \( A \) is central simple over \( k' \), thus the Skolem-Noether theorem applies.
Splitting Fields

Prop. (2.4.3.10)[Centralizer Theorem]. Let \( k \in \text{Field} \) and \( A \in \text{Az}_k \), and \( B \) a simple sub \( k \)-algebra of \( A \), then

- \( C = C_A(B) \) is also simple.
- \( \dim_k A = \dim_k B \cdot \dim_k C \).
- \( C_A(C) = B \).

Proof: Cf.[Sta]074T.

Cor. (2.4.3.11). Let \( k \in \text{Field} \) and \( B \subset A \in \text{Az}_k \), then \( C = C_A(B) \) is also in \( \text{Az}_k \), and \( A \cong B \otimes_k C \).

In particular, if a division ring \( D \) is of f.d. over its center \( k \), then \( D \in \text{Az}_k \), and \( \dim_k D \) is a square.

Proof: \( \dim_k A = \dim_k (B \otimes_k C) \) by (2.4.3.10), and \( B \otimes_k C \) is simple by (2.4.3.5), so the natural map \( B \otimes_k C \to A \) is an isomorphism, and the center of \( C \) is \( k \) by (2.4.3.5).

Prop. (2.4.3.12). For \( k \in \text{Field} \), \( A \in \text{Az}_k \), If \( K \subset A \) is a sub \( k \)-field, then the following are equivalent:

- \( \dim_k A = [K : k]^2 \).
- \( C_A K = K \).
- \( K \) is a maximal commutative subring of \( A \).

Proof: 1, 2 are equivalent by (2.4.3.10), and 2, 3 are clearly equivalent, as \( C_A K \) is a commutative subring containing \( K \).

Cor. (2.4.3.13). If \( D \) is a division ring with center \( k \), then every maximal subfield of \( D \) satisfies \( \dim_k A = [K : k]^2 \).

Proof: This is because any commutative subring of \( A \) is a field.

Def. (2.4.3.14)[Splitting Fields]. For \( k \in \text{Field} \) and \( B \) a finite semisimple \( k \)-algebra, then \( B \) is said to split if \( B \) is isomorphic to a product of matrix algebras over \( k \). A field extension \( K/k \) is called a splitting field of \( B \) if \( B_K \) is split.

Prop. (2.4.3.15). If \( k \in \text{Field}, k = \overline{k} \), then any finite semisimple \( k \)-algebra is split.

Proof: This follows from (2.4.1.22) and (2.2.1.10).

Cor. (2.4.3.16)[Central Simple Algebras are of Square Dimensions]. Let \( k \in \text{Field}, A \in \text{Az}_k \), then \( \dim_k A \) is a square.

Proof: This is true because \( A \otimes_k \overline{k} \) is a matrix algebra.

Prop. (2.4.3.17)[Maximal Subfields are Splitting]. Let \( k \in \text{Field}, A \in \text{Az}_k, k'/k \) a finite field extension, then \( k \) is a splitting field of \( A \) iff there exists a \( B \in \text{Az}_k \) similar to \( A \)? s.t. \( k' \subset B \) and \( \dim_k B = [k' : k]^2 \).

In particular, if \( D \) is a division ring, any maximal subfield of \( D \) is a splitting field of \( D \), by (2.4.3.12).

Proof: Cf.[Sta]074Z.
Cor. (2.4.3.18). If \( k \in \text{Field} \) and \( D \) is a central division ring with \( \dim_k D = d^2, d \in \mathbb{Z}_+ \) by (2.4.3.16), then for any splitting field \( k'/k, d|([k': k]) \).

**Proof:** By (2.4.3.17), there exists \( B \in \text{Az}_k \) similar to \( D \) s.t. \( \dim_k B = [k': k]^2 \). Then it follows from (9.2.2.1) that \( B \cong \text{Mat}(n, D) \) for some \( n \in \mathbb{Z}_+ \). Then \( n^2d^2 = [k': k]^2 \), so \( d|[k': k] \). \( \square \)

Prop. (2.4.3.19) [Galois Splitting Fields, Noether-Köthe]. If \( k \in \text{Field} \) and \( D \) is a central division ring over \( k \), then there exists a maximal subfield \( K \subset D \) s.t. \( K/k \) is finite separable. In particular, by (9.2.2.1)(2.4.3.17), any central simple algebra has a finite Galois splitting field.

**Proof:** Notice it suffices to prove that: if \( D \neq k \), there exists \( \alpha \in D \setminus k \) s.t. \( k(\alpha)/k \) is separable. This is because if we find such \( \alpha \), then \( D' = C_D(\alpha) \) is another simple division algebra with center \( k(\alpha) \), by (2.4.3.10), so we can use induction on \( D'/k(\alpha) \).

We may assume \( k \) is non-perfect of characteristic \( p \in \mathbb{P} \), thus an infinite field. Suppose we cannot find such an element, then every element satisfies an equation of the form \( T^{p^r} - a = 0 \), where \( a \in k \). And because \( \dim_k D < \infty \), there exists an \( r \) s.t. \( x^{p^r} \in k \) for any \( x \in D \). Then we can use the fact \( \#k = \infty \) to show that \( x^{p^r} \in \overline{k} \) for any \( x \in D \otimes_k \overline{k} \). But then every \( p^r \)-th power of \( D \otimes_k \overline{k} \cong \text{Mat}(n, \overline{k}) \) is central, which is not true, as \( n > 1 \) and we can take \( e_{11} \).

**Cor. (2.4.3.20).** Let \( k \in \text{Field} \), then for \( A \in \text{Ring}/k \), \( A \in \text{Az}_k \) iff \( A \otimes_k \text{sep} \cong \text{Mat}(n, k\text{sep}) \) for some \( n \in \mathbb{Z}_+ \), by (2.4.3.7).

Def. (2.4.3.21) [Reduced Degree]. For \( k \in \text{Field} \) and \( B \) a finite semisimple \( k \)-algebra, suppose \( B = \prod_i B_i \) where \( B_i \) are simple \( k \)-algebras with center \( k_i \), define the **reduced degree** of \( B \) over \( k \) to be

\[
[B : k]_{\text{red}} = \sum_i [B_i : k_i]^{1/2}[k_i : k],
\]

which is an integer by (2.4.3.16). And for any field extension \( k'/k \),

\[
[B_{k'} : k']_{\text{red}} = [B : k]_{\text{red}}.
\]

**Proof:** ? Why invariant? \( \square \)

Prop. (2.4.3.22). For \( k \in \text{Field} \) and \( B \) a finite semisimple \( k \)-algebra, any maximal étale \( k \)-subalgebra of \( B \) has rank \( [B : k]_{\text{red}} \) over \( k \).

**Proof:** This follows from (2.4.3.13). \( \square \)

Prop. (2.4.3.23). For \( k \in \text{Field} \) and \( B \) a finite semisimple \( k \)-algebra, then for any faithful \( B \)-module \( M \),

\[\dim_k M \geq [B : k]_{\text{red}}.\]

And the equality holds iff \( B \) is split.

**Proof:** This is clear from (2.4.1.21). \( \square \)

Prop. (2.4.3.24). If \( k \in \text{Field} \) and \( A \in \text{Az}_k \), then \( A \otimes_k A^{\text{op}} \cong \text{Mat}(n, k) \), where \( n = \dim_k A \).

**Proof:** There is a map \( A \otimes_k A^{\text{op}} \to \text{End}_k(A) : (a \otimes a') \mapsto (x \mapsto axa') \). By (2.4.3.6), \( A \otimes_k A^{\text{op}} \) is simple, thus this is an injective map, but both sides have the same dimension, thus this is an isomorphism. \( \square \)
Finite Semisimple $k$-Algebras with Involution

**Def. (2.4.3.25) [Involution].** Let $*$ be an involution on a semisimple algebra $B$ over a field $k$. It is called an **involution of first kind** if it fixes elements in the center of $B$. It is called an **involution of second kind** otherwise.

**Prop. (2.4.3.26) [Decomposition].** Let $(B, *)$ be a f.d. semisimple $k$-algebra with an involution, if $k$ is alg.closed and has characteristic 0, then it decomposes as products of pairs of the following types:

- $(A): M_n(k) \times M_n(k), (a, b)^* = (b^t, a^t)$.
- $(C): M_n(k), b^* = b^t$.
- $(BD): M_{2n}(k), b^* = Jb^tJ^{-1}$, where $J = \begin{bmatrix} 0 & -I \\ I & 0 \end{bmatrix}$.

**Proof:** Let $B = B_1 \times \ldots \times B_r$ be the decomposition into products of simple $k$-algebras, where $B_i$ are the minimal two-sided ideals of $B$. Applying $*$, $B = B_1^* \times \ldots \times B_r^*$ so $B_i^*$ is a permutation of $B_i$, so $B$ is a product of algebras either simple or product of two simple algebras that $*$ interchanges them.

If $B$ is simple, then $B \cong M_n(k)$ as $k$ is alg.closed, so $b^* = ub^tu^{-1}$ for some $u \in M_n(k)$ by Skolem-Noether (2.4.3.8). Then $b = b^{**} = (u^t u^{-1})^{-1}bu^t u^{-1}$, so $u^t u^{-1}$ is in the center, denote it by $c$, then $u^t = cu$, $u = c^2 u$, so $c = \pm 1$, and $u$ is symmetric or skew-symmetric. Up to a congruence, we see the situation is $(C)$ or $(BD)$.

The other case is also easy. \qed

4 Idempotented Algebras

**Lemma (2.4.4.1).** Let $R$ be a ring and $e, f$ be idempotents of $R$ that $ef = fe = e$, then $f = e + e'$, where $e'$ is an idempotent and $M[f] = M[e] \oplus M[e']$.

Moreover, if $R$ is an algebra over an alg.closed field $k$ and $M[e]$ is a simple $R[e]$-module of f.d. over $k$, then $\dim \text{Hom}_{R[e]}(M[e], M[f]) = 1$.

**Proof:** Let $e' = f - e$, then it is easily verified to be an idempotent, and $ee' = e'e = 0$, thus $M[f] = M[e] \oplus M[e']$ is clear.

For the second, because $R[e]$ acts by 0 in $R[e']$, $\text{Hom}_{R[e]}(M[e], M[f]) = \text{Hom}_{R[e]}(M[e], M[e])$ has dimension 1, by Shur’s lemma (2.4.1.2) and (2.2.1.10). \qed

**Def. (2.4.4.2) [Idempotented Algebra].** An **idempotented algebra** $\mathcal{H}$ is an algebra over a field $k$ together with a set $\mathcal{E}$ of idempotents that if $e_1, e_2 \in \mathcal{E}$, then there exists $e_0 \in \mathcal{E}$ such that

$$e_0 e_1 = e_1 e_0 = e_1, e_0 e_2 = e_2 e_0 = e_2,$$

and also for any $\varphi \in \mathcal{H}$, there exists $e \in \mathcal{E}$ that $e \varphi = \varphi e = \varphi$.

We can define a partial order on $\mathcal{E}$: $e < f$ iff $ef = fe = f$, then this order is cofinal.

If $e$ is an idempotent, denote $\mathcal{H}[e] = e \mathcal{H} e$, which is a subring of $\mathcal{H}$ with unit $e$. Also if $M$ is an $\mathcal{H}$-module, we denote $M[e]$ the $R[e]$-module $eM$.

**Prop. (2.4.4.3).** If $0 \rightarrow M_1 \rightarrow M_2 \rightarrow M_3 \rightarrow 0$ is an exact sequence of $\mathcal{H}$-modules, $e \in \mathcal{E}$, then $0 \rightarrow M_1[e] \rightarrow M_2[e] \rightarrow M_3[e] \rightarrow 0$ is also exact.

**Proof:** Because tensoring an idempotent is exact. \qed
Def. (2.4.4.4) [Smooth Representations of Idempotented Algebras]. Let \((\mathcal{H}, \mathcal{E})\) be an idempotented algebra, a smooth \(\mathcal{H}\)-module \(M\) is an \(\mathcal{H}\)-module \(M = \bigcup_{e \in \mathcal{E}} M[e]\), and an admissible \(\mathcal{H}\)-module is a smooth \(\mathcal{H}\)-module that each \(M[e]\) is of f.d. over \(k\).

A smooth \(\mathcal{H}\)-module is clearly non-degenerate.

Def. (2.4.4.5) [Contragradient Module]. If \(M\) be a smooth \(\mathcal{H}\)-module, then we can define a contragradient \(\hat{M}\) of \(M\), which is the smooth \(\mathcal{H}\)-module consisting of smooth vectors in \(M^*\), where the action is defined as \(((\varphi)m)(m) = \lambda(x)m\). Notice if \(M\) is admissible, then so does \(\hat{M}\), because an element in \(M[e]\) is determined by its restriction on \(M[\ell(e)]\), so \(\hat{M}[e]\) is of f.d. if \(M[\ell(e)]\) does.

Prop. (2.4.4.6) [Simpleness Checked on Idempotents]. Let \(M\) be a non-zero module over an idempotented algebra \((\mathcal{H}, \mathcal{E})\) over \(C\), \(\mathcal{E}^0\) be a cofinal subset of \(\mathcal{E}\), then \(M\) is a simple \(\mathcal{H}\)-module iff \(M[e]\) is simple \(\mathcal{H}[e]\)-modules for any \(e \in \mathcal{E}^0\).

Proof: If there exists a proper \(\mathcal{H}\)-submodule \(M_1\) of \(M\), then \(M/M_1 = M_2\), then \(M[e]/M_1[e] = M_2[e]\) for all \(e\) by (2.4.4.3). Thus we can choose \(e\) s.t. \(M_1[e] \neq 0, M_2[e] \neq 0\), thus \(M[e]\) is reducible. Conversely, If \(W_0 \subset M[e_K]\) is a proper non-zero \(\mathcal{H}[e_K]\)-submodule, then \([\pi(\mathcal{H})W_0][e] = W_0\), thus \(\pi(\mathcal{H})W_0\) is a proper submodule of \(M\).

Prop. (2.4.4.7) [Isomorphism Checked on Idempotents]. Let \(V_1, V_2\) be two simple admissible modules over an idempotented algebra \((\mathcal{H}, \mathcal{E})\), if \(e \in E\) that \(V_1[e] \cong V_2[e] \neq 0\), then \(V_1 \cong V_2\).

Proof: Choose an isomorphism \(j: V_1[e] \rightarrow V_2[e]\), then the subspace \(V' = \{(x, xj) \subseteq V_1[e] \oplus V_2[e] \subset V_1 \oplus V_2\) is a \(\mathcal{H}[e]\)-submodule. Let \(V = \pi(\mathcal{H})V'\), then \(V[e] = V'\), so \(V\) is not contained or contains any of \(V_1\) or \(V_2\), thus \(V \cap V_1 = V \cap V_2 = 0\) as \(V_i\) are irreducible. Thus the projections \(V \rightarrow V_1, V \rightarrow V_2\) are isomorphisms as \(V_i\) are irreducible, and \(V_1 \cong V_2\).

Prop. (2.4.4.8) [Extension Theorem]. Let \((\mathcal{H}, \mathcal{E})\) be an idempotented algebra and \(e \in E\). If \(V_e\) is a simple \(\mathcal{H}[e]\)-module, then there is a simple \(\mathcal{H}\)-module \(V\) that \(V[e] = V_e\).

Proof: Let \(V_e \cong \mathcal{H}[e]/I\), where \(I\) is a left ideal of \(V_e\). Let \(E_1, E_2\) be the module generated by \(I\) and \(\mathcal{H}[e]\) in \(\mathcal{H}\) by left action of \(\mathcal{H}\), then \(E_1[e] = I\) and \(E_2[e] = \mathcal{H}[e]\), thus \((E_3 = E_1/E_2)[e] \cong V_e\) by (2.4.4.3). Now if \(E'\) is a submodule of \(E_3\), then either \(E'[e] = 0\) thus \((E_3/E')[e] \cong L\), or \(E'[e] = L\), thus \(E' = E_3\) by (2.4.4.7). Thus if we choose the proper submodule \(E'\) that \(E_3/E'\) is irreducible by (15.1.1.21), then \(E_3/E'[e] = L\).

Prop. (2.4.4.9). If \(\mathcal{H}\) is an idempotented algebra, then \(\mathcal{M}(\mathcal{H})\) has enough projectives.

Proof: For any idempotent \(e \in \mathcal{H}\), consider the module \(\mathcal{H}e\), then it is projective, because \(\text{Hom}_{\mathcal{H}}(\mathcal{H}e, X) = e.X\), thus it is clearly exact. Now any \(m \in V\) has an idempotent \(e \in \mathcal{H}\) that \(ev = v(\text{use definition})\). Thus by taking the direct sum, we are done.

### Spherical Idempotents

Def. (2.4.4.10) [Spherical Idempotents]. Let \((\mathcal{H}, \mathcal{E})\) be an idempotented algebra over a field \(\Omega\). Then an idempotent \(e \in \mathcal{E}\) is called spherical idempotent if there exists an anti-involution \(\iota: \mathcal{H} \rightarrow \mathcal{H}\) that \(\iota(x) = x\) for any \(x \in \mathcal{H}[e^0]\). Notice this implies \(\mathcal{H}[e^0]\) is commutative, as \(xy = \iota(xy) = yx\).
Def. (2.4.4.11) [Spherical Vectors]. Let \( e^0 \) be a spherical idempotent of the idempotented algebra \((\mathcal{H}, \mathcal{E})\) and \( \iota \) is the corresponding involution. If \( M \) is an admissible \( \mathcal{H} \)-module, then a spherical (unramified) module is a \( \mathcal{H} \)-module \( M \) that \( M[e^0] \neq 0 \), and elements in \( M[e^0] \) are called spherical vectors.

Then if \( M \) is simple and spherical, then \( M \) has at most one spherical vector up to scalar, and \( \hat{M} \) is also spherical. Thus the space of spherical vectors is fixed by \( \mathcal{H}[e^0] \), and the action of \( \mathcal{H}[e^0] \) on that defines a spherical character.

Proof: In fact, \( M[e^0] \) is a simple \( \mathcal{H}[e^0] \)-module(2.4.4.6), and is of f.d., and \( \mathcal{H}[e^0] \) is commutative(2.4.4.10), so(2.4.1.11) shows it is of dimension 1. so if \( m^0 \neq 0 \in M[e^0] \), then we can define a \( \hat{m}^0 \neq 0 \in M[e^0] \) as:

\[ e^0 m = \hat{m}^0(m) \cdot m^0. \]

Prop. (2.4.4.12) [Isomorphism Checked on Spherical Idempotents]. Let \((\mathcal{H}, \mathcal{E})\) be an idempotented algebra over a field \( \Omega \) and \( e^0 \) is a spherical idempotent. If \( M, N \) are simple admissible spherical \( \mathcal{H} \)-modules that \( M[e^0] \cong N[e^0] \) over \( \mathcal{H}[e^0] \), then \( M \cong N \) as \( \mathcal{H} \)-modules.

Proof: This follows from(2.4.4.7).

Restricted Tensor Product

Def. (2.4.4.13) [Restricted Tensor Product]. Give an infinite number of vector spaces \( V_v \) indexed by a set \( \Sigma \) and elements \( x_v^0 \in V_v \) be given for a.e. \( v \), we can define the restricted tensor product \( \bigotimes V_v \) as the direct limit

\[ \lim_{S \subseteq \Sigma \text{ finite}} \bigotimes_{v \in S} V_v. \]

It can be thought of as the vector spaces spanned by all symbols \( \otimes_v x_v \) where \( x_v = x_v^0 \) for a.e. \( v \).

Notice if \( V_v \) are idempotented algebras and \( x_v^0 \in V_v \) are idempotents for a.e. \( v \), then \( \prod V_v \) also has a natural idempotented algebra structure.

Def. (2.4.4.14) [Tensor Product Module of Idempotented Algebras]. Given a set of idempotented algebras \( (\mathcal{H}_v, \mathcal{E}_v) \) and specify an idempotent \( e_v^0 \) for a.e. \( v \). Let \( M_v \) be \( \mathcal{H}_v \)-modules over \( k \) for all \( v \), and assume \( M_v[e_v^0] \) be of dimension 1 a.e. \( v \), and specify a.e. a non-zero element \( m_v^0 \in M_v[e_v^0] \)

Then we can define tensor product(2.4.4.13) \( \prod \mathcal{H}_v \) which is an idempotented algebra and \( \prod M_v \).

Then we can define an restricted tensor module structure of \( M_v \) over \( \prod \mathcal{H}_v \) by the action

\[ (\otimes_v \varphi_v)x_v = \otimes_v (\varphi_v)x_v. \]

Lemma (2.4.4.15) [Simple Module of Tensor Product]. Let \( (\mathcal{H}_1, \mathcal{E}_1), (\mathcal{H}_2, \mathcal{E}_2) \) be idempotented algebras over an alg.closed field \( \Omega \), and let \((\mathcal{H}, \mathcal{E})\) be the tensor product. If \( M_1, M_2 \) are simple admissible modules over \( \mathcal{H}_1, \mathcal{H}_2 \), respectively, then \( M_1 \otimes M_2 \) are simple admissible modules over \( \mathcal{H}_1 \otimes \mathcal{H}_2 \), and any simple admissible module over \( \mathcal{H} \) comes uniquely from a pair \( (M_1, M_2) \) like this.

Proof: If \( M_1, M_2 \) are simple admissible over \( H_1, H_2 \) respectively, then if \( e_1 \in \mathcal{E}_1, e_2 \in \mathcal{E}_2 \), then \( (M_1 \otimes M_2)(e_1 \otimes e_2) = M_1[e_1] \otimes M_2[e_2] \) is simple and of f.d. by(2.4.4.6) and(2.4.1.16), so \( M_1 \otimes M_2 \) is simple by(2.4.4.6).
Now if $M$ is simple admissible over $\mathcal{H}_1 \otimes \mathcal{H}_2$, then we find an $e_1^0 \otimes e_2^0 \in \mathcal{E}$ that $M[e_1^0 \otimes e_2^0] \neq 0$. Let $\mathcal{E}_i^0 = \{ e_i \in \mathcal{E}_i | e_i < e_i^0 \}$, then $\mathcal{E}_i^0$ is cofinal in $\mathcal{E}_i$. Then for any $e_i \in \mathcal{E}_i^0$, $M[e_1 \otimes e_2]$ is non-zero thus simple, thus it is of the form

$$M[e_1 \otimes e_2] = M_1(e_1, e_2) \otimes M_2(e_1, e_2)$$

where $M_i(e_1, e_2)$ are simple $\mathcal{H}[e_i]$-modules by (2.4.1.16).

Now we show that $M_2(e_1, e_2)$ depends only on $e_1$: it suffices to show $M_2(e_1, e_2) = M_2(f_1, e_2)$ for $f_1 < e_1$. For this, notice that for any idempotents $g_1, g_2$,

$$M[g_1 \otimes g_2] = M_1(g_1, g_2) \otimes M_2(g_1, g_2)$$

is a finite direct sum of simple modules $M_2(g_1, g_2)$ as an $\mathcal{H}_2[g_2]$-module. Notice that by (2.4.4.1), $M[e_1 \otimes e_2] = M[f_1 \otimes e_2] \oplus M[e' \otimes e_2]$ for $e' = f_1 - e_1$, so by (2.4.1.3), $M_2(f_1, e_2) = M_2(e_1, e_2)$.

Similarly we know $M_1(e_1, e_2)$ only depends on $e_1$.

Next we have:

$$\dim_k \text{Hom}_{\mathcal{H}_1}[e_1](M_1[e_1], M_1[f_1]) \geq 1, \quad f_1 \leq e_1.$$ 

and similar for $\mathcal{H}_2$. For this, it suffices to prove that $\dim_k \text{Hom}_{\mathcal{H}_1}[e_1](M[e_1 \otimes e_2], M[f_1 \otimes e_2]) \geq 1$, by what we just said, but this is by the decomposition

$$M[e_1 \otimes e_2] = M[f_1 \otimes e_2] \oplus M[e' \otimes e_2]$$

above. But

$$\dim_k \text{Hom}_{\mathcal{H}_1}[e_1] \otimes \mathcal{H}_2[e_2] \cdot (M_1(e_1) \otimes M_2(e_2), M_1(f_1) \otimes M_2(f_2)) = 1, \quad f_1 \leq e_1, f_2 \leq e_2$$

by (2.4.4.1), so the $\geq$ above should change to $=.$

Now we know the homomorphism is of dimension 1, we want to choose a family of maps that is compatible for $g_1 \leq f_1 \leq e_1 \leq e_0^1$. For this, we can choose the maps $\lambda(e_1, e_0^1)$ arbitrarily, then choose $\lambda(e_1, f_1)$ to be compatible with $\lambda(e_1, e_0^1)$ and $\lambda(f_1, e_0^1)$, then these are compatible choices. Hence we can define a direct limit

$$M_1 = \lim_{\rightarrow (e_0^1)^{op}} M(e_1).$$

It is easy to see $M_1(e_1) \to M_1$ are all injective, and $M_1(e_1) = M[e_1]$. Similarly, we can define an $M_2$ that $M_2[e_2] = M_2(e_2)$.

Finally, we have

$$M[e_1 \otimes e_2] = M_1[e_1] \otimes M_2[e_2] = (M_1 \otimes M_2)[e_1 \otimes e_2]$$

for all $e_1 \in \mathcal{E}_1^0, e_2 \in \mathcal{E}_2^0$, thus $M \cong M_1 \otimes M_2$ by (2.4.4.7).

As for the uniqueness of $M_1, M_2$, notice the decomposition of $M[e_1 \otimes e_2]$ is unique by (2.4.1.16), so $M_i[e_i]$ is uniquely determined, thus by (2.4.4.7) $M_i$ are determined.

Prop. (2.4.4.16) [Flath Theorem]. Let $(\mathcal{H}_c, \mathcal{E}_v)$ be an indexed family of idempotent $k$-algebras, and for a.e. $v$ let $e_v^0 \in \mathcal{E}_v$ be a spherical idempotent. Let $(\mathcal{H}, \mathcal{E})$ be the restricted tensor product of $\mathcal{H}_c$ w.r.t. $e_v^0$, which is an idempotent algebra. For each $v \in \Omega$, there is a simple $\mathcal{H}_v$-module $M_v$ and for a.e. $v$ we specify a non-zero spherical vector. Let $\otimes_v M_v$ be the tensor product module, then it is a simple admissible $\mathcal{H}$-module, and every simple admissible module is of this type, with $M_v$ uniquely determined.
Proof: Firstly the tensor product is simple and admissible: For any idempotent $e = \otimes e_v \in \mathcal{E}$, there is a finite set $S$ that if $v \notin S$, then $e_v = e_v^0$, hence for these $v \dim M_v[e_v] = 1$. Then

$$M[e] = \otimes_{v \in S} M_v[e_v].$$

which is simple of f.d. by (2.4.4.15), so $M$ is simple admissible by (2.4.4.6).

Conversely, for any simple $\mathcal{H}$-module $M$, we need to show it is a tensor product. If there are only f.m. indices, then this follows from (2.4.4.15).

Suppose first that $e_0^v$ is defined and spherical for all $v$, and $e = \otimes e_0^v$, and $M[e] \neq 0$. Then $\dim M[e] = 1$ (2.4.4.11). Let $m$ be a spherical vector, then there is a ring homomorphism $\gamma : \mathcal{H}[e] \rightarrow k$ defined by $hm = \gamma(h)m$. Because $\mathcal{H}[e] = \otimes'_v M_v[e_0^v]$, we have

$$\gamma(\otimes_v h_v) = \prod_v \gamma_v(h_v).$$

Now if we decompose $\mathcal{H} = \mathcal{H}_v \otimes \mathcal{H}_v'$, then by (2.4.4.15), there exists simple admissible module $M_v$ over $\mathcal{H}_v$, $M_v'$ over $\mathcal{H}_v'$ respectively, that $M = M_v \otimes M_v'$, thus $M[e] = M_v[e_0^v] \otimes M_v'[e_0^v]$. Now consider $M_v$ for all $v$, and $N = \otimes'_v M_v$ w.r.t. $m_v$, then it is simple admissible $\mathcal{H}$-module, and we have $N[e] = \otimes'_v M_v[e_0^v] \cong M[e]$ as $\mathcal{H}[e]$-modules of dimension 1, which is because they are both simple and have the same character

$$\gamma(\otimes_v h_v) = \prod_v \gamma_v(h_v).$$

Hence $M \cong N$, by (2.4.4.12).

Now the general case follows from the two situations above: choose $e \in \mathcal{E}$ that $M[e] \neq 0$, then let $S$ be large that for $v \notin S$, $e_v = e_v^0$. Then we decompose $\mathcal{H}$ as $\mathcal{H} = \otimes_{v \in S} \mathcal{H}_v \otimes (\otimes_{v \notin S} H_v)$, then

$$M = \bigotimes_{v \in S} M_v \otimes M_v' = \bigotimes_{v \in S} M_v \otimes (\bigotimes_{v \notin S} M_v) = \otimes_{v \notin S} M_v.$$

□

5 Miscellaneous

Lemma (2.4.5.1). Let $R$ be a (possibly non-commutative) unital ring of characteristic 0 with the following properties:

- $R$ has no zero-divisors,
- rankZ $R \leq 4$,
- $R$ has an involution $(-)^\wedge : R \rightarrow R^{\text{op}}$,
- For any $\alpha \in R$, $\alpha \bar{\alpha} \in \mathbb{N}$, and $\alpha \bar{\alpha} = 0$ iff $\alpha = 0$.

Then $R$ is isomorphic to exactly one of the following:

- \Z.
- an order in an imaginary quadratic extension over \Q.
- an order in a definite quaternion algebra over \Q.

And the third case won’t happen in characteristic 0, by (13.8.1.24).
Proof: It suffices to show $K = R \otimes_{\mathbb{Z}} \mathbb{Q}$ is either $\mathbb{Q}$, an imaginary quadratic field or a definite quaternion algebra. For $\alpha \in K$, denote $N\alpha = \alpha \hat{\alpha}$, $\text{tr} \alpha = \alpha + \hat{\alpha}$, then $\text{tr} \alpha = 1 + N\alpha - N(1 - \alpha) \in \mathbb{Q}$.

Assume $K \neq \mathbb{Q}$, let $\alpha \in K \setminus \mathbb{Q}$. We may replace $\alpha$ by $\alpha - \frac{1}{2} \text{tr} \alpha$ to assume $\text{tr} \alpha = 0$, then $\alpha^2 = -N\alpha < 0 \in \mathbb{Z}$. So $\mathbb{Q}(\alpha)$ is an imaginary quadratic field.

Assume $K \neq \mathbb{Q}(\alpha)$, let $\beta \in K \setminus \mathbb{Q}(\alpha)$. We may replace $\beta$ by $\beta - \frac{1}{2} \text{tr} \beta - \frac{\text{tr}(\alpha \beta)}{\alpha^2} \alpha$ to assume $\text{tr}(\beta) = \text{tr}(\alpha \beta) = 0$. Hence $\beta^2 = -N\beta < 0 \in \mathbb{Z}$, and $\alpha \beta = -\beta \alpha$. So $\mathbb{Q}(\alpha, \beta)$ is a definite quadratic extension of $\mathbb{Q}$. Then $K = \mathbb{Q}(\alpha, \beta)$ because they are has rank 4 over $\mathbb{Z}$. $\square$


2.5 Lie Algebras

Basic references are [Car05], [Ser87], [Mil13], [Kna96], [Lie Algebras and Lie Groups Serre], and [Eti21].

In this section, if not otherwise pointed out, $k$ is assumed to be a field of char0 or just $C$.

1 Basics

Def.(2.5.1.1)[Lie Algebras]. A Lie algebra $L$ is an non-associative algebra over a field $k$ with a bilinear Lie bracket operation that satisfies:

$$[x, x] = 0, \quad [xyz] = [[xy]z] + [yzx]$$ (Jacobi Identities).

It is easily deduced that $[xy] = -[yx]$.

Denote $\text{ad}_x(y) = [xy]$, then $\text{ad}_x$ are all derivatives of $L$.

An element $x \in \mathfrak{g}$ is called nilpotent or semisimple if $\text{ad}_x$ is nilpotent or semisimple.

Prop.(2.5.1.2)[Associative Algebra]. For any associative algebra $A$ over $k$, it can be given naturally a Lie algebra structure by defining $[xy] = xy - yx$. In this way, we get a natural functor $\text{AssAlg}_k \to \text{Lie}_k: A \mapsto [A]$.

Prop.(2.5.1.3)[Derivatives form a Lie Algebra]. Given a $k$-algebra $A$, the set of derivatives $\text{Der}_k(A) = \text{Der}_k(A, A)$ is a Lie algebra under the associative bracket.

Proof: \[ [D_1, D_2](ab) = D_1(D_2(a)b + aD_2(b)) - D_2(D_1(a)b + aD_1(b)) = D_1D_2(a)b + D_2(a)D_1(b) + D_1(a)D_2(b) + aD_1D_2(b) - (D_2D_1(a)b + D_1(a)D_2(b) + D_2(a)D_1(b) + aD_2D_1(b)) = [D_1, D_2](a)b + a[D_1, D_2](b) \]

□

Prop.(2.5.1.4)[Base Change of Fields]. Let $\mathfrak{a}$ be a subalgebra of a Lie algebra $\mathfrak{g}$ over $k$, and $k'/k$ a field extension, then $\mathfrak{a}_{k'}$ is a subalgebra of $\mathfrak{g}_{k'}$, and

$$N_{\mathfrak{g}_{k'}}(\mathfrak{a}_{k'}) = N_{\mathfrak{g}}(\mathfrak{a})_{k'},$$

$$e_{\mathfrak{g}_{k'}}(\mathfrak{a}_{k'}) = e_{\mathfrak{g}}(\mathfrak{a})_{k'}.$$

Proof: This is because the normalizer and centralizer is defined by linear equations with coefficients in $k$, thus the vector space is defined over $k$.

□

Prop.(2.5.1.5). Let $D$ be a derivative of a $k$-algebra $A$ that is nilpotent, then $e^D$ is an automorphism of $A$(as an algebra).

Proof: Routine calculation.

□

Def.(2.5.1.6)[Semidirect Product of Lie Algebras]. Let $\mathfrak{g}, \mathfrak{h}$ be Lie algebras and $\tau: \mathfrak{g} \to \text{Der}(\mathfrak{h})$, then we can define a semi-direct product Lie algebra $\mathfrak{g} \ltimes \mathfrak{h}$ that is isomorphic to $\mathfrak{g} \oplus \mathfrak{h}$ as vector spaces, and $\mathfrak{g}, \mathfrak{h}$ are subalgebras of $\mathfrak{g} \ltimes \mathfrak{h}$, with $[g, h] = \tau(g)(h)$. It can be shown that this is truly a Lie algebra.
Def. (2.5.1.7) [Elementary Automorphisms]. Let \( g \) be a Lie algebra, a \textbf{special automorphism} is an automorphism of \( g \) of the form \( e^{ad_x} \), where \( x \) is in the nilpotent radical (2.5.1.34).

The group of \textbf{elementary automorphisms} is the subgroup of the automorphism group of \( g \) generated by the automorphisms of the form \( e^{ad_x} \) where \( ad(x) \) is nilpotent.

Def. (2.5.1.8) [Ideals]. A subspace \( a \subset g \) is called an \textbf{ideal} of \( g \) iff \([g,a] \subset a\). If \( I \) is an ideal of \( L \), then \( L/I \) can be made into a Lie algebra by defining \([I + x, I + y] = I + [xy]\).

Def. (2.5.1.9) [Center]. The \textbf{center} of a Lie algebra \( g \) is the elements \( a \) that \( ad a = 0 \). It is an ideal.

Def. (2.5.1.10) [Simple Lie Algebras]. A Lie algebra \( g \) is called \textbf{simple} if it is not 1-dimensional and it has no nontrivial ideal.

Def. (2.5.1.11) [Lie Algebra of Affine Maps]. Let \( V \) be a f.d. \( k \)-vector space. If we regard \( V \) as a commutative algebra, then \( \text{Der}_k(V) = \mathfrak{gl}_V \). Then \( V \times \mathfrak{gl}_V \) is a Lie algebra, denoted by \( \mathfrak{af}(V) \).

Let \( V' = V \oplus k \), and let \( \mathfrak{h} = \{ w \in \mathfrak{gl}_V, |w(V') \subset V \} \), which is a Lie subalgebra of \( \mathfrak{gl}_V \). If we define

\[
\eta : \mathfrak{h} \to \mathfrak{gl}_V : \eta(w) = w|_V, \quad \zeta : \mathfrak{h} \to V : \zeta(w) = w(0,1),
\]

then \((\eta, \zeta)\) defines a Lie algebra homomorphism from \( \mathfrak{h} \) to \( \mathfrak{af}(V) \). This map is bijective, with the inverse given by sending \((v, f) \in \mathfrak{af}(V)\) to the morphism

\[
(v', c) \mapsto (f(v') + cv, 0).
\]

Lemma (2.5.1.12). Let \( \lambda, \mu \in k \) and \( x, y, z \in g \), then we have

\[
(ad(x) - \lambda - \mu)^m[y, z] = \sum_{i=1}^m \left( \begin{array}{c} m \\ i \end{array} \right) [(ad(x) - \lambda)^iy, (ad(x) - \mu)^m-i]z].
\]

Proof:

\[
(ad(x) - \lambda - \mu)^m[y, z] = \sum_{p+q+r+s=m} (-1)^{r+s} \frac{m!}{p!q!r!s!} \lambda^r \mu^s [(ad x)^p(y), (ad x)^q(z)]
\]

\[
= \sum_{k+l=m} \frac{m!}{k!l!} [(ad(x) - \lambda)^ky, (ad(x) - \mu)^lz]
\]

\( \square \)

Def. (2.5.1.13) [Killing Form]. A bilinear form \( B \) on \( g \) is called \textbf{invariant} if \( B([x, y], z) + B(x, [y, z]) = 0 \).

The \textbf{Killing form} on a Lie algebra \( g \) of f.d. is the invariant symmetric bilinear form defined by

\( B(x, y) = \text{tr}(ad x \circ ad y) \).

If \( a \) is an ideal of a Lie algebra \( g \), then the Killing form on \( a \) is that of the Killing form on \( a \) as a Lie algebra. This is linear algebra.

Prop. (2.5.1.14). Any invariant symmetric bilinear form on a \textbf{simple} Lie algebra \( g \) is a multiple of the Killing form.

Prop. (2.5.1.15). A subalgebra \( h \) of a Lie algebra \( g \) is commutative if it consists of semisimple elements.
Proof: For an element \( x \in \mathfrak{h} \), we need to show that \( \text{ad}_\mathfrak{a}(x) = 0 \). If it is not, because \( \text{ad}_\mathfrak{h}(x) \) is semisimple by (2.3.6.8), there is a nonzero eigenvector \( y \) at least after a base change, so \([x, y] = cy, y \neq 0 \in \mathfrak{h} \). So \( \text{ad}(y)(x) = -cy \), and \( \text{ad}(y)^2(x) = 0 \), so \( \text{ad}(y) \) is non-semisimple on the subspace \( \{x, y\} \), which means \( \text{ad}(y) \) is non-semisimple on \( \mathfrak{q} \), by (2.3.6.8) again. \( \square \)

Lemma (2.5.1.16). If \( \mathfrak{g} \subset \mathfrak{g}_n \) is a Lie subalgebra, and \( a \in \mathfrak{g} \) is a nilpotent matrix, then \( \text{ad}(a) \) is also nilpotent.

Proof: This is because \( \text{ad}(a) = l(a) - g(a) \), where \( l(a) \) is left multiplication and \( r(a) \) is right multiplication. The left and right multiplication commutes, so it is clear \( \text{ad}(a)^{2n} = 0 \) if \( \text{ad}(a)^n = 0 \). \( \square \)

Nilpotent and Solvable Lie Algebras

Def. (2.5.1.17)[Nilpotent and Solvable Lie Algebras]. Let \( \mathfrak{g} \) be a Lie algebra, the lower central series of \( \mathfrak{g} \) is the descending sequence of ideals of \( \mathfrak{g} \) defined inductively by \( C^1\mathfrak{g} = \mathfrak{g} \) and \( C^n\mathfrak{g} = [\mathfrak{g}, C^{n-1}\mathfrak{g}] \).

Let \( \mathfrak{g} \) be a Lie algebra, the derived series of \( \mathfrak{g} \) is the descending sequence of ideals of \( \mathfrak{g} \) defined inductively by \( D^1\mathfrak{g} = \mathfrak{g} \) and \( D^n\mathfrak{g} = [D^{n-1}\mathfrak{g}, D^{n-1}\mathfrak{g}] \).

A Lie algebra is called nilpotent if there is an \( n \) that \( C^n\mathfrak{g} = 0 \). This is equivalent to \( \text{ad} x_1 \text{ad} x_2 \ldots \text{ad} x_n = 0 \) for any \( n \) element \( x_1, \ldots, x_n \). It is called solvable if \( D^n = 0 \) for some \( n \). It is clear that \( D^n \subset C^n \), so nilpotent Lie algebra is solvable.

Prop. (2.5.1.18). The lower central series satisfies: \([C^n\mathfrak{g}, C^m\mathfrak{g}] \subset C^{m+n}\mathfrak{g}\).

The operation of taking derived series or lower central series commutes with base change of fields.

Proof: Prove by induction on \( n \): \( n = 0, 1 \) is trivial, and if the assertion is true for \( n \geq k \), then for \( n = k + 1 \), \([C^n\mathfrak{g}, C^m\mathfrak{g}] \subset [\mathfrak{g}, [C^{n-1}\mathfrak{g}, C^m\mathfrak{g}]] + [C^{n-1}\mathfrak{g}, C^{m+1}\mathfrak{g}] \subset C^{m+n}\mathfrak{g}\). \( \square \)

Cor. (2.5.1.19). Let \( \mathfrak{g} \) be a Lie algebra over a field \( k \), and \( k'/k \) is a field extension, then \( \mathfrak{g} \) is solvable/nilpotent iff \( \mathfrak{g} \otimes_k k' \) is solvable/nilpotent.

Prop. (2.5.1.20). If \( \mathfrak{g} \) is a nilpotent Lie algebra, then for any subalgebra \( \mathfrak{h} \subseteq \mathfrak{g} \), \( N_{\mathfrak{g}}(\mathfrak{h}) \neq \mathfrak{h} \).

Proof: Because \( \mathfrak{g}^n = 0 \) for some \( n \), take \( n \) to be the maximal one that \( \mathfrak{h} \not\subset \mathfrak{g}^n \), then \( [\mathfrak{g}^n, \mathfrak{h}] \subset \mathfrak{g}^{n+1} \subset \mathfrak{h} \), so \( \mathfrak{g}^n \subset N_{\mathfrak{g}}(\mathfrak{h}) \), so \( N_{\mathfrak{g}}(\mathfrak{h}) \neq \mathfrak{h} \). \( \square \)

Prop. (2.5.1.21). Subalgebras, quotient algebras and extension algebras of solvable algebras are solvable.

Proof: Let \( \mathfrak{h} \subset \mathfrak{g} \), then \( D^n(\mathfrak{h}) \subset D^n(\mathfrak{g}) \), so if \( \mathfrak{g} \) is solvable, then so is \( \mathfrak{h} \). Also the quotient is clearly solvable. For an extension of Lie algebras

\[ 0 \rightarrow \mathfrak{h} \rightarrow \mathfrak{g} \rightarrow r \rightarrow 0, \]

if \( \mathfrak{h}, r \) are both solvable, let \( D^m(\mathfrak{h}) = 0, D^n(r) = 0 \), then the image of \( D^n(\mathfrak{g}) \) is 0 in \( r \), so \( D^n(\mathfrak{g}) \subset \mathfrak{h} \), so \( D^{m+n}(\mathfrak{g}) = 0 \). \( \square \)

Cor. (2.5.1.22)[Radical]. If \( \mathfrak{a}, \mathfrak{b} \) are solvable ideals of a Lie algebra \( \mathfrak{g} \), then the ideal \( \mathfrak{a} + \mathfrak{b} \) is also solvable, because \( 0 \rightarrow \mathfrak{a} \rightarrow \mathfrak{a} + \mathfrak{b} \rightarrow \mathfrak{b}/\mathfrak{a} \cap \mathfrak{b} \).

Let \( \mathfrak{r} \subset \mathfrak{g} \) be the sum of all solvable ideals of \( \mathfrak{g} \), called the radical \( \text{Rad}(\mathfrak{g}) \). When \( \mathfrak{g} \) is of f.d., this is the maximal solvable ideal.
Def. (2.5.1.23) [Semisimple Lie Algebra]. A Lie algebra \( L \) is called **semisimple** if \( \text{Rad} \ L = 0 \), or equivalently \( \mathfrak{g} \) has no solvable ideals or no commutative ideals. Notice \( L/\text{Rad}(L) \) is semisimple, by (2.5.1.22).

Prop. (2.5.1.24) [Lie]. Let \( \mathfrak{g} \subseteq \mathfrak{gl}(V) \) be a solvable lie algebra over an alg.closed field \( k \) of char\(0\), then \( \mathfrak{g} \) is upper triangular. Equivalently, there exists a vector \( v \in V \) which is a common eigenvector for all \( X \in \mathfrak{g} \), and moreover equivalently, any irreducible representation of \( \mathfrak{g} \) is 1-dimensional.

**Proof:** Idea is to prove by induction on dimension of \( \mathfrak{g} \).

Produce a codimension 1 ideal \( \mathfrak{h} \) of \( \mathfrak{g} \). Let \( \mathfrak{g} \) be generated (as a vector space) by \( \mathfrak{h} \) and \( Y \). Being a subalgebra of solvable algebra \( \mathfrak{g} \), \( \mathfrak{h} \) is itself a solvable lie algebra. Apply induction step on \( \mathfrak{h} \) and choose \( v \in V \) such that \( v \) is an eigenvector for all \( X \in \mathfrak{h} \).

The idea is to consider set \( W \) all common eigenvectors of elements of \( \mathfrak{h} \) and produce an eigenvector of \( Y \) from this \( W \). Let

\[
W = \{ v \in V | X(v) = \lambda(X)v \; \forall \; X \in \mathfrak{h} \; \text{for a fixed} \; \lambda(X) \in \mathbb{C} \}.
\]

Suppose \( W \) is an invariant subspace of \( Y \), we then have restriction map \( Y : W \to W \). As we are in complex vector space (algebraically closed) there exists an eigenvector for \( Y \) in \( W \) say \( w_0 \). Thus, \( w_0 \) is common eigenvector for all elements of \( \mathfrak{g} \).

It remains to show that \( W \) is an invariant subspace of \( Y \) i.e., \( Y(w) \in W \) for all \( w \in W \) i.e., given \( X \in \mathfrak{h} \), we need to have \( X(Y(w)) = \lambda(X)Y(w) \).

Let \( w \in W \), we have

\[
X(Y(w)) = Y(X(w)) + [X,Y](w) = Y(\lambda(X)w) + \lambda([X,Y])w = \lambda(X)Y(w) + \lambda([X,Y])w.
\]

This is almost the same as what we want but with an extra term \( \lambda([X,Y])w \). Suppose we prove \( \lambda([X,Y]) = 0 \) for all \( X \in \mathfrak{h} \) then we are done.

Then considers subspace \( U \) spanned by elements \( \{w, Y(w), Y^2(w), \cdots\} \) and then says that \( U \) is invariant subspace of each element of \( \mathfrak{h} \) and (assuming \( n \) is the smallest integer such that \( Y^{n+1}w \) is in the subspace generated by \( \{w, Y(w), \cdots, Y^n(w)\} \)) representation of an element \( Z \) of \( \mathfrak{h} \) with the basis \( \{w, Y(w), \cdots, Y^n(w)\} \) is an upper triangular matrix with \( \lambda(Z) \) in the diagonal. So, \( \text{tr}(Z) = n\lambda(Z) \).

So, \( \text{tr}([X,Y]) = n\lambda([X,Y]) \). As \( [X,Y] = XY - YX \), we have \( \text{tr}([X,Y]) = \text{tr}(XY) - \text{tr}(YX) = 0 \). Thus, \( \lambda([X,Y]) = 0 \) and we are done. \( \square \)

Cor. (2.5.1.25). If \( \mathfrak{g} \) is a solvable algebra over an alg.closed field \( k \) of char \(0\), then all irreducible representations of \( \mathfrak{g} \) is of dimension \( 1 \).

Cor. (2.5.1.26). \( \mathfrak{g} \) is a solvable algebra iff \( [\mathfrak{g}, \mathfrak{g}] \) is nilpotent.

**Proof:** If \([\mathfrak{g}, \mathfrak{g}]\) is nilpotent, then clearly \( \mathfrak{g} \) is solvable. Conversely, if \( \mathfrak{g} \) is solvable, we need to prove \([\mathfrak{g}, \mathfrak{g}]\) is nilpotent. For this, we can assume \( k \) is alg.closed, and then \( \text{ad}(\mathfrak{g}) \subseteq \mathfrak{b}_g \) for some basis, thus \( \text{ad}(\mathfrak{g}, \mathfrak{g}) \subseteq \mathfrak{n}_g \) is nilpotent, and the kernel of \( \text{ad} \) is an Abelian subalgebra, so \([\mathfrak{g}, \mathfrak{g}]\) is nilpotent. \( \square \)

Cor. (2.5.1.27). If \( \mathfrak{g} \) is a Lie subalgebra of \( \mathfrak{gl}_n(k) \) where \( k \) is an alg.closed field of char\(0\), then

\[
\mathfrak{g} \text{ is solvable} \iff \text{tr}(xy) = 0, \; \forall \; x \in \mathfrak{g}, \; y \in [\mathfrak{g}, \mathfrak{g}].
\]
Proof: Firstly if $\mathfrak{g}$ is solvable, then by Lie’s theorem, we can assume $\mathfrak{g} \in \mathfrak{b}_V$ the upper-triangular matrices, so $[\mathfrak{g}, \mathfrak{g}] \in \mathfrak{n}_V$ is nilpotent, and so $xy \in \mathfrak{n}_V$ is also nilpotent, and $\text{tr}(xy) = 0$.

Conversely, if $\text{tr}(xy) = 0$ for all $x \in \mathfrak{g}, y \in [\mathfrak{g}, \mathfrak{g}]$, we only need to prove $[\mathfrak{g}, \mathfrak{g}]$ is solvable, so we may change $\mathfrak{g}$ to $[\mathfrak{g}, \mathfrak{g}]$ and assume $\text{tr}(xy) = 0$ for all $x, y \in \mathfrak{g}$.

Now to show $\mathfrak{g}$ is solvable, it suffices to show $[\mathfrak{g}, \mathfrak{g}]$ is nilpotent, or by Engel’s theorem\ref{2.5.1.29} all $x \in [\mathfrak{g}, \mathfrak{g}]$ defines a nilpotent endomorphism on $V$. Choose a basis that $x$ is upper-triangular by\ref{2.3.6.3}, and let $x_s$ be the semisimple part of $x$, then it suffices to show $x_s = 0$, or equivalently $\text{tr}(\bar{x}_s x) = 0$. To show this, notice $x \in [\mathfrak{g}, \mathfrak{g}]$, so it suffices to show $\text{tr}(\bar{x}_s[y, z]) = 0$ for any $y, z$. But this equals $\text{tr}([\bar{x}_s, y], z)$. Finally, this is 0 because of the hypothesis and the fact $\bar{x}_s$ is a polynomial in $x$\ref{2.3.6.7} so $[\bar{x}_s, y] \in \mathfrak{g}$.

\begin{corollary}[Cartan’s Criteria for Solvability] A Lie algebra $\mathfrak{g}$ over a field of characteristic 0 is solvable if $\kappa_\mathfrak{g}(x, y)$ for any $x \in \mathfrak{g}, y \in [\mathfrak{g}, \mathfrak{g}]$, where $\kappa$ is the Killing form.

Proof: By\ref{2.5.1.19}, it suffices to show for $k$ alg.closed. Because the kernel of the adjoint map is the center of $\mathfrak{g}$, so $\mathfrak{g}$ is solvable iff $\text{ad}(\mathfrak{g})$ is solvable.

\end{corollary}

\begin{proposition}[Engel] If $(\mathfrak{V}, \rho)$ is a representation of a Lie algebra $\mathfrak{g}$ that $\rho(x)$ is nilpotent for all $x \in \mathfrak{g}$, then there is a basis of $\rho(\mathfrak{g})$ contained in $\mathfrak{n}_V$, in particular $\mathfrak{g}$ is nilpotent.

Proof: It suffices to show if a sub-Lie algebra of $\mathfrak{gl}_V$ consists of nilpotent elements, then there is a common 0-eigenvector. Use Induction, choose a maximal subalgebra $K$ of $L$, then notice the normalizer of $K$ in $L$ is strictly containing $K$, because we can let $K$ acts by adjoint on $L/K$, and notice $\text{ad} x = \lambda_x - \rho_x$ is nilpotent for $x$ a nilpotent matrix, so by induction hypothesis there is an $x \in L$ that $[x, K] \subset K$. But $K$ is maximal, so it must be of codimension 1, and $L = K + Fz$. The 0-eigenvectors for $K$ is a nonzero subspace by induction hypothesis. Now this space is invariant under $z$: for any $h \in K$,

$$h(z(v)) = [h, z](v) + zh(v) = 0.$$ 

So now a 0-eigenvector for $z$ in this space will suffice.

\end{proposition}

\begin{corollary}[2.5.1.30] If all elements of $L$ are ad-nilpotent (i.e. $\text{ad} x = 0$), then $L$ is nilpotent. Equivalently, elements of $L$ has a common 0-eigenvector.

Proof: Consider $\text{ad} : \mathfrak{g} \rightarrow \mathfrak{gl}_\mathfrak{g}$, then the image is nilpotent by Engel’s theorem\ref{2.5.1.29}, and the kernel of ad is the center of $\mathfrak{g}$, so $\mathfrak{g}$ is also nilpotent.

\end{corollary}

\begin{corollary}[2.5.1.31] Let $\mathfrak{a}$ be an ideal of a Lie algebra $\mathfrak{g}$. Then $\mathfrak{a}$ is nilpotent if $\text{ad}\mathfrak{a}(a)$ is nilpotent for any $a \in \mathfrak{a}$.

Proof: If $\text{ad}\mathfrak{a}(a)$ is nilpotent for any $a \in \mathfrak{a}$, then also $\text{ad}\mathfrak{a}(a)$ is nilpotent, so $\mathfrak{a}$ is nilpotent by Engel’s theorem. Conversely, if $\mathfrak{a}$ is nilpotent, then $\text{ad}\mathfrak{a}(a)$ is nilpotent for any $a \in \mathfrak{a}$. And $\text{ad}(\mathfrak{a})(\mathfrak{g}) \subset \mathfrak{a}$, so $\text{ad}\mathfrak{a}(a)$ is nilpotent.

\end{corollary}

\begin{corollary}[2.5.1.32] The sum of two nilpotent ideals of $\mathfrak{g}$ is nilpotent.

Proof: We need to show for any $a \in \mathfrak{a}, b \in \mathfrak{b}$, $\text{ad}\mathfrak{a}(a + b)$ is nilpotent. For this, we need to factor $\mathfrak{g}$ as Jordan sequence $0 \subset \mathfrak{g}_1 \subset \mathfrak{g}_2 \subset \ldots \subset \mathfrak{g}_n = \mathfrak{g}$ over itself via the adjoint representation, then I claim that $\text{ad}(a)(\mathfrak{g}_k) \subset \mathfrak{g}_{k-1}$. Because $V = \mathfrak{g}_k/\mathfrak{g}_{k-1}$ is simple, let $V' \subset V$ consists of vectors $v$ that $a(v) = 0$ for any $a \in \mathfrak{a}$, then it is non-empty by Engel’s theorem, and also it is invariant under action of $\mathfrak{g}$: $a(gv) = [a, g](v) + g(av) = 0$. So it is all of $V$.

Then, we have $\text{ad}(a + b)(\mathfrak{g}_k) \subset \mathfrak{g}_{k-1}$, thus $\text{ad}(a + b)$ is nilpotent.
**Cor. (2.5.1.33)** [Maximal Nilpotent Ideal]. For any Lie algebra \( \mathfrak{g} \), there exists a maximal nilpotent ideal, denoted by \( \mathfrak{n} \).

**Def. (2.5.1.34)** [Nilpotent Radical]. The nilpotent radical \( \mathfrak{s} = s(\mathfrak{g}) \) of a Lie algebra is the intersection of the kernels of simple representations of \( \mathfrak{g} \).

\( \mathfrak{s} \) is nilpotent for any f.d. representation of \( \mathfrak{g} \), in particular the adjoint representation of \( \mathfrak{g} \). Thus it is nilpotent, by (2.5.1.31).

**Lemma (2.5.1.35).** Let \( \mathfrak{g} \subset \mathfrak{gl}_V \) be a subalgebra, and let \( \mathfrak{a} \) a commutative ideal of \( \mathfrak{g} \). If \( V \) is simple as a \( \mathfrak{g} \)-module, then \( [\mathfrak{g}, \mathfrak{a}] \cap \mathfrak{a} = 0 \).

**Proof:** Cf. [Mil13] P58.

**Prop. (2.5.1.36).** Let \( \mathfrak{g} \) be a Lie algebra, and \( \mathfrak{r} \) its radical, \( \mathfrak{s} \) it nilpotent radical, then

\[
\mathfrak{s} = D(\mathfrak{g}) \cap \mathfrak{r} = [\mathfrak{g}, \mathfrak{r}].
\]

In particular, \( [\mathfrak{g}, \mathfrak{r}] \) is nilpotent (2.5.1.34).

**Proof:** To show \( D(\mathfrak{g}) \cap \mathfrak{r} \subset \mathfrak{s} \), we need to show that \( \rho(D(\mathfrak{g}) \cap \mathfrak{r}) = 0 \) for any simple representation \( \rho \). Because \( \mathfrak{r} \) is solvable, let \( r \) be the smallest integer that \( \rho(D^r(\mathfrak{r})) = 0 \), then \( \mathfrak{a} = \rho(D^r(\mathfrak{r})) \) is a commutative ideal of \( \rho(\mathfrak{g}) \). Hence by (2.5.1.35) \( D(\rho(\mathfrak{g})) \cap \mathfrak{a} = 0 \), so \( \rho(D(\mathfrak{g}) \cap D^r(\mathfrak{r})) = 0 \). Now if \( r > 0 \), then \( \rho(D^r(\mathfrak{r})) = 0 \), contradicting the minimality of \( r \), so \( \rho(D(\mathfrak{g}) \cap r) = 0 \).

To show \( \mathfrak{s} \subset [\mathfrak{g}, \mathfrak{r}] \), let \( \mathfrak{q} = \mathfrak{g}/[\mathfrak{g}, \mathfrak{r}] \), and \( f \) the quotient map. Then because the kernel is solvable, \( f(r) \) is the radical of \( \mathfrak{q} \) (2.5.1.22), but it is also contained in the center of \( \mathfrak{q} \), so \( \mathfrak{q} \) is reductive, and thus has a faithful semisimple representation (2.5.4.4), then the kernel of this representation is just \([\mathfrak{g}, \mathfrak{r}]\), showing that \( \mathfrak{s} \subset [\mathfrak{g}, \mathfrak{r}] \).

**Def. (2.5.1.37)** [Levi Subalgebras]. Let \( \mathfrak{g} \) be a Lie algebra and \( \mathfrak{r} \) its radical, then a Lie subalgebra \( \mathfrak{s} \) is called a Levi subalgebra if \( \mathfrak{g} = \mathfrak{r} \oplus \mathfrak{s} \).

**Prop. (2.5.1.38)** [Levi-Malcev]. Every Lie algebra over a field \( k \) of char0 has a Levi subalgebra, and any two Levi subalgebras of \( \mathfrak{g} \) are conjugate by a special automorphism of \( \mathfrak{g} \) (2.5.1.7).

**Proof:** If \( \mathfrak{q} \) is reductive, then Levi subalgebra exists uniquely, by (2.5.4.2) and (2.5.4.3).

If \( \mathfrak{r} \) is a minimal ideal of \( \mathfrak{g} \), then \( [\mathfrak{g}, \mathfrak{r}] = \mathfrak{r} \), and \( [\mathfrak{r}, \mathfrak{r}] = 0 = Z(\mathfrak{g}) \). Consider the adjoint action of \( \mathfrak{g} \) on \( \text{End}_k(\mathfrak{g}) \). Also consider the subspaces \( V, W \) of \( \text{End}_k(\mathfrak{g}) \), where \( V \) is the subspace of maps from \( \mathfrak{g} \) to \( \mathfrak{r} \) that restriction to \( \mathfrak{r} \) is a constant multiple of identity, and \( W \) is the subspaces of \( V \) consisting of maps vanishing on \( \mathfrak{r} \). Both of \( V, W \) are invariant under action of \( \mathfrak{g} \).

Let \( \varphi : \mathfrak{r} \to \mathfrak{g} \) be the adjoint action, which is injective and has image \( P \subset W \). Also \( \Psi \) is invariant under action of \( \mathfrak{g} \) (because \( \mathfrak{r} \) is an ideal).

For \( x \in \mathfrak{r}, y \in \mathfrak{g}, \alpha \in V \), \( (zx)(y) = [x, \alpha(y)] - \alpha([x, y]) = -\lambda(\alpha)[x, y], \) so \( x\alpha = \text{ad}(\lambda(\alpha)x) \), which means elements of \( r \) map \( V \) into \( P \). Thus now \( \mathfrak{r} \) acts trivially on \( V/P \), and \( W/P \) is invariant under the action of \( \mathfrak{g}/\mathfrak{r} \), which is a semisimple Lie algebra. Thus by Weyl’s theorem (15.15.1.2), there exists a \( \mathfrak{g} \)-stable line \( L \) that \( V/P = W/P \oplus L \). But \( \mathfrak{g} \) acts trivially on \( L \) by (15.15.1.1).

Let \( \alpha_0 \) generates \( L \) and normalized that \( \lambda(\alpha) = 1 \), then \( \mathfrak{g}\alpha_0 \in P \), We consider the map \( \mathfrak{g} \xrightarrow{g \mapsto g\alpha_0} P \xrightarrow{\varphi^{-1}} \mathfrak{r} \), whose restriction to \( \mathfrak{r} \) is the identity map, so its kernel is a Levi subgroup for \( \mathfrak{r} \).

Still in this case, let \( \mathfrak{s}' \) be a second Levi subgroup for \( \mathfrak{r} \). For each \( x \in \mathfrak{s}' \), there is a unique \( h(x) \in \mathfrak{r} \) that \( x + h(x) \in \mathfrak{s} \). Hence this \( h \) satisfies \( h([x, y]) = [h(x), y] + [x, h(y)] \). But then
by (15.15.1.3), \( h(x) = [a, x] \) for some \( a \in \mathfrak{r} \). Then \( 1 + \text{ad}(a) \) maps \( \mathfrak{s} \) to \( \mathfrak{s}' \), and \( \text{ad}(a)^2 = 0 \) because \( \mathfrak{r} \) is commutative. And \( \mathfrak{r} = [\mathfrak{r}, \mathfrak{g}] \), so \( a \) is in the nilpotent radical of \( \mathfrak{g} \), thus \( \mathfrak{s}, \mathfrak{s}' \) are conjugate by a special automorphism.

For the general case, we can use induction on the dimension of \( \mathfrak{g} \). After the first two cases, we can assume that \( [\mathfrak{g}, \mathfrak{r}] \neq 0 \) and \( \mathfrak{r} \) contains a proper non-trivial ideal. As \( [\mathfrak{g}, \mathfrak{r}] \) is nilpotent (2.5.1.36), its center is non-zero. So we can choose a maximal ideal \( \mathfrak{m} \) contained in the center of \( [\mathfrak{g}, \mathfrak{r}] \), and \( \mathfrak{m} \neq \mathfrak{r} \). Now \( \mathfrak{g}/\mathfrak{m} \) has radical \( \mathfrak{r}/\mathfrak{m} \) because \( \mathfrak{m} \) is solvable, so we can apply induction to find a Levi subgroup \( \mathfrak{h}' \) for \( \mathfrak{g}/\mathfrak{m} \) in \( \mathfrak{g}/\mathfrak{m} \), and let \( \mathfrak{h}'' \) be its preimage in \( \mathfrak{g} \). Then \( \mathfrak{h}'' \) has radical \( \mathfrak{m} \), and thus by induction there is a Levi subgroup \( \mathfrak{h} \) for \( \mathfrak{m} \) in \( \mathfrak{h}'' \), and this \( \mathfrak{h} \) is a Levi subgroup for \( \mathfrak{r} \) in \( \mathfrak{g} \). Similarly any two such Levi subgroups are conjugate by a special automorphism.

This has another cohomological proof in [Etingof, Section 48].

2 Semisimple Lie Algebra

Prop. (2.5.2.1) [Cartan-Killing Criteria for Semisimplicity]. A f.d. Lie algebra \( \mathfrak{g} \) is semisimple iff its Killing form (2.5.1.13) is non-degenerate.

\textbf{Proof:} If \( \mathfrak{g} \) is semisimple, then the adjoint representation is faithful, thus by (2.5.9.6) the Killing form is non-degenerate. Conversely, if the Killing form is non-degenerate and \( \mathfrak{a} \) is a commutative ideal of \( \mathfrak{g} \) and \( a \in \mathfrak{a}, g \in \mathfrak{g} \), then \( (\text{ad}a \circ \text{ad}g)^2 = 0 \), so \( \text{ad}a \circ \text{ad}g \) is nilpotent and has trace 0. So \( a \in \mathfrak{g}^\perp \), which is 0 because the Killing form is non-degenerate.

Cor. (2.5.2.2). Let \( \mathfrak{a} \) be a semisimple ideal of a Lie algebra \( \mathfrak{g} \), then the orthogonal space \( \mathfrak{a}' \) w.r.t the Killing form is an ideal and is a complement for \( \mathfrak{a} \) in \( \mathfrak{g} \), and \( \mathfrak{g} \cong \mathfrak{a} \times \mathfrak{a}' \).

\textbf{Proof:} \( \mathfrak{a}^\perp \) is an ideal because the Killing form is invariant. The Killing form of \( \mathfrak{a} \) is the restriction of the Killing form of \( \mathfrak{g} \) (2.5.1.13), so \( \mathfrak{a} \cap \mathfrak{a}' = 0 \) because \( \kappa_{\mathfrak{a}} \) is non-degenerate.

Cor. (2.5.2.3). A Lie algebra is semisimple iff it is isomorphic to a product of simple algebras \( \mathfrak{g} = \mathfrak{a}_1 \times \cdots \times \mathfrak{a}_r \), and these \( \mathfrak{a}_i \) are all its minimal ideals, (Not only up to isomorphism).

\textbf{Proof:} The Killing form of \( \mathfrak{a} \cap \mathfrak{a}' \perp = 0 \), thus it is solvable, by (2.5.1.28), and then 0, so we can continue the decomposition.

For any minimal nonzero ideal \( \mathfrak{a} \subset \mathfrak{g} \), then \([\mathfrak{g}, \mathfrak{a}] \) is an ideal contained in \( \mathfrak{a} \) which is nonzero because \( \mathfrak{g} \) has trivial center. Then

\[ \mathfrak{a} = [\mathfrak{g}, \mathfrak{a}] = \bigoplus_i [\mathfrak{a}, \mathfrak{a}_i] \]

so \( \mathfrak{a} \subset [\mathfrak{a}, \mathfrak{a}_i] \subset \mathfrak{a}_i \), and then \( \mathfrak{a} = \mathfrak{a}_i \) by simplicity.

Cor. (2.5.2.4). If \( \mathfrak{g} \) is semisimple, then \([\mathfrak{g}, \mathfrak{g}] = \mathfrak{g} \).

Cor. (2.5.2.5). Let \( \mathfrak{g} \) be a Lie algebra over a field \( k \) and \( k'/k \) is a field extension, then \( \mathfrak{g} \) is semisimple iff \( \mathfrak{g} \otimes_k k' \) is semisimple.

Prop. (2.5.2.6) [Examples of Semisimple Lie Algebras].

- The subalgebra \( \mathfrak{sl}(V) \) of all elements of \( \text{End}(V) \) of trace 0 is semisimple.

Prop. (2.5.2.7). If \( L \) is semisimple, then every derivative of \( L \) is inner.

\textbf{Proof:} This is a special case of (15.15.1.3) applied to the adjoint representation.
Prop. (2.5.2.8). If \( \mathfrak{g} \) is a semisimple algebra of \( \mathfrak{gl}_n(k) \) where \( k \) is a field of \( \text{char} 0 \), then it contains the semisimple and nilpotent parts of each of its elements under the Jordan decomposition (2.3.6.7).

Proof: We may assume \( k \) is alg. closed, because the Jordan decomposition is invariant of the field that contains \( \mathfrak{g} \), and an element is contained in a vector space can be checked after base change to a larger field. For any subspace \( W \subset V \), let \( \mathfrak{g}_W = \{ \alpha \in \mathfrak{gl}_V | \alpha(W) \subset W, \text{tr}(\alpha|W) = 0 \} \), then if \( \mathfrak{g}_W \subset W \), then \( \mathfrak{g} \subset \mathfrak{g}_W \), because every element of \( \mathfrak{g} \) is a sum of brackets by (2.5.2.4), thus have zero trace. Now consider

\[
\mathfrak{g}' = \bigcap_{\mathfrak{g}_W \subset W} \mathfrak{g}_W.
\]

If \( x \in \mathfrak{g}' \), then so does \( x_s \) and \( x_n \), because they are polynomials in \( x \) without constant terms, and \( \text{ad}(x)_s = \text{ad}(x_n) \).

So it suffices to show that \( \mathfrak{g} = \mathfrak{g}' \). We claim that \( \mathfrak{g}' = \mathfrak{g} \): As \( \mathfrak{g} \) is a semisimple ideal of \( \mathfrak{g}' \), by (2.5.2.2), we have a decomposition

\[
\mathfrak{g}' = \mathfrak{g} \oplus \mathfrak{g}^\perp.
\]

Let \( \alpha \in \mathfrak{g}^\perp \) and \( W \) a simple \( \mathfrak{g} \)-module of \( V \), then \( \alpha \) acts on \( W \) as a scalar, which must be 0 because \( \alpha \in \mathfrak{g}_W \) and \( k \) has char 0. As \( W \) is a sum of simple \( \mathfrak{g} \)-modules by Weyl’s theorem (15.15.1.2), we get the desired conclusion.

Prop. (2.5.2.9) [Abstract Jordan Decomposition]. A semisimple/nilpotent element \( x \) in a Lie algebra \( \mathfrak{g} \) is an element that \( \rho(x) \) is semisimple/nilpotent for any representation \( (V, \rho) \) of \( \mathfrak{g} \). And \( x = x_s + x_n \) is called a Jordan decomposition iff \( \rho(x) = \rho(x_s) + \rho(x_n) \) is a Jordan decomposition (2.3.6.7) for any representation \( \rho \) of \( \mathfrak{g} \).

Every element of a semisimple Lie algebra \( \mathfrak{g} \) over a field of characteristic 0 has a unique Jordan decomposition, and \( x = x_s + x_n \) is a Jordan decomposition if \( \rho(x) = \rho(x_s) + \rho(x_n) \) is a Jordan decomposition for one faithful representation \( \rho \) of \( \mathfrak{g} \). In particular, this holds for the adjoint representation \( \text{ad} \).

Proof: Let \( x \in \mathfrak{g} \) and \( (V, \rho) \) a faithful representation of \( \mathfrak{g} \) (for example the adjoint representation), then there is at most one \( x = x_s + x_n \) that \( \rho(x) = \rho(x_s) + \rho(x_n) \) is the Jordan decomposition, which proves the uniqueness.

Now for any \( x \in \mathfrak{g} \), as (2.5.2.8) shows, there do exist two elements that \( \rho(x) = \rho(x_s) + \rho(x_n) \). But then it can be checked directly \( \text{ad}(x) = \text{ad}(x_s) + \text{ad}(x_n) \) is the Jordan decomposition of \( \text{ad}(x) \) as an endomorphism of \( \mathfrak{g} \), by (2.5.1.16). As the adjoint representation is faithful, this shows the Jordan decomposition is independent of the faithful representation chosen.

Now every representation is a subrepresentation of a faithful representation, so we can prove the existence.

Simple Lie Algebras

Main references are [Car05]Chap8 and [Kna96], more data about simple Lie algebras can be found in [Kna96]P508.

Def. (2.5.2.10) [Lie Algebras of Type \( A_n \): \( \mathfrak{sl}(n + 1, \mathbb{C}) \)].

Def. (2.5.2.11) [Lie Algebras of Type \( A_1 \)]. \( A_1 \) is also called \( \mathfrak{sl}_2(\mathbb{C}) \). It has a basis \( f, h, e \) with

\[
[he] = 2e, \quad [hf] = -2f, \quad [ef] = h.
\]
In matrix form,
\[
    h = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad e = \begin{bmatrix} 0 & 1 \\ 0 & 0 \end{bmatrix}, \quad f = \begin{bmatrix} 0 & 0 \\ 1 & 0 \end{bmatrix}.
\]

It can also be realized by
\[
    H = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}, \quad R = \frac{1}{2} \begin{bmatrix} 1 & i \\ i & -1 \end{bmatrix}, \quad L = \frac{1}{2} \begin{bmatrix} 1 & -i \\ -i & -1 \end{bmatrix}.
\]

These two representation differ by a conjugation by the Cayley transformation \( C = -\frac{1+i}{2} \begin{bmatrix} i & 1 \\ i & -1 \end{bmatrix} \).

It is simple by \(?\). The subalgebra \( \mathfrak{b} \) generated by \( X \) and \( H \) is solvable, called the canonical Borel subalgebra of \( \mathfrak{sl}_2 \).

**Proof:**

\[\square\]

**Prop.(2.5.2.12)** [Lie Algebras of Type \( B_n \): \( \mathfrak{so}(2n+1, \mathbb{C}) \)].

**Prop.(2.5.2.13)** [Lie Algebras of Type \( C_n \): \( \mathfrak{sp}(n, \mathbb{C}) \)].

**Prop.(2.5.2.14)** [Lie Algebras of Type \( D_n \): \( \mathfrak{so}(2n, \mathbb{C}) \)].

**Prop.(2.5.2.15)** [Lie Algebras of Type \( G_2 \)].

**Prop.(2.5.2.16)** [Lie Algebras of Type \( F_4 \)].

**Prop.(2.5.2.17)** [Lie Algebras of Type \( E_8 \)].

**Prop.(2.5.2.18)** [Classification of F.D. Complex Simple Lie Algebras].

**Prop.(2.5.2.19)** [Group Automorphisms of Simple Lie Algebras], Cf.[Carter, P184].

**Prop.(2.5.2.20).** \( \mathfrak{sl}_2(k) \) is simple if \( k \) has characteristic \( \neq 2 \).

**Def.(2.5.2.21)** [Exponent]. Let \( \mathfrak{g} \) be a simple Lie algebra,
\[
    e = \sum e_i, \quad h = 2\rho^\vee = \sum_i (2\rho^\vee, \alpha_i) h_i, \quad f = \sum_i (2\rho^\vee, \omega_i) f_i,
\]

then by definition, \([h, e] = 2e, [e, f] = h\), and
\[
    [h, f] = \sum_i \sum_j (2\rho^\vee, \alpha_i)(\alpha_j)(2\rho^\vee, \omega_j) f_j
    = \sum_j [(\sum_i (2\rho^\vee, \alpha_i))(2\rho^\vee, \omega_j)] f_j
    = \sum_j (2\rho^\vee, \alpha_j)(2\rho^\vee, \omega_j)f_j
    = -2f.
\]

So \( \{h, e, f\} \) is a \( \mathfrak{sl}_2 \)-tuple, called the principal \( \mathfrak{sl}_2 \)-subalgebra of \( \mathfrak{g} \). The highest weights of subrepresentation of the adjoint action of this subalgebra on \( \mathfrak{g} \) is called the exponents of \( \mathfrak{g} \), counted with multiplicity.

Equivalently, as \( h|_{\mathfrak{g}^0} = \text{ht}(\alpha) \text{id} \), if \( r_m \) is the number of roots of \( \mathfrak{g} \) of height \( m \), the exponents of \( \mathfrak{g} \) is the numbers \( m \) that \( r_m > r_{m+1} \).
Cor. (2.5.2.22). While \( r_m = 0 \) for \( m \) large and \( r_1 = r(\mathfrak{g}) \), there are \( r \) exponents of \( \mathfrak{g} \). Since the roots of height 2 are all \( \alpha_i + \alpha_j \) where \( i, j \) are connected by an edge in the Dynkin diagram, thus \( r_2 = r - 1 \), thus \( 1 = m_1 \leq \ldots \leq m_r \), \( \sum_{i=1}^r = |R^+| \). And \( \mathfrak{g} \cong \oplus_{r=1}^r L_{2m_i+1} \) as a representation of the principal \( \mathfrak{sl}_2 \)-subalgebra.

Prop. (2.5.2.23) [Exponents of Simple Lie Algebras]. Let \( \mathfrak{g} \) be a Lie algebra, the exponents are.
- \( A_n \): 1, 2, \ldots, \( n \).
- \( B_n \): 1, 3, \ldots, 2\( n \) − 1.
- \( C_n \): 1, 3, \ldots, 2\( n \) − 1.
- \( D_n \): 1, 3, \ldots, 2\( n \) − 3 and \( n \).
- \( G_2 \): 1, 5.
- \( F_4 \): 1, 5, 7, 11.
- \( E_6 \): 1, 4, 5, 7, 8, 11.

3 Cartan Subalgebras

Lie algebras in this subsection are assumed to be of f.d..

Def. (2.5.3.1) [Cartan Subalgebras]. A Cartan subalgebra of a Lie algebra \( \mathfrak{g} \) is a nilpotent subalgebra \( \mathfrak{h} \) that equals to its own normalizer in \( \mathfrak{g} \).

Remark (2.5.3.2). As a proper subalgebra of a nilpotent algebra is never its own normalizer (2.5.1.20), a Cartan subalgebra is a maximal nilpotent subalgebra, but a maximal nilpotent subalgebra may not be a Cartan subalgebra.

If \( k'/k \) is a field extension, then \( \mathfrak{h} \) is a Cartan subalgebra of \( \mathfrak{g} \) iff \( \mathfrak{h}_{k'} \) is a Cartan subalgebra of \( \mathfrak{g}_{k'} \). This is because being nilpotent and the normalizer is also compatible with base change (2.5.1.4).

Prop. (2.5.3.3) [Diagonal Cartan Algebra]. Let \( \mathfrak{g} \subset \mathfrak{gl}_V \) be a subalgebra containing a diagonal matrix \( a = \text{diag}(a_1, \ldots, a_n) \) with distinct \( a_i \), and let \( \mathfrak{h} \) be the subspace of all diagonal matrices in \( \mathfrak{g} \), then \( \mathfrak{h} \) is a Cartan subalgebra of \( \mathfrak{g} \).

Proof: Firstly \( \mathfrak{h} \) is Abelian, and if \( b = \sum b_{ij} e_{ij} \in N_\mathfrak{g}(\mathfrak{h}) \), then \( [a, b] \in \mathfrak{h} \). But
\[
[a, b] = \sum_{ij} (a_{ii} - a_{jj}) b_{ij} e_{ij}
\]
is in \( \mathfrak{h} \) iff \( b \) is diagonal, or \( b \in \mathfrak{h} \), so \( \mathfrak{h} = N_\mathfrak{g}(\mathfrak{h}) \) and \( \mathfrak{h} \) is a Cartan subalgebra. \( \square \)

Def. (2.5.3.4) [Regular Elements]. Let \( \mathfrak{g} \) be a f.d. Lie algebra, for any \( x \in \mathfrak{g} \), let \( P_x(T) \) be the characteristic polynomial of \( \text{ad}(x) \):
\[
P_x(T) = \det(T - \text{ad}(x)) = T^m + a_{m-1}(x)T^{m-1} + \ldots + a_0(x).
\]
Then the rank of \( \mathfrak{g} \) is the minimal \( n \) that \( n(x) \neq 0 \) for some \( x \in \mathfrak{g} \). A regular element is an element \( x \in \mathfrak{g} \) that \( a_n(x) \neq 0 \).
Prop. (2.5.3.5) [Regular Elements and Cartan Subalgebras]. For any regular element \( x \in \mathfrak{g} \), the nilspace \( \mathfrak{g}_x^0 \) is a Cartan subalgebra of \( \mathfrak{g} \).

**Proof:** Let
\[
U_1 = \{ y \in \mathfrak{g}_x^0 | \text{ad}_\mathfrak{g} (y)|_{\mathfrak{g}_x^0} \text{ is not nilpotent} \},
\]
\[
U_2 = \{ y \in \mathfrak{g}_x^0 | \text{ad}_\mathfrak{g} (y)|_{(\mathfrak{g}/\mathfrak{g}_x^0)} \text{ is invertible} \}.
\]
They are both Zariski open subsets of \( \mathfrak{g}_x^0 \). According to Engel’s theorem (2.5.1.29), to show \( \mathfrak{g} \) is nilpotent, it suffices to show that \( U_1 \) is empty. \( U_2 \) is non-empty because it contains \( x \), so if \( U_1 \) is non-empty, \( U_1 \cap U_2 \) is non-empty and there is a \( y \in U_1 \cap U_2 \). For this \( y \), \( n(y) < \dim \mathfrak{g}_x^0 = n(x) \), contradicting the regularity of \( x \).

It remains to show that \( \mathfrak{g}_x^0 \) is its own normalizer. If \( z \) normalizes \( \mathfrak{g}_x^0 \), then \([z, x] \in \mathfrak{g}_x^0\), which means \((\text{ad}(x))^n[z, x] = 0\), so \( \text{ad}(x)^{n+1}(z) = 0 \), thus \( z \in \mathfrak{g}_x^0 \).

Cor. (2.5.3.6) [Cartan Subalgebras Exist]. Let \( \mathfrak{g} \) be a Lie algebra over an infinity field \( k \) contains some Cartan subalgebra, and when \( k \) is alg.closed, all Cartan subalgebras come from some regular element, by (2.5.3.13).

**Proof:** Regular elements exist because \( k \) is infinite.

Cor. (2.5.3.7). Every Lie algebra over an infinite field is a sum of Cartan subalgebras.

**Proof:** This is because the sum of Cartan subalgebras is a vector space thus Zariski closed but it contains all regular elements, which is a Zariski open subset.

Cor. (2.5.3.8). Let \( \mathfrak{a} \) be a subalgebra of a Lie algebra \( \mathfrak{g} \) that \( \text{ad}_\mathfrak{g} (a) \) is semisimple for any \( a \in \mathfrak{a} \), then \( \mathfrak{a} \) is contained in a Cartan subalgebra of \( \mathfrak{g} \).

**Proof:** Cf.[Mil13]P81.

Prop. (2.5.3.9). Let \( \mathfrak{h} \) be a Cartan subalgebra of \( \mathfrak{g} \) over an alg.closed field \( k \). Consider the generalized eigenvalue decomposition (2.5.3.12), if \( x \in \mathfrak{g}^a \), then \( \text{ad}(x)(\mathfrak{g}^b) \in \mathfrak{g}^{a+b}(2.5.1.12) \), and thus \( \text{ad}(x) \) is nilpotent. Let \( E(\mathfrak{h}) \) be the subgroup of the group of elementary automorphisms (2.5.1.7) of \( \mathfrak{g} \) generated by the set of all the automorphisms \( e^{\text{ad}(x)} \), where \( x \in \mathfrak{g}^a \) for some \( \alpha \in \mathfrak{h}^* \backslash 0 \).

Now let \( \mathfrak{h}, \mathfrak{h}' \) be two Cartan subalgebras of \( \mathfrak{g} \), then there exists \( u \in E(\mathfrak{h}), u' \in E(\mathfrak{h}') \) that \( u(\mathfrak{h}) = u'(\mathfrak{h}') \).

**Proof:** Number the elements of \( \mathfrak{h}^* \backslash 0 \) as \( \alpha_1, \ldots, \alpha_n \), and consider the map
\[
f : \mathfrak{g}^{\alpha_1} \times \cdots \times \mathfrak{g}^{\alpha_n} \times \mathfrak{h} \to \mathfrak{g} : (x_1, \ldots, x_n, h) \mapsto e^{\text{ad}(x_1)} \cdots e^{\text{ad}(x_n)} h.
\]
Given a \( h_0 \in \mathfrak{h} \), it can be shown that
\[
(df)_{(0 \ldots, 0, h_0)} : (x_1, \ldots, x_n, h) \mapsto h + \sum_i [x_i, h_0] .
\]
Thus if we choose a regular \( h_0 \in \mathfrak{h} \), then \((df)_{(0 \ldots, 0, h_0)}\) is surjective from \( \mathfrak{g} \) to \( \mathfrak{g} \). Thus \( E(\mathfrak{h})\mathfrak{h}_r \) contains a dense open subset of \( \mathfrak{g} \). Similarly, \( E(\mathfrak{h}')\mathfrak{h}'_r \) contains a dense open subset of \( \mathfrak{g} \). So their intersection is not empty, i.e. \( u(h) = u'(h') \) for some \( u, u', h, h' \). Now
\[
u(\mathfrak{h}) = u(\mathfrak{h}_r^0) = \mathfrak{h}_r^0 = u(\mathfrak{h}') = u'(\mathfrak{h}_r^0) = u'(\mathfrak{h}')
\]
\[\Box\]
Cor. (2.5.3.10). All Cartan subalgebras in a Lie algebra have the same dimension, which is the rank of $\mathfrak{g}$ (2.5.3.4).

Proof: Because we can take a base change to an alg. closed field, under which a Cartan subalgebra is also a Cartan subalgebra by (2.5.3.2), then they have the same rank. □

Cor. (2.5.3.11) [Cartan Subalgebras are Conjugate]. Any two Cartan subalgebras of a f.d. Lie algebra over an alg. closed field $k$ are conjugate by an elementary automorphism (2.5.1.7).

Cartan Subalgebra of Semisimple Lie Algebras

Lemma (2.5.3.12) [Decomposition w.r.t. a Cartan Subalgebra]. Let $\mathfrak{h}$ be a Cartan subalgebra of a semisimple Lie algebra $\mathfrak{g}$, and assume that

$$\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{\alpha \in \mathfrak{h}^* \setminus 0} \mathfrak{g}^\alpha.$$ 

where $R = R(\mathfrak{g}, \mathfrak{h})$ is called the root system associated to $(\mathfrak{g}, \mathfrak{h})$. This is true, for example, when $k$ is alg. closed, by (2.5.9.10). (See (2.5.3.21) for when this decomposition is possible).

Cor. (2.5.3.13). If $k$ is alg. closed, the set $\mathfrak{h}_r$ of regular elements $h$ in $\mathfrak{h}$ that $\mathfrak{g}_h^0 = \mathfrak{h}$ is open and dense in $\mathfrak{h}$ in the Zariski topology.

Proof: The condition is equivalent to $\prod_{\alpha \in \mathfrak{h}^* \setminus 0} \alpha(h) \neq 0$, which is an open condition. □

Lemma (2.5.3.14). In the decomposition above, if $\alpha + \beta \neq 0$, then $\mathfrak{g}^\alpha$ and $\mathfrak{g}^\beta$ is orthogonal w.r.t. the Killing form.

Proof: $\text{ad}(x)\text{ad}(y)\mathfrak{g}^\gamma \subset \mathfrak{g}^{\alpha + \beta + \gamma}$, so if $\alpha + \beta \neq 0$, then $\text{ad}(x)\text{ad}(y)$ is nilpotent, thus $\kappa(x, y) = 0$. □

Prop. (2.5.3.15) [Cartan Subalgebras of Semisimple Lie Algebras]. Let $\mathfrak{h}$ be a Cartan subalgebra of a semisimple Lie algebra $\mathfrak{g}$, then

- Every element of $\mathfrak{h}$ is semisimple. In particular, $\mathfrak{h}$ is commutative (2.5.1.15).
- The centralizer of $\mathfrak{h}$ in $\mathfrak{g}$ is $\mathfrak{h}$.
- The restriction of the Killing form to $\mathfrak{h}$ is non-degenerate.

Proof: By (2.5.3.2), it suffices to prove this after $k$ is replaced by its alg. closure, so the generalized eigenvalue decomposition (2.5.3.12) holds. We prove 3 first: by (2.5.3.14), $\mathfrak{h}$ is orthogonal to all $[\mathfrak{h}, x]$ for any $x$. But if $x \in \mathfrak{g}^{\alpha}$, we can see that $[\mathfrak{h}, x] = \mathfrak{g}^\alpha$, so $\mathfrak{h}$ is orthogonal to all $\bigoplus \mathfrak{g}^\alpha$, so $\kappa$ must be non-degenerate on $\mathfrak{h}$.

Because $\mathfrak{g}$ has trivial center, the adjoint representation realizes $\mathfrak{h}$ as a subalgebra of $\mathfrak{gl}_\mathfrak{g}$, and Lie’s theorem (2.5.1.24) shows there is a basis that $\mathfrak{h} \subset \mathfrak{h}_\mathfrak{g}$, hence $\text{ad}([\mathfrak{h}, \mathfrak{h}]) \subset \mathfrak{n}_\mathfrak{g}$, and so $\text{tr}(\mathfrak{h}, [\mathfrak{h}, \mathfrak{h}]) = 0$. As $\kappa$ is non-degenerate on $\mathfrak{h}$, $[\mathfrak{h}, \mathfrak{h}] = 0$, thus $\mathfrak{h}$ is commutative. Now $\mathfrak{h} \subset c_\mathfrak{g}(\mathfrak{h}) \subset N_\mathfrak{g}(\mathfrak{h})$, thus $\mathfrak{h} = c_\mathfrak{g}(\mathfrak{h})$.

If $x \in \mathfrak{h}$, and $x = x_s + x_n$ is the Jordan decomposition (2.5.2.9), then $\text{ad}(x_n)$ are polynomials of $\text{ad}(x)$ thus lies in $\mathfrak{h}$. Now $\text{ad}(x_n)$ commutes with all $\text{ad}(y)$ for $y \in \mathfrak{h}$, thus $\text{ad}(y)\text{ad}(x_n)$ is nilpotent, thus $\kappa(y, x_n) = 0$. Thus $x_n = 0$ as $\kappa$ is non-degenerate on $\mathfrak{h}$. □
Cor. (2.5.3.16) [Cartan Subalgebra Maximal Abelian]. The Cartan subalgebras of a semisimple Lie algebra are the maximal subalgebras consisting of semisimple elements (2.5.2.9), and they are maximal Abelian subalgebras.

WARNING: maximal Abelian subalgebra may not be Cartan subalgebras, as they may contain non-semisimple elements.

Proof: A subalgebra consisting of semisimple elements is contained in a Cartan subalgebra, by (2.5.3.8).

Conversely, if \( h \subset h' \) and \( h \) is a Cartan subalgebra and \( h' \) consists of semisimple elements, then by (2.5.1.15), \( h' \) is commutative, and thus \( h' \subset c_{g}(h) \), so \( h = h' \).

Cartan subalgebras are Abelian by (2.5.3.15), and the are maximal Abelian because they are self-centralizing.

□

Cor. (2.5.3.17). Every regular element is semisimple, because it is contained in a Cartan subalgebra by (2.5.3.5).

Split Semisimple Lie Algebras

Def. (2.5.3.18) [Split Semisimple Lie Algebras]. A split Cartan subalgebra of a semisimple Lie algebra \( g \) over a field \( k \) is a Cartan subalgebra that all the eigenvalues of the linear maps \( \text{ad}(h) \) lies in \( k \) for all \( h \in h \). A split semisimple Lie algebra is a pair \((g, h)\) where \( g \) is semisimple and \( h \) is a split Cartan subalgebra.

Remark (2.5.3.19). For example, the diagonal matrices in \( \mathfrak{sI}_n \) is a splitting Cartan subalgebra over any field.

\( \mathfrak{sI}_2(\mathbb{R}) \) has a non-split Cartan subalgebra \( \left\{ \begin{bmatrix} 0 & -a \\ a & 0 \end{bmatrix} \mid a \in \mathbb{R} \right\} \).

Prop. (2.5.3.20). Let \( \alpha \) be a root of the split semisimple Lie algebra \((g, h)\), then

- The subspaces \( g^\alpha \) and \( h_\alpha = [g^\alpha, g^{-\alpha}] \) are both 1-dimensional.
- There is a unique element \( h_\alpha \in h_\alpha \) such that \( \alpha(h_\alpha) = 2 \), and \( (h_\alpha, h_\alpha) \neq 0 \).
- For each nonzero \( x_\alpha \in g^\alpha \), there is a \( y_\alpha \in g^{-\alpha} \) such that
  \[
  [x_\alpha, y_\alpha] = h_\alpha, \quad [h_\alpha, x_\alpha] = 2x_\alpha, \quad [h_\alpha, y_\alpha] = -2y_\alpha.
  \]
  i.e. \( \mathfrak{s}_\alpha = \{x_\alpha, y_\alpha, h_\alpha\} \cong \mathfrak{sI}_2 \).
- \( k\alpha \) is a root iff \( k = 0, \pm 1 \).

Proof: Define \( h_\alpha = [g^\alpha, g^{-\alpha}] \subset h \). Because the Killing form is non-degenerate on \( h \), we can define for each \( \alpha \in R \) a unique element \( h^\alpha \in h \) that \( \alpha(h) = k(h, h^\alpha) \) for all \( h \in h \). Then \( h_\alpha \) is the subspace spanned by \( h^\alpha \): This is because for \( x \in g^\alpha, y \in g^{-\alpha} \),

\[
\kappa(h, [x, y]) = \kappa([h, x], y) = \alpha(x)\kappa(x, y)
\]

so \([x, y] = \kappa(x, y)h^\alpha \). Combine this with the fact \( \kappa(g^\alpha, g^{-\alpha}) \neq 0 \), we get the fact \( h_\alpha = kh^\alpha \) is 1-dimensional.

Next, there is a unique element \( h_\alpha \in h_\alpha \) that \( \alpha(h_\alpha) = 2 \). For this, it suffices to show that \( \alpha \) doesn’t vanish on \( h_\alpha \): Otherwise let \( x \in g^\alpha \) and \( y \in g^{-\alpha} \) that \([x, y] = h \neq 0 \), then \([h, x] = 0 \).
\(\alpha(h)x = 0 = [h,y]\). So \(\{x,y,h\}\) spans a solvable subalgebra \(\mathfrak{a}\) of \(\mathfrak{g}\). As \(h \in [\alpha,\alpha]\). By Lie’s theorem, \(\rho(h)\) is nilpotent for any representation \(\rho\) of \(\alpha\). But \(h\) is in the Cartan subalgebra so \(\text{ad}(h)\) is semisimple \((2.5.3.15)\), so \(h = 0\), contradiction.

If \((h_\alpha,h_\alpha) = 0\), let \(h_\alpha = [x_\alpha,y_\alpha]\) for \(x_\alpha \in \mathfrak{g}^\alpha, y_\alpha \in \mathfrak{g}^{-\alpha}\), then \(\{x_\alpha,y_\alpha,h_\alpha\}\) is solvable, so by Lie’s theorem, there is a basis of \(\mathfrak{g}\) that the adjoint action is upper-triangular (when pass to the alg. closure). But then \(\text{ad}(h_\alpha)\) is nilpotent, but it is also semisimple, so \(h_\alpha = 0\), contradiction.

Because \(x_\alpha \neq 0\), there exists a unique \(y_\alpha \in \mathfrak{g}^{-\alpha}\) that \([x_\alpha,y_\alpha] = h_\alpha\). Now \([h_\alpha,x_\alpha] = \alpha(h_\alpha)x_\alpha = 2x_\alpha, [h_\alpha,y_\alpha] = -\alpha(h_\alpha)y_\alpha = -2y_\alpha\).

Finally, \(\mathfrak{h}_\alpha \oplus \oplus_{k \neq 0} \mathfrak{g}^{2k\alpha}\) is a subrepresentation of \(x_\alpha, y_\alpha, h_\alpha \cong \mathfrak{sl}_2\), so if \(\mathfrak{g}^{2\alpha} \neq 0\), then \(\text{ad}(x_\alpha)\) induces an isomorphism \(\mathfrak{g}^\alpha \cong \mathfrak{g}^{2\alpha}\) by the representation theory of \(\mathfrak{sl}_2(15.15.1.11)\). But \(\mathfrak{g}^\alpha\) is generated by \(x_\alpha\), contradiction. So \(\mathfrak{g}^{k\alpha} \neq 0\) only for \(k = 0, \pm1\).

**Prop. (2.5.3.21) [Root Decompositions]**. If \(\mathfrak{h}\) is a split Cartan subalgebra, then \(\text{ad}(\mathfrak{h})\) is a commuting family of semisimple endomorphisms with eigenvalues in \(k(2.5.3.15)\). so the decomposition

\[
\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{\alpha \in R} \mathfrak{g}^\alpha
\]

holds as in \((2.5.3.12)\). And it is in fact an eigenvalue decomposition, not only generalized eigenvalue decomposition, by \((2.5.3.20)\).

Then \(R\) is a reduced root system \((2.7.2.2)\) in \(\mathfrak{h}^\vee\), with \(s_\alpha(\beta) = -\beta(h_\alpha)\alpha\). In particular, \(\alpha^\vee = h_\alpha\).

**Proof**: Firstly \(R\) spans \(\mathfrak{h}^\vee\): if \(h \in \mathfrak{h}\) lies in the center of all \(\alpha \in R\), then \([h,\mathfrak{g}^\alpha] = 0\) for all \(\alpha \in R\), and as \([h,\mathfrak{h}] = 0\), this means \(h\) is in the center of \(\mathfrak{g}\), which is trivial, so \(h = 0\). So \(R\) spans \(\mathfrak{h}^\vee\).

We need to prove that if \(\alpha, \beta \in R\), then \(\beta(h_\alpha) \in \mathbb{Z}\) and \(\beta(h_\alpha) \in R\). For this, regard \(\mathfrak{g}\) as a \(\mathfrak{s}_\alpha\)-module \((2.5.3.20)\) under the adjoint action, then the assertion follows from the representation theory of \(\mathfrak{sl}_2(15.15.1.11)\): \(h_\alpha\) acts on \(\mathfrak{g}^\beta\) by \(\beta(h_\alpha)\), and \(y_\alpha^n\) induces an isomorphism \(\mathfrak{g}^\beta \cong \mathfrak{g}^{\beta - n\alpha}\).

Finally, \(R\) is reduced by \((2.5.3.20)\).

**Prop. (2.5.3.22) [Splitting Cartan Subalgebras are Conjugate]**. The group of elementary automorphisms of \(\mathfrak{g}(2.5.1.7)\) acts transitively on the set of pairs \((\mathfrak{b},\mathfrak{h})\) consisting of a Borel subalgebra \((2.5.4.7)\) and a splitting Cartan subalgebra of \(\mathfrak{g}\).


**Prop. (2.5.3.23) [Jacobson-Morozov]**. Let \(\mathfrak{g}\) be a semisimple Lie algebra and \(e \in \mathfrak{g}\) nilpotent, then there exists a homomorphism \(\mathfrak{sl}_2 \rightarrow \mathfrak{g}\) mapping \(X\) to \(e\).


**Recovering Split Semisimple Lie Algebras from Dynkin Diagrams**

Main references are [Car05]Chap7.

**Def. (2.5.3.24) [Cartan Matrix]**. Let \((\mathfrak{g},\mathfrak{h})\) be a split semisimple Lie algebra with root system \(R\), with notations in \((2.5.3.20)\), define the Cartan matrix of \(\mathfrak{g}\) to be the Cartan matrix \(A\) of \(R\), \(A = (a_{ij})\), where \(a_{ij} = \alpha_j(h_\alpha)\), where \(\{\alpha_1, \ldots, \alpha_n\}\) is a base \(S\) of \(R\).

**Prop. (2.5.3.25) [Serre Relations]**. Let \((\mathfrak{g},\mathfrak{h})\) be a split semisimple Lie algebra with root system \(R\) and a base \(S\), and Cartan matrix \(A = (a_{ij})\). Denote \(\mathfrak{n}_\pm = \oplus_{\alpha \in R^\pm} \mathfrak{g}^\alpha\), then \(\mathfrak{g} = \mathfrak{n}_- \oplus \mathfrak{h} \oplus \mathfrak{n}_+\). Take \(e_i \in \mathfrak{g}^{\alpha_i}, f_i \in \mathfrak{g}^{-\alpha_i}\) s.t. \([e_i,f_i,h_i = [e_i,f_i]] = \mathfrak{s}_i\) is a \(\mathfrak{sl}_2\)-triple \((2.5.3.20)\). Then
• \(e_i, f_i, h_i\) generate \(\mathfrak{g}\).

• (Serre Relations):

\[
[h_i, h_j] = 0, \quad [h_i, e_j] = a_{ij}, \quad [h_i, f_j] = -a_{ij}f_j, \quad [e_i, f_j] = \delta_{ij}h_i,
\]

\[
(\text{ad}(e_i))^{1-a_{ij}}e_j = 0, \quad (\text{ad}(f_i))^{1-a_{ij}}f_j = 0, \quad i \neq j
\]

**Proof:**

1: Because \(\mathfrak{h}_i\) generate \(\mathfrak{h}\), it suffices to show \(e_i\) generate \(\mathfrak{n}_+\), then dually \(f_i\) generate \(\mathfrak{n}_-\). We prove any \(\mathfrak{g}^\alpha\) is in the span by induction on the height of \(\alpha\). If \(\alpha = \sum n_i\alpha_i\), where \(n_i > 0\), then \(0 < \langle \alpha, \alpha \rangle = \sum n_i\langle \alpha, \alpha_i \rangle\), thus \((\alpha, \alpha_i) > 0\) for some \(i\), thus by (2.7.2.21) \(\alpha - \alpha_i\) is a root, and the representation theory of \(\mathfrak{s}_i\) shows \(e_i\) induces an isomorphism \(\mathfrak{g}^{\alpha - \alpha_i} \cong \mathfrak{g}^\alpha\). So we are done.

2: Only the last two assertions need a proof. The irreducible \(\mathfrak{s}_i\) representation generated by \(e_j\) satisfies \([f_i, e_j] = 0, [h_i, e_j] = a_{ij}\), thus this submodule is isomorphic to \(W_{a_{ij}}\), and \((\text{ad}(e_i))^{1-a_{ij}}e_j = 0\). The \(f_i\) case is similar. \(\square\)

**Prop. (2.5.3.26) [Criterion of Semisimplicity].** Let \(\mathfrak{g}\) be a Lie algebra and \(\mathfrak{h}\) a commutative Lie subalgebra. If

- there is a decomposition

\[
\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{\alpha \in R} \mathfrak{g}^\alpha,
\]

where \(R \subseteq \mathfrak{h}^\vee\) is the finite set of \(\alpha \in \mathfrak{h}^\vee \setminus \{0\}\) that \(\mathfrak{g}^\alpha \neq 0\), and \(\dim \mathfrak{g}^\alpha = 1\) for all \(\alpha \in R\).

- \(R\) generates \(\mathfrak{h}^\vee\).

- If \(\alpha \in R\), then \(-\alpha \in R\), and \([\mathfrak{g}^\alpha, \mathfrak{g}^{-\alpha}], \mathfrak{g}^\alpha) \neq 0\).

Then \(\mathfrak{g}\) is semisimple and \(\mathfrak{h}\) is a split Cartan subalgebra of \(\mathfrak{g}\) with root system \(R\).

**Proof:** If \(I\) is a commutative ideal of \(\mathfrak{g}\), by action of \(\mathfrak{h}\), we can assume that \(\mathfrak{g}^\alpha \subseteq I\) for some \(\alpha\). If \(\alpha \neq 0\), then \(\mathfrak{g}^\alpha\) and \([\mathfrak{g}^{-\alpha}, \mathfrak{g}^\alpha] \subseteq I\), so \([\mathfrak{g}^\alpha, \mathfrak{g}^{-\alpha}, \mathfrak{g}^\alpha] = 0\), contradiction. If \(I \subseteq \mathfrak{h}\), then by the hypothesis some \(\alpha(I) \neq 0\), so \(\mathfrak{g}^\alpha = [I, \mathfrak{g}^\alpha] \subseteq \mathfrak{g}^\alpha\), contradiction. So \(I = 0\).

\(\mathfrak{h}\) consists of semisimple elements and it is its own centralizer, so it is a Cartan subalgebra by (2.5.3.16). It is clearly split. \(\square\)

**Cor. (2.5.3.27) [Criterion of Simplicity].** Let \((\mathfrak{g}, \mathfrak{h})\) be a split semisimple Lie algebra. A decomposition \(\mathfrak{g} = \mathfrak{g}_1 \oplus \mathfrak{g}_2\) of Lie algebras defines a decomposition \((\mathfrak{g}, \mathfrak{h}) = (\mathfrak{g}_1, \mathfrak{h}_1) \oplus (\mathfrak{g}_2, \mathfrak{h}_2)\), and hence a decomposition of the root system \(R(\mathfrak{g}, \mathfrak{h})\).

In particular, if the root system \(R(\mathfrak{g}, \mathfrak{h})\) is indecomposable, then \(\mathfrak{g}\) is simple.

**Proof:** Let

\[
\mathfrak{g} = \mathfrak{h} \oplus \bigoplus_{\alpha \in R} \mathfrak{g}^\alpha, \quad \mathfrak{g}_1 = \mathfrak{h}_1 \oplus \bigoplus_{\alpha \in R_1} \mathfrak{g}_1^\alpha, \quad \mathfrak{g}_2 = \mathfrak{h}_2 \oplus \bigoplus_{\alpha \in R_2} \mathfrak{g}_2^\alpha
\]

be the eigenvalue decomposition of \(\mathfrak{g}, \mathfrak{g}_1, \mathfrak{g}_2\) w.r.t. the adjoint action of \(\mathfrak{h}\), then \(\mathfrak{h} = \mathfrak{h}_1 \oplus \mathfrak{h}_2\), and \(R = R_1 \sqcup R_2\). \(\square\)

**Prop. (2.5.3.28) [Serre Presentations].** Let \(\mathfrak{g}(R)\) be the Lie algebra generated by \(e_i, f_i, h_i\) with defining relations as in (2.5.3.25), then

- The Lie subalgebra \(\mathfrak{n}_+\) generated by \(e_i\) has \((\text{ad}(e_i))^{1-a_{ij}}(e_j) = 0\) as defining relations. The Lie subalgebra \(\mathfrak{n}_-\) generated by \(f_i\) has \((\text{ad}(f_i))^{1-a_{ij}}(f_j) = 0\) as defining relations. And \(h_i\) are linearly independent.
We prove by induction on the height of the $s = \alpha \in Q$ statement is clear as $\alpha$ is of f.d.

Thus we have a decomposition
\[
\tilde{g}(R) = \tilde{n}_+ \oplus \tilde{h} \oplus \tilde{n}_-
\]
by degree, and clearly $\tilde{n}_+$ is generated by $e_i$, $\tilde{h}$ is generated by $h_i$ and $\tilde{n}_-$ is generated by $f_i$.

Now I claim that $\tilde{n}_+$ is a free Lie algebra on generators $e_i$, $\tilde{n}_-$ is a free Lie algebra on generators $f_i$ and $h_i$ are linearly independent. It suffices to prove for $e_i$, and $f_i$ is true with the dual polarization. For this, let $b'$ be a vector space with basis $h'_i$, and consider the Lie algebra $\alpha = FL_r \times b'$, where $FL_r$ is the free Lie algebra generated by $f'_i$, and $b'$ acts on $FL_r$ by $[h'_i, f'_j] = -a_{ij} f'_j$, then $U = U(\alpha) = k(f'_1, \ldots, f'_n) \times k[h'_1, \ldots, h'_n]$, and there is an action of $\tilde{g}(R)$ on $U$ that is defined on the generators as follows: if $w = f'_{j_1} \ldots f'_{j_k}$ is a word in $f'_i$ of weight $\alpha$ and $P \in k[h'_1, \ldots, h'_n]$, then
\[
h_i(w \otimes P) = w \otimes (h'_i - \alpha(h_i))P
\]
\[
f_i(w \otimes P) = fw \otimes P
\]
\[
e_i(f'_{j_1} \ldots f'_{j_k} \otimes P) = \sum_{k|j_k = i} f'_{j_1} \ldots f'_{j_{k-1}} f'_{j_k} (h'_i - (\alpha_{j_{k+1}} + \ldots + \alpha_{j_n})(h'_i))P.
\]

It can be shown that this is truly a representation, and then it induces a map $\tilde{g}(R) \to U : x \mapsto x(1)$, and this maps Lie polynomials of $f$ in $\tilde{n}_+$ to Lie polynomials of $f'_i$, and $h$ to $h'_i$, so the assertions are true.

1: Now consider the elements $S^+_{ij} = (ad e_i)^1 - a_{ij} e_j \in \tilde{n}_+$ and $S^-_{ij} = (ad f_i)^1 - a_{ij} f_j \in \tilde{n}_-$. Then $[f_k, S^+_{ij}] = 0$: If $k \neq i, j$, then this is true, and if $k = j$, then $[f_j[e_i e_j]] = [e_i f_j e_j] = [h_j e_i] = a_{ji} e_i$, thus $[f_j (ad e_i)^r(e_j)] = 0$ for $r \geq 2$. If $a_{ij} \geq -1$, then this is true, and if $a_{ij} = 0$, then $a_{ji} = 0$ too, so the assertion is also true. If $k = i$, then we can prove by induction that $[f_i (ad e_i)^r(e_j)] = -r(a_{ij} + r - 1)(ad e_i)^{-1}(e_j)$. Thus $[f_i (ad e_i)^1 - a_{ij} (e_j)] = 0$, too.

So by induction we see that the ideals $I^+ \in \tilde{n}_+$ generated by such $S^+_{ij}$ is ideals $I^+ = I^+ \oplus I^-$, which implies the assertion.

2: The Serre relations shows that $e_j$ generates the representation $W_{-a_{ij}}$ of $s_i$ for $j \geq i$, and so does $f_j$. Also $e_i, f_i, h_i$ generate $W_2$, and $h_j$ generates $W_0$ or $W_0 \oplus W_2$, so $g(R)$ is a sum of f.d. modules over $s_1$, as the module generated by $\{a, b\}$ is a subquotient of $V \oplus W$ the modules generated by $\{a\}$ and $\{b\}$.

3: $g(R) = \oplus_{\alpha \in Q} g_{\alpha}$, where $g_{\alpha}$ is the subspace of $g(R)$ of weight $\alpha$. Then $g_{\alpha} \neq 0$ only if $\alpha \in Q_+$ or $Q_-$, and each $g_{\alpha}$ is of f.d.. Now we show that $g_R \neq 0$ only if $\alpha \in R \cup \{0\}$, which will suffice. We prove by induction on the height of $\alpha$: the height 1 case is trivial, and if $\alpha = ke_i$, then the statement is clear as $g^{ke_i} = 0$ for $k \geq 2$, because $n_\alpha$ is generated by $e_i$. If it is not of the form $\alpha = ke_i$, $\langle \alpha, \alpha \rangle > 0$ for some $i$, so by the representation theory of $s_1 \cong sl_2$, $g^{k_{\alpha}} \neq 0$, where $s_{\alpha} = \alpha - \alpha_i \alpha_i / 2 \not\in Q_-$, thus $s_{\alpha} \in Q_+$, and then by induction hypothesis $s_{\alpha} \in R$, so $\alpha \in R$. 

\[2.5. \text{LIE ALGEBRAS}\]
4: \( \widehat{g}(R)^\alpha \) is 1-dimensional for any \( \alpha \), so this is also true for \( g(R)^\alpha \). Then \( g(R) \) is semisimple with root system \( R \) by (2.5.3.26).

\[ \square \]

Cor. (2.5.3.29) [Classification of Split Simple Lie Algebras]. By 2, split simple Lie algebras over \( k \) are in bijection with Dynkin diagrams \( A_l, l \geq 1, B_l, l \geq 2, C_l, l \geq 3, D_l, l \geq 4 \) and \( E_6, E_7, E_8, F_4, G_2 \), by (2.7.3.5).

Notations for Split Semisimple Lie algebras

Def. (2.5.3.30) [Notations for a Split Semisimple Lie Algebra]. Let \( (g, h) \) be a split semisimple Lie algebra, then

- Its (positive/negative) root system is denoted by \((R^+/R^-)R\).
- Notation for root system is the same as in (2.7.4.1).
- \( g \) has a weight decomposition \( g = h \oplus_{\alpha \in R} g^\alpha \).
- \( x_\alpha \in g^\alpha, y_\alpha \in g^{-\alpha} \), where \( \alpha \in R^+ \).
- \( \mathfrak{s}_i = \{x_i, y_i, h_i\} \) is a \( \mathfrak{sl}_2 \)-triple, where \( x_i \in g^{\alpha_i}, y_i \in g^{-\alpha_i} \) (2.5.3.20).
- \( \alpha_i^\vee = h_i(2.5.3.21) \).

4 Reductive Lie Algebra

Def. (2.5.4.1) [Reductive Lie Algebra]. A Lie algebra is called reductive if \( \text{rad}(L) = Z(L) \), or equivalently \( Z(L) \subset \text{rad}(L) \).

Prop. (2.5.4.2). The following conditions on a Lie algebra \( g \) are equivalent:

- \( g \) is reductive.
- The adjoint representation of \( g \) is semisimple.
- \( g \) is a product of a commutative Lie algebra \( c \) and a semisimple Lie algebra \( b \).

Proof: 1 \( \rightarrow \) 2: The adjoint representation factors through the center of \( g \), which is also the radical of \( g \), so it is a representation of \( g/\text{rad}(g) \), which is semisimple (2.5.1.23), so Weyl’s theorem (15.15.1.2) shows the adjoint representation is semisimple.

2 \( \rightarrow \) 3: If the adjoint representation is semisimple, then \( g \) decomposes as a sum of minimal nonzero ideals \( a_i \) of \( g \), and then \( g \) is a product of these \( a_i \). Let \( c \) be the product of the one-dimensional ideals, then \( c \) is in the center thus commutative, and \( b \) the product of the remaining ideals, then \( b \) is semisimple because it has no solvable ideals.

3 \( \rightarrow \) 1 is trivial. \( \square \)

Cor. (2.5.4.3). The decomposition of \( g \) into a product of commutative Lie algebra and a semisimple Lie algebra is unique: in fact \( c \) is the center of \( g \), and \( b = [g, g] \), by (2.5.2.4).

Prop. (2.5.4.4). A Lie algebra \( g \) is reductive iff it has a faithful semisimple representation iff it has a trivial nilpotent radical (2.5.1.34).

Proof: If \( g \) has a faithful semisimple representation, then the nilpotent radical \( s = 0 \), thus by (2.5.1.36), \( r \) is in the center of \( g \), thus \( g \) is reductive.
Conversely, if \( g \) is reductive, then we need to show \( g \) has a faithful semisimple representation: For this, we can take the tensor product of the trivial representation of the commutative part and the adjoint representation of the semisimple part (2.5.2.3).

The last assertion is clear from (2.5.1.36).

\[ \text{Cor. (2.5.4.5) [Trace Form Criterion for Reductiveness]. If the trace form } B_{\rho}(2.5.9.5) \text{ is non-degenerate for some representation } (\rho, V) \text{ of } g, \text{ then } g \text{ is reductive.} \]

\[ \text{Proof: If } x \in \mathfrak{s}, \text{ then } \rho(x) = 0, \text{ thus } B_{\rho}(x, y) = 0 \text{ for any } y, \text{ thus } x = 0. \text{ So } \mathfrak{s} = 0, \text{ and } g \text{ is reductive.} \]

\[ \text{Cor. (2.5.4.6) [Classical Lie Algebras are Reductive]. All classical Lie groups over } \mathbb{R} \text{ or } \mathbb{C} \text{ are reductive.} \]

\[ \text{Proof: Apply (2.5.4.5) their standard representations.} \]

\[ \text{Def. (2.5.4.7) [Borel Subalgebras]. Let } g \text{ be a split reductive Lie algebra and } \mathfrak{h} \text{ a Cartan subalgebra with a system of positive roots } \Pi, \text{ and consider the corresponding triangular decomposition } g = n_- \oplus \mathfrak{h} \oplus n_+(2.5.3.21). \text{ Denote } b_+ = \mathfrak{h} \oplus n_+, \text{ and call any Lie subalgebra of } g \text{ conjugate to } b_+ \text{ a borel subalgebra of } g. \text{ The definition is independent of the choice of the Cartan subalgebra } \mathfrak{h}, \text{ by (2.5.3.22).} \]

5 Compact Lie Algebras

Main references are [李群讲义, 项武义] and [Kna96].

\[ \text{Def. (2.5.5.1) [Compact Lie Algebras]. A compact Lie algebra is Lie algebra that is the Lie algebra of a compact Lie group.} \]

\[ \text{Prop. (2.5.5.2) [Killing Form of Compact Lie Algebra]. The Killing form of a compact Lie algebra } g \text{ is negatively semi-definite, with the kernel the center of } g. \]

\[ \text{Proof: Choose an invariant inner product on } g \text{ w.r.t. the adjoint representation of } G \text{ by (10.9.4.1). Take derivative w.r.t the equation } (\text{Ad}(g)Y, \text{Ad}(g)Z) = (Y, Z), \text{ we get by (11.6.1.12),} \]

\[ (\text{ad}(X)Y, Z) + (Y, \text{ad}(X)Z) = 0. \]

so \( \text{ad}(X) \) is skew-symmetric w.r.t. this inner product, thus the eigenvalues are all purely imaginary. Then \( B(x, x) = \text{tr}(\text{ad}(x) \text{ ad}(x)) \leq 0. \)

\[ \text{Cor. (2.5.5.3) [Compact Lie Algebra is Reductive]. A compact Lie algebra } g \text{ is reductive.} \]

\[ \text{Proof: Because of the invariant inner form, any ideal } \mathfrak{a} \text{ of } g \text{ has a complement } \mathfrak{a}^\perp, \text{ thus the adjoint representation of } g \text{ is semisimple, thus } g \text{ is reductive (2.5.4.2).} \]

\[ \text{Cor. (2.5.5.4) [Compact Lie algebra Elements Semisimple]. For a compact Lie algebra } g, \text{ every element is semisimple, and the eigenvalues of any adjoint operator } \text{ad}(x) \text{ is purely imaginary.} \]

\[ \text{Proof: Because the Killing form is negative definite, thus its negation is an inner product on } g, \text{ and } \text{ad}(x) \text{ acts by skew-Hermitian matrices, thus has purely imaginary eigenvalues.} \]

\[ \text{Prop. (2.5.5.5). If } g \text{ is reductive and the Killing form is negative definite on } [g, g], \text{ then } g \text{ is compact.} \]
Proof: For the commutative part we can take the torus \((S^1)^n\), so it suffices to prove the semisimple case: for this, we consider \(\text{Int}(g)^0 \subset GL(g)\), it is contained in \(O(g)\) with the inner product defined by the negation of the Killing form, thus it is compact. And the Lie algebra of it is \(\text{Der}(g) = \text{ad}(g)(2.5.2.7)\).

\[\square\]

Prop.(2.5.5.6)[Representation of Compact Lie Algebras]. Let \(g\) be a compact Lie algebra that is the Lie algebra of a simply-connected compact Lie group, then \(\text{Rep}(g)\) is semisimple.

Proof: \[\square\]

6 Singular element

Introduction

Singular element in \(g\) is a linear space and is defined by some homogenous ideal in \(S(g)\).

The paper [Singular element] of Kostant tells in fact it is defined by some \(r\)-homogenous functions \(M_r\) in \(S(g)\), and further describes the properties of this ideal such as the \(G\)-module decomposition and as span of determinant minors.

Preliminary

Let complex simple Lie algebra \(g = \text{Lie} G, n = l + 2r\). The non-degenerate Killing form \(B \triangleq (x, y)\) on \(g\) generate a nonsingular pair on \(S(g)\) and \(\land(g)\) by

\[
(x_1 \cdots x_k, y_1 \cdots y_k) = \sum_{\sigma \in \Sigma_k} (x_1, y_{\sigma(1)}) \cdots (x_k, y_{\sigma(k)})
\]

\[
(x_1 \land \cdots \land x_k, y_1 \land \cdots \land y_k) = \sum_{\sigma \in \Sigma_k} sg(\sigma)(x_1, y_{\sigma(1)}) \cdots (x_k, y_{\sigma(k)})
\]

So \(g \leftrightarrow g', S(g) \leftrightarrow S(g') \leftrightarrow\) polynomial functions on \(g\); and \(S(g)\) and \(\land(g)\) are \(g\) thus \(G\) modules extending the adjoint representation.

Recall that \(\delta\) and \(\partial\) are called \(B\)-dual if \((\delta x, y) = (x, \partial y)\). Set antiderivation \(-d\ \mathcal{B}\)-dual to the operator

\[
\partial(x_1 \land \cdots \land x_p) = \sum_{i<j} (-1)^{i+j+1}[x_i, x_j] \land x_1 \land \cdots \hat{x}_i \land \cdots \hat{x}_j \land \cdots \land x_p
\]

on \(\land(g)\) and antiderivation \(\epsilon(u)\ \mathcal{B}\)-dual to the operator \(\epsilon(u)v = u \land v\) on \(\land(g)\).

Element \(v\) of \(S(g)\) are called invariant iff \(gv = v, \forall g \in G\) and element \(u\) of \(S(g)\) are called harmonic iff \((u, v) = 0, \forall v\) invariant and no constant term.

Denote by \(J, H\) respectively the graded subspace of invariant and harmonic elements, then:

Prop.(2.5.6.1)[Separation of Variables (in [Kos63])]. \(S(g) \cong J \otimes H\).

the Ideal of Sing \(g\)

In the projection \(\tau : T(g) \rightarrow U(g)\), PBW theorem asserts that \(S(g) \rightarrow U(g)\) is an isomorphism. Denote:

\[
\Gamma = \tau|_{S(g)} \circ \tau
\]

\(\Gamma\) is a \(G\)-map (as a consequence of the next prop).
Denote by $\Gamma_{2r,2}$ the subgroup of permutation that preserves the set of unordered pairs \{(1, 2), (3, 4), \ldots, (2r-1, 2r)\} and let $\Pi_r$ be a left coset representative of $\Gamma_{2r,2}$ in $\Gamma_{2r}$ that $sg(\Pi_r) = 1$

In [Amitsur-Levitski], Kostant proved:

**Prop. (2.5.6.2)** [in *Kos81*].

\[
\Gamma(\wedge^2(\mathfrak{g})) = R^k \in S^k(\mathfrak{g})
\]

\[
\Gamma(x_1 \wedge \cdots \wedge x_k) \mapsto \sum_{v \in \Pi_k} [x_v(1), x_v(2)] \cdots [x_v(2k-1), x_v(2k)]
\]

**Prop. (2.5.6.3)** [in *Kos81*].

\[
M = R^r \in H^r
\]

so it consists of harmonic functions.

Let $w \in \wedge^2 \mathfrak{g}$ of rank $k$ standardized as $v_1 \wedge v_2 + \cdots + v_{2k-1} \wedge v_{2k}$. Let

\[
\text{Rad}w = \{y \in \mathfrak{g}|\iota(y)w = 0\} = \{y \in \mathfrak{g}|(w, \epsilon(y)z) = 0, \forall z\}
\]

then $w$ of rank $2k \iff w^k \neq 0 \& w^{k+1} = 0 \iff \dim \text{Rad}w = n - 2k$.

**Lemma (2.5.6.4).**

\[
\iota(y)dx = [y, x]
\]

Thus

\[
\text{Rad}dx = \mathfrak{g}^x, \text{ Sing}\mathfrak{g} = \{x \in \mathfrak{g}|(dx)^r = 0\}.
\]

**Proof:** $(\iota(y)dx, z) = (dx, y \wedge z) = (x, -[y, z]) = ([y, x], z)$

So in order to find the module $M$, it's the best to find the dual of

\[
\gamma : S(\mathfrak{g}) \rightarrow \wedge^{\text{even}} \mathfrak{g} : x \rightarrow -dx
\]

Luckily:

**Prop. (2.5.6.5)** [in *Kos81*]. $\gamma$ is $B$ dual to $\Gamma$, in particular,

\[
(\Gamma(\zeta), x) = \left(\frac{-1}{r!}\right)(\zeta, (dx)^r) \ (\forall \zeta \in \wedge^2 \mathfrak{g} \text{ and } x \in \mathfrak{g})
\]

So: $f(x) = 0, \forall f \in M \iff x \in \text{Sing}\mathfrak{g}$.

**Cor. (2.5.6.6).** Let $\alpha$ be a CSA of $\mathfrak{g}, \Delta_+(\alpha)$ be the positive roots, then

\[
f|\alpha = C_f \cdot \prod_{\beta \in \Delta_+(\alpha)} \beta \quad (\forall f \in M)
\]

**Proof:** This is because that an element in a CSA is singular iff it commutes with an element outside this CSA, and taking root decomposition, this is equivalent to annihilated by a root, and by counting degree, the cor follows. □

By propositions of [[[Kos59]]] a regular nilpotent element $e$ is uniquely in a nilpotent radical $n$ of a Borel subalgebra and that $\mathfrak{g}^e \cap [n, n] = (\text{Sing}\mathfrak{g}) \cap \mathfrak{g}^e$. So there is a linear function $\xi$ on $\mathfrak{g}^e$ that $\ker \xi = (\text{Sing}\mathfrak{g}) \cap \mathfrak{g}^e$. Thus:
Cor. (2.5.6.7). \( f|g^e = C_f \cdot \xi^r \quad (\forall f \in M) \).

Proof: By counting degree, the same reason as before.
Now we think of a natural question: Can singular elements be defined by functions of even lower degree? The answer is NO.

Prop. (2.5.6.8). Assume \( 0 \neq f \) homogenous vanishes on \( \text{Sing}_g \), then deg \( f \geq r \)

Proof: By the last cor, if \( f \) has degre less than \( r \) then \( f \) vanish on any CSA, but semisimple regular element, thus CSAs are Zariski dense in \( g \) (this is because semisimple element are defined by a polynomial), so \( f = 0 \).

Thus we have established that \( \text{Sing}_g \) is an algebraic set defined by a set of harmonic \( r \)-homogenous functions on \( g \) and not by functions of degree lower than \( r \).

Next we offer a different formation of \( M \).

\[ M \text{ as minors of determinants} \]

For a \( B \) dual basis \( y_i, w_j \), define a derivation

\[ d_W(f \otimes u) = \sum^n_i \partial_{y_i} f \otimes \epsilon(w_i)u \quad \text{on} \quad S(g) \otimes \wedge g. \]

Here \( \partial_{x_i} \) is defined as \( \sum a_i \frac{\partial}{\partial x_i} \) for a standard basis \( x_i \) of \( g \). It’s easy to verify that \( d_W \) is well defined and is a \( G \)-map (Take a different basis \( Aw_i \) and \( Bz_i \), then \( AB^t = I \), substitute into the formula of \( d_W \), it doesn’t change).

**Chevalley Thm** tells us \( J \) is a polynomial ring \( \mathbb{C}[p_1, \ldots, p_l] \), where \( p_i \) are homogenous polynomials of fixed degree \( d_i \) and \( \sum^l_i (d_j - 1) = r \). So:

\[ d_W p_1(x) \wedge \ldots \wedge d_W p_l(x) = \sum_{1 \leq i_1 < \ldots < i_n \leq n} \phi(y_{i_1}, \ldots, y_{i_n}) w_{i_1} \wedge \ldots \wedge w_{i_n} \]

Where \( \phi(y_{i_1}, \ldots, y_{i_n}) = \det \partial_{y_i} p_j \) is homogenous of degree \( r \). (counting degree).

To see this, notice that \( f \otimes u \) acts as a function from \( g \) to \( \wedge g : f \otimes u(x) = f(x)u \). So:

\[ d_W p_j(x) = \sum^n_{i=1} \partial_{z_i} p_j(x) w_i. \]

Prop. (2.5.6.9). For any CSA \( \mathfrak{h} \) of \( g \) and a basis \( \{v_i\} \) of \( \mathfrak{h}, \forall x \in \mathfrak{h}, \)

\[ d_W p_1(x) \wedge \ldots \wedge d_W p_l(x) = \kappa \cdot \prod_{\phi \in \Delta^+} \phi(y)v_1 \wedge \ldots \wedge v_l \]

Lemma (2.5.6.10) [in [Kos63]], \( \{d_W p_1(x), \ldots, d_W p_l(x)\} \) is linearly independant iff \( x \in \text{Reg}_g \).

Proof: Notice that \( d_W p_j \) is a \( g \)-map, \( d_W p_j = d_W p_j([y, x]) \) so \( d_W p_j(x) \) commutes with \( g^x \); so
\( \in g^x \). Then the \( \text{lm} \) tells us when \( y \) is regular, \( d_W p_j(y) \) forms a basis of \( g^y \). Considering in \( g^y \), \( x \) is regular iff \( \prod_{\phi \in \Delta^+} \phi(x) \neq 0 \), the prop follows.

Next we give an explicit expression for \( \gamma \).

It can be verified (taking a \( z_i \) basis) that \( dx = \frac{1}{2} \sum^n_{i=1} w_i \wedge [z_i, x] \).
2.5. LIE ALGEBRAS

Now \( x \in \mathfrak{h} \),

\[
dx = \sum_{\phi \in \Delta^+} \phi(x) e_\phi \wedge f_{-\phi}
\]

(just take the basis \( w_i \) and \( z_i \) as a standard basis of \( \mathfrak{g} \) consisting of \( \{h_i, \ldots, h_l, e_\phi, f_\phi\} \))

So

\[
\gamma_r(x^r) = r!(\lambda - 1)^r \prod_{\phi \in \Delta^+} \phi(x) e_\phi \wedge f_{-\phi}
\]

Let \( \mu = i^r v_1 \wedge \cdots \wedge v_l \wedge \prod_{\phi \in \Delta^+} e_\phi \wedge f_{-\phi} \) then \( (\mu, \mu) = 1 \).

Denote \( v^* = \iota(v) \mu \) for \( v \in \wedge \mathfrak{g} \), then

\[
(v_1 \wedge \cdots \wedge v_l)^* = i^r \prod_{\phi \in \Delta^+} e_\phi \wedge f_{-\phi} = \kappa \gamma_r(x^r)
\]

(notice that \( \iota(u) \iota(v) = \iota(v \wedge u) \) and use \( \text{ln } 1 \))

Prop.(2.5.6.11). \( (dW p_1(x) \wedge \cdots \wedge dW p_l(x))^* = \kappa \gamma_r(x^r) \neq 0 \).

Proof: For \( y \in \mathfrak{h} \) regular, this follows from previous calculations, and notice both side are \( G \)-maps, and semisimple regular elements are Zariski open, conclusion follows. \( \square \)

Lemma(2.5.6.12). \( (s, t) = (s^*, t^*) \), so that \( -^* \) is a \( \mathcal{B} \)-isomorphism.

Prop.(2.5.6.13). Let \( \{w_1, \ldots, w_{2r}\} \) be linearly independent and \( \{u_1, \ldots, u_l\} \) be a basis of \( \{w_1, \ldots, w_{2r}\}^\perp \), then

\[
\Gamma(w_1 \wedge \cdots \wedge w_{2r}) = \kappa_1 \det \partial_{u_j} p_j \neq 0
\]

Thus, \( M \) is the span of all the minors \( \det \partial_{u_j} p_j \).

Proof: By the preceding props,

\[
\det \partial_{u_j} p_j = \phi(u_1, \ldots, u_l)(x) = (dW p_1(x) \wedge \cdots \wedge dW p_l(x), u_1 \wedge \cdots \wedge u_l) = ((dW p_1(x) \wedge \cdots \wedge dW p_l(x))^*, (u_1 \wedge \cdots \wedge u_l)^*) = \kappa \kappa_2(\phi_r(x^r), w_1 \wedge \cdots \wedge w_{2r}) = \kappa^{-1} \Gamma(w_1 \wedge \cdots \wedge w_{2r})(x).
\]

\( \square \)

\( G \)-module structure of \( M \)

Now we show the \( G \)-module structure of \( M \).

Let \( \theta \) be the derivative that \( \theta(x)(y) = [x, y] \) on \( \mathfrak{g} \). \( \text{Cas} = \sum_{i=1}^n \theta(z_i) \theta(w_i) \).

It’s in fact just the action of the Casimir element in center of \( U(\mathfrak{g}) \). Let \( m_l \) and \( M_l \) be the maximal eigenvalue and eigenspace of \( \text{Cas} \).

For a commutative Lie subalgebra \( c \) of rank \( l \), denote by \( [c] \) the line it defines on \( \wedge^l \mathfrak{g} \). The span of these \( [c] \) is denoted \( A_l \). Notice that \( \mathfrak{g}^y \subset A_l \) for a regular \( y \), and \( A_l \) is a \( G \)-submodule.
Prop. (2.5.6.14)[in [Kos65]].
\[ A_I = M_l; \quad m_I = l. \]

An ideal in a Borel subalgebra of \( \mathfrak{g} \) is necessarily spanned by root vectors and a prop of [[K-W09]] says any ideal of \( \dim I \) is (denoted by \( I \)) in fact abelian.

A prop in [[Kos65]] asserts that for two different ideals \( \Phi_1, \Phi_2 \), sum of their weight vectors \( \langle \Phi \rangle \) is distinct.

So \( G[\Phi_i] \) is an irreducible \( G \)-module \( V_\Phi \) with highest weight \( \langle \Phi \rangle \) and \( V_\Phi \) are inequivalent \( G \)-modules (because an irreducible representation have only one highest vector).

Prop. (2.5.6.15)[in [Kos65]].
\[ M_I = \bigoplus_{\Phi \in I} V_\Phi \bigoplus V_\Phi. \]

Now denote \( M_{2r} \) image of \( M_l \) under the isomorphism \( u \rightarrow u^* \), then

Prop. (2.5.6.16)[in [K-W09]]. \( M_I \) is the span of \( G \cdot [\mathfrak{g}^x] \) for \( x \) regular.

but by precious prop,
\[ [\mathfrak{g}^x] = \mathbb{C} W p_1(x) \wedge \ldots \wedge p_l(x). \]

thus \( M_{2r} \) is the span of \( G \cdot (\gamma_r(\frac{x^t}{1!})), x \) regular.

Prop. (2.5.6.17) [Final]. \( \Gamma|_{M_{2r}} : M_{2r} \rightarrow M \) is an isomorphism and \( M \cong M_{2r} \cong M_I = A_I \) as \( G \)-module.

So \( M \) is a multiplicity one module with \( |I| \) irreducible components.

Proof: Notice that \( \Gamma(\zeta)(x) = (\zeta, \gamma_r(\frac{x^t}{1!})) \) and \( M_{2r} \) is the span of \( G \cdot (\gamma_r(\frac{x^t}{1!})) \), the first part follows, and the rest is a recapitulation of previous props. \( \square \)

7 Real Lie Algebra

Prop. (2.5.7.1)[Passage from Real to Complex]. If \( g_\mathbb{R} \) is a Lie algebra over \( \mathbb{R} \) and \( \mathfrak{g} = g_\mathbb{R} \otimes \mathbb{C} \) its complexification, then \( g_\mathbb{R} \) is Abelian/nilpotent/solvable/semisimple iff \( \mathfrak{g} \) does.

Def. (2.5.7.2). A compact real form is a real subalgebra \( \mathfrak{l} \) of \( \mathfrak{g} \) s.t. \( \mathfrak{g} \) is the complexification of \( \mathfrak{l} \) and \( \mathfrak{l} \) is the lie algebra of a compact simply-connected Lie group.

Prop. (2.5.7.3). A real Lie algebra is compact iff there exists an invariant inner product iff the Killing form is negative definite.

Proof: One direction is easy, just use the average method to find a \( G \)-invariant inner product and then take derivative. For the other direction, the identity shows that a complement of an ideal is an ideal so \( \mathfrak{g} \) is decomposed into simple lie groups and reduce to the case that \( \mathfrak{g} \) is simple. The ideal is to show that \( \mathfrak{g} \cong \ad(\mathfrak{g}) \) is the whole outer derivative group \( \partial(\mathfrak{g}) \)(the following lm). So \( \mathfrak{g} \) equals to the identity component of \( \text{Aut}(\mathfrak{g}) \) which is a closed subgroup thus closed but it is also a subgroup of the compact group \( O(\mathfrak{g}) \) thus it is compact. \( \square \)

Lemma (2.5.7.4). If a real semisimple Lie algebra \( X \) has an invariant inner product, then every outer derivative is inner. (In fact, this is true by Cartan Criterion for semisimplicity (2.5.2.7)).
Proof: since \( \text{ad}(X) \) is skew-symmetric, it’s diagonalizable and its eigenvalue is pure imaginary, so the Killing form of \( X \) is negative definite. Now choose the complement \( \mathfrak{a} \) of \( \text{ad}(X) \) in \( \partial(X) \), then \( \mathfrak{a} \cap X = 0 \). Thus for \( D \in \mathfrak{a} \), \( \text{ad}(D(g)) = [D, \text{ad}(g)] = 0 \) for all \( g \) in \( X \), so \( D = 0 \), thus \( \text{ad}(X) = \partial(X) \). □

Prop. (2.5.7.5).

1. The complexification of the Lie algebra of a connected compact Lie group is reductive.

2. A complex Lie algebra is semisimple iff it is isomorphic to the complexification of the Lie algebra of a simply-connected compact Lie group. i.e. every complex semisimple Lie algebra has a compact real form.

Proof: 1: Because a connected compact Lie group is completely reducible so does the Lie algebra and so does the complexification. So it is reductive by (2.5.4.1). 2: Cf.[Varadarajan Lie Groups Lie algebras and Their Representations]. The idea is to find a real form whose corresponding simply-connected group is compact. □

Prop. (2.5.7.6). If \( \mathfrak{g} \) is the Lie algebra of a matrix Lie group \( G \), then:

1. every Cartan subalgebra comes from a maximal commutative subalgebra of a compact real form and any two Cartan subalgebras are conjugate under the Ad-action of \( G \).

2. any two compact real form is conjugate under the Ad-action of \( G \).

3. any two maximal commutative subalgebra of a compact real form is conjugate under the Ad-action of the corresponding compact compact subgroup.

Prop. (2.5.7.7). A real Lie algebra is semisimple iff its complexification is semisimple. Cf.[Varadarajan].

Cor. (2.5.7.8). The real Lie algebra of a compact simply-connected group is semisimple.

Note: For the classification of real semisimple Lie algebras, Cf.[李群讲义项武义 §6]

Prop. (2.5.7.9). If a complex representation of a Lie group admits an invariant bilinear form, then it is non-degenerate and unique. In fact, this is equivalent to a \( G \)-map from \( V \) to \( V^* \). Thus there is unique invariant inner product in a compact real form by the preceding proposition.

8 Universal Constructions

In this subsection \( k \) can be a field of any characteristics.

Def. (2.5.8.1) [Universal Enveloping Algebra]. The universal enveloping algebra of a Lie algebra \( \mathfrak{g} \) is defined to be

\[
U(\mathfrak{g}) = T(\mathfrak{g})/J, \quad T(\mathfrak{g}) = \bigoplus_{n=0}^{\infty} \mathfrak{g}^\otimes n
\]

which is a graded algebra \( T(\mathfrak{g}) \) quotienting the ideal \( J = \langle x \otimes y - y \otimes x - [xy] \rangle \).

There is a natural linear map \( \sigma : \mathfrak{g} \to U(\mathfrak{g}) \).

Prop. (2.5.8.2). The universal enveloping algebra \( U : \mathfrak{g} \mapsto U(\mathfrak{g}) \) defines a functor \( \text{LieAlg} \to \text{Alg}^{asso} \) that is left adjoint to the canonical functor \( \text{Alg}^{asso}_k \to \text{LieAlg}_k(2.5.1.2) \).
Proof: For any associative algebra $A$ and a morphism of Lie algebras $q \to [A]$, there is easily seen a morphism $U(q) \to A$, and it is unique. 

Cor. (2.5.8.3) [Representation as Modules]. A representation of $g(2.5.12.4)$ is the same as a representation of $U(q)$.

Prop. (2.5.8.4) [Poincaré-Birkhoff-Witt]. Let $q$ be a Lie algebra, define a filtration on $U(q)$ by assigning $F_n U(q) = \text{the image of } \bigoplus_{i=0}^{k} q^{\otimes i}$ in $U(q)$. We have $[F_1 U(q), F_2 U(q)] \subset F_{i+j-1} U(q)$, thus $g r U(q)$ has a graded commutative ring structure. Thus there is an algebra homomorphism $S(q) \to g r U(q)$, and this homomorphism is an isomorphism.

If $q$ has a basis $\{x_i\}, i \in I$, and is an order on $I$, then $U(q)$ has a basis consisting of elements $\{x_{i_1}^{r_1} \cdots x_{i_k}^{r_k}\}$ where $i_1 < i_2 < \ldots < i_r$.

Proof: We assign any monomial $a_{i_1} \ldots a_{i_n}$ in $g_s$ a pair $(k, N)$ where $k$ is the number of factors in a monomial and $N$ is the number of inversions (meaning the number of pairs $1 \leq r, s \leq n$ that $i_r > i_s$), pairs $(k, N)$ are lexicographical ordered. Let $T^{(k,N)}$ be the space of $T(q)$ generated by monomials of index $(k, N)$, $T^k = \bigcup_{N=1}^{\infty} T^{(k,N)}$, and $U^{(k,N)}$, $U^k$ the space of $T(q)$ the image of $T^{(k,N)}, T^k$ in $U(q)$. We will use induction on $(k, N)$. Notice for any $k$, $T^k = T^{(k,N)}$ for $N$ large.

To show that the monomials in $(*)$ generates $U(q)$, if we have a monomial $a_{i_1} a_{i_2} \ldots a_{i_n}, a_{i_{s+1}} \ldots a_{i_k}$ that $i_s > i_{s+1}$, then

$$a_{i_1} a_{i_2} \ldots a_{i_s} a_{i_{s+1}} \ldots a_{i_k} = a_{i_1} a_{i_2} \ldots (a_{i_{s+1}} a_{i_s}) + [a_{i_s}, a_{i_{s+1}}] \ldots a_{i_k},$$

which is in $\bigcup_{N=1}^{\infty} U^{(k',N')}$ for simplicity.

To show that the monomials are linearly independent, we first show that there is a linear map

$$\theta: T(q) \to R = C[z_i]_{i \in I}$$

satisfying the following conditions:

$$\theta(a_{i_1} \ldots a_{i_n}) = z_{i_1} \ldots z_{i_n}, \text{if } i_1 \leq i_2 \ldots \leq i_n, \quad (**)$$

$$\theta(a_1 \ldots a_k a_{i_{k+1}} \ldots a_{i_n}) = \theta(a_1 \ldots a_{i_{k+1}} a_{i_k} \ldots a_{i_n}) + \theta(a_1 \ldots [a_{i_k}, a_{i_{k+1}}] \ldots a_{i_n}). \quad (***)$$

We construct this map by construction on $\bigcup_{(k',N') \leq (k,N)} U^{(k',N')}$ and use induction on $(kN)$. For $k = 0$, let $\theta(1) = 1$. If $\theta$ is defined for any monomials of index $(k, N)$ that $k < n$, define $\theta$ on $T^{n,0}$ by $\theta(a_{i_1} \ldots a_{i_n}) = z_{i_1} \ldots z_{i_n}$, then it satisfies $(**)$.

And if $\theta$ is already defined for any $T^{n,k}$ that $k < i$, suppose that the monomial $a_{i_1} \ldots a_{i_n}$ has index $(n, i)$, then there is a smallest $k$ that $a_{i_1} \ldots a_{i_{k+1}} a_{i_k} \ldots a_{i_n}$ has index $i - 1$. Then we define

$$\theta(a_{i_1} \ldots a_{i_n}) = \theta(a_{i_1} \ldots a_{i_{k+1}} a_{i_k} \ldots a_{i_n}) + \theta(a_{i_1} \ldots [a_{i_k}, a_{i_{k+1}}] \ldots a_{i_n}).$$

Now we need to check that this definition satisfies $(***)$;

If there is another $k'$ that $i_{k'} > i_{k'+1}$, then $k < k'$. Suppose first that $k + 1 < k'$, let $a_{i_k} = a, a_{i_{k+1}} = b, a_{i_{k'}} = c, a_{i_{k'+1}} = d$, then

$$\theta(\ldots ab \ldots cd \ldots) = \theta(\ldots ba \ldots cd \ldots) + \theta(\ldots [a, b] \ldots cd \ldots)$$
\begin{align*}
\theta(\ldots ba \cdots dc \ldots) + \theta(\ldots ba \ldots [cd] \ldots) + \theta(\ldots [ab] \ldots dc \ldots) + \theta(\ldots [ab] \ldots [cd] \ldots) \\
= \theta(\ldots ab \ldots dc \ldots) + \theta(\ldots ab \ldots [cd] \ldots)
\end{align*}

where the terms except the first one are all in \(\cup_{\langle k'\rangle < \langle k\rangle} T^{(k',N')}\) so the equalities come from induction hypothesis. So it satisfies (** *).

Suppose next that \(k' = k + 1\), let \(a_{i_k} = a, a_{i_{k+1}} = b, a_{i_{k+2}} = c\), then

\begin{align*}
\theta(\ldots abc \ldots) &= \theta(\ldots bac \ldots) + \theta(\ldots [ab]c \ldots) \\
&= \theta(\ldots bca \ldots) + \theta(\ldots [bc]a \ldots) + \theta(\ldots [ac]b \ldots) + \theta(\ldots [ac]c \ldots) \\
&= \theta(\ldots cab \ldots) + \theta(\ldots [ac]b \ldots) + \theta(\ldots [ac]c \ldots) \\
&= \theta(\ldots acb \ldots) + \theta(\ldots [ac]b \ldots)
\end{align*}

where the terms except the first one are all in \(\cup_{\langle k'\rangle < \langle k\rangle} T^{(k',N')}\) so the equalities come from induction hypothesis, and in the third equality we used the Jacobi identity. So it satisfies (** *).

Now all elements in \(J\) is a linear combination of elements of the form

\[a_1 \ldots a_{i_k} a_{i_{k+1}} \ldots a_{i_n} - a_1 \ldots a_{i_k+1} a_{i_k} \ldots a_{i_n} - a_1 \ldots [a_{i_k} a_{i_{k+1}}] \ldots a_{i_n},\]

so the map \(\theta\) factors through \(T(\mathfrak{g}) \to U(\mathfrak{g})\) to a map \(\overline{\theta} : U(\mathfrak{g}) \to R\), and the elements \(a_{i_1} a_{i_2} \ldots a_{i_k}, i_1 \leq i_2 \leq \ldots \leq i_k\) are mapped to \(z_{i_1} \ldots z_{i_n}\), which are linearly independent in \(R\), so the elements \(a_{i_1} a_{i_2} \ldots a_{i_k}, i_1 \leq i_2 \leq \ldots \leq i_k\) are also linearly independent in \(U(\mathfrak{g})\). \(\square\)

**Cor. (2.5.8.5).** The map \(\mathfrak{g} \to U(\mathfrak{g})\) is injective.

**Cor. (2.5.8.6).** \(U(\mathfrak{g})\) has no zero-divisors.

**Proof:** We can use the identities \(x \otimes y - y \otimes x = [xy]\) to make any element in their right representations under the PBW prop(2.5.8.4), so it is clear that the product of two nonzero elements cannot be 0. \(\square\)

**Cor. (2.5.8.7).** If \(\mathfrak{h} \subset \mathfrak{g}\), then the subalgebra of \(U(\mathfrak{g})\) generated by \(\mathfrak{h}\) is isomorphic to \(U(\mathfrak{h})\).

**Proof:** There is a natural map \(U(\mathfrak{h}) \to U(\mathfrak{g})\), and the image is just the subgroup generated by \(\mathfrak{h}\). The PBW theorem shows this map is injective. \(\square\)

**Cor. (2.5.8.8).** If \(\mathfrak{g} = \mathfrak{a} \times \mathfrak{b}\), then \(U(\mathfrak{g}) = U(\mathfrak{a}) \otimes U(\mathfrak{b})\).

**Def. (2.5.8.9)[Coproduct of \(U(\mathfrak{g})\)].** Let \(\mathfrak{g}\) be a Lie algebra, there is a coproduct \(\Delta\) on \(T(\mathfrak{g})\) defined by \(\Delta(g) = g \otimes 1 + 1 \otimes g\). This coproduct descends to a coproduct \(\Delta : U(\mathfrak{g}) \to U(\mathfrak{g}) \otimes U(\mathfrak{g})\).

**Proof:** It suffices to check that \(\Delta(J) \subset J \otimes T(\mathfrak{g}) + T(\mathfrak{g}) \otimes J\), and this is because

\begin{align*}
\Delta(x \otimes y - y \otimes x - [xy]) &= (x \otimes 1 + 1 \otimes x)(y \otimes 1 + 1 \otimes y) - (y \otimes 1 + 1 \otimes y)(x \otimes 1 + 1 \otimes x) - ([xy] \otimes 1 + 1 \otimes [xy]) \\
&= (x \otimes y - y \otimes x - [xy]) \otimes 1 + 1 \otimes (x \otimes y - y \otimes x - [xy])
\end{align*}

\(\square\)

**Prop. (2.5.8.10)[\(\mathfrak{g}\)-Module Structure].** Let \(\mathfrak{g}\) be a Lie algebra, then \(T(\mathfrak{g})\) is a \(\mathfrak{g}\)-module, and this action descends to a \(\mathfrak{g}\)-module structure on \(U(\mathfrak{g})\).
Proof: It suffices to show that $\mathfrak{g}J \subset J$ and $\mathfrak{g}I \subset I$:

$$y(a \otimes b - b \otimes a - [ab]) = [ya] \otimes b + a \otimes [yb] - [yb] \otimes a - b \otimes [ya] - [y[ab]]$$

$$= [ya] \otimes b - b \otimes [ya] - [[ya]b] + a \otimes [yb] - [yb] \otimes a - [a[yb]]$$

\[\square\]

Prop. (2.5.8.11) [Transpose]. There is an anti-automorphism $u \mapsto u^t$ of $U(\mathfrak{g})$ that $X^t = -X$ for $X \in \mathfrak{g}$.

Proof: We first extend this $t$ to an automorphism of $T(\mathfrak{g})$, then we compose with the obvious anti-automorphism $T(\mathfrak{g}) \to T(\mathfrak{g})$. Then we check that this map descends to $U(\mathfrak{g})$: $(X \otimes Y - Y \otimes X - [X,Y])^t = Y \otimes X - X \otimes Y - [Y,X] \in J$, so $J^t \in J$.

\[\square\]

Prop. (2.5.8.12) [Graded Algebra of $U(\mathfrak{g})$]. Let $L$ be a Lie algebra, if we let $S(L) = T(L)/(x \otimes y - y \otimes x)$ be the universal symmetric algebra of $L$, then it is a graded algebra. There is a filtered structure on $U(L)$ given by $U_i = \{\text{subalgebra generated by } a_1a_2 \ldots a_j, j \leq i\}$, then the associated graded algebra of $U(L)$ is isomorphic to $S(L)$ by PBW theorem.

Cor. (2.5.8.13). If $W$ is a subspace of $T^n(L)$ that is sent isomorphically onto $S^n(L)$, then the image of $W$ is a complement of $U_n(L)$ complementary to $U_{n-1}(L)$.

Cor. (2.5.8.14) [Symmetrization Map]. Over a field of characteristic 0, the symmetrization map $\sigma : S(\mathfrak{g}) \to T(\mathfrak{g}) \to U(\mathfrak{g})$ (2.3.9.2) is an isomorphism of $\mathfrak{g}$-modules that

$$U^n(\mathfrak{g}) = \sigma(S^n(\mathfrak{g})) \oplus U^{n-1}(\mathfrak{g}).$$

Proof: It is clearly an isomorphism of vector spaces. It suffices to show the map is compatible with $\mathfrak{g}$-actions: Because

$$\sigma(y_1 \ldots y_n) = \frac{1}{n!} \sum_{\sigma \in \Sigma_n} y_{\sigma(1)} \ldots y_{\sigma(n)},$$

$$\sigma(g(y_1 \ldots y_n)) = \sigma([gy_1] \ldots y_n + \ldots + y_1 \ldots [gy_n])$$

$$= \frac{1}{n!} \sum_{\sigma \in \Sigma_n} ([gy_{\sigma(1)}] \ldots y_{\sigma(n)} + \ldots + y_{\sigma(1)} \ldots [gy_{\sigma(n)}])$$

$$= g(\frac{1}{n!} \sum_{\sigma \in \Sigma_n} y_{\sigma(1)} \ldots y_{\sigma(n)})$$

\[\square\]

Prop. (2.5.8.15). If $\mathfrak{g}$ is a Lie algebra over a field $k$ of characteristic 0, then the set of primitive elements (2.9.1.3) are just $\mathfrak{g}$.

Proof: If $f$ is primitive, then the leading term $f_0$ of $f$ is also primitive in $grU(\mathfrak{g}) \cong S(\mathfrak{g})$. Now consider $S(g) \xrightarrow{\Delta} S(\mathfrak{g}) \otimes S(\mathfrak{g}) \xrightarrow{\mu} S(\mathfrak{g})$, then if $f$ is of degree $n$, then $2^n f_0 = 2 f_0$, which means $n = 1$. So $f = c + f_0$, and $c = 0$.

\[\square\]

Prop. (2.5.8.16) [$U(\mathfrak{g})$ is Noetherian]. For a f.d. Lie algebra $\mathfrak{g}$, $U(\mathfrak{g})$ is left Noetherian.

Proof: This is because the graded stricture on $U(\mathfrak{g})$ satisfies $gr U(\mathfrak{g}) \cong S(\mathfrak{g}) \cong \mathbb{C}[X_1, \ldots, X_n]$ is Noetherian, so $U(\mathfrak{g})$ is Noetherian itself.
Free Lie Algebras

Def. (2.5.8.17) [Free Lie Algebra]. Let $X$ be a set, then we define the free Lie algebra $\text{FL}(X)$ to be the intersection of Lie subalgebras in $[F(X)]$ containing $\sigma(X)$, where $F(X)$ is the free algebra generated by $X$.

Then the free Lie algebra $\text{FL} : X \mapsto \text{FL}(X)$ defines a functor $\text{Set} \to \text{LieAlg}$ that is left adjoint to the forgetful functor.

Proof: We need to show that for any Lie algebra $L$ and a map fo sets $\theta : X \to L$, there is a unique $\varphi$ completing the upper left triangular diagram:

$$
\begin{array}{ccc}
X & \xrightarrow{i} & \text{FL}(X) \\
\downarrow{\theta} & & \downarrow{\varphi} \\
L & \xrightarrow{\varphi} & U(L)
\end{array}
$$

Notice $\varphi^{-1}(\sigma(L))$ is a Lie algebra containing $X$ thus containing $\text{FL}(X)$, so it induces a $\varphi$.

And for the uniqueness, if there are two $\varphi_1, \varphi_2$, then the element that they coincide is a Lie algebra containing $X$, thus containing $\text{FL}(X)$, so $\varphi_1 = \varphi_2$. 

\[\square\]

Cor. (2.5.8.18). $U(\text{FL}(X)) \cong FX$ for any set $X$.

Proof: Because $U \circ \text{FL}$ and $F$ are both left adjoint to the forgetful functor $\text{AssAlg} \to \text{Set}$. 

Center of $U(\mathfrak{g})$

Prop. (2.5.8.19) [g Action on U(g)]. $\mathfrak{g}$ acts on $T(\mathfrak{g})$ by adjoint (2.5.9.2), and notice

$$
\text{ad}(z)(x \otimes y - y \otimes x - [xy]) = [zx] \otimes y + x \otimes [zy] - [zy] \otimes x - y \otimes [zx] - [z[xy]] \in J,
$$

so the action of $\mathfrak{g}$ descends to an action on $U(\mathfrak{g})$.

In fact, this action is inner: $\text{ad}(g)(z) = gz - zg$ for $z \in U(\mathfrak{g})$. In particular,

$$
Z(U(\mathfrak{g})) = U(\mathfrak{g})^{\text{ad}(\mathfrak{g})}.
$$

Invariant Polynomials

Prop. (2.5.8.20) [Chevalley]. The center of the universal enveloping algebra is isomorphic to the polynomial ring over $\mathbb{C}$ of $l$ elements, where $L$ is a semisimple lie algebra of rank $l$. In particular, The center for $\mathfrak{sl}_2$ is the algebra generated by the Casimir element $1/2h^2 + ef + fe$.

Proof: Because there is a commutative diagram of isomorphisms of algebras:

$$
\begin{array}{ccc}
S(L)^G & \xrightarrow{\alpha} & P(L)^G \\
\downarrow{\eta} & & \downarrow{\phi} \\
S(H)^W & \xrightarrow{\beta} & P(H)^W
\end{array}
$$

Where $P$ is the polynomial ring $\cong S(L^*)$, the horizontal is Killing isomorphisms and vertical is the restriction maps. Cf.[Carter prop 13.32]?
The twisted Harish-Chandra map gives an isomorphism of algebras $Z(L) \rightarrow S(H)^W$ (It just maps $z \in Z(L)$ to its pure $H$ part and transform every indeterminants $h_i$ to $h_i - 1$). e.g. $z = h^2 + 2h + 1 + 4fe \in Z(\mathfrak{sl}_2)$ is mapped to $h^2$ in $S(H)$. And $P(H)^W$ is isomorphic to a polynomial ring in $l$ generators over $\mathbb{C}$.

**Def. (2.5.8.21) [Casimir Element].** If $L$ is semisimple Lie algebra, by (2.5.2.1) the Killing form is non-degenerate, thus we choose a basis $x_i$ of $L$ and a dual basis $y_i$, then $c = \sum x_i y_i$ is independent of $x_i$ chosen by (2.3.8.9), and is called the Casimir element of $U(L)$.

**Prop. (2.5.8.22).** The Casimir element lies in the center of $U(L)$.

**Proof: □**

**Prop. (2.5.8.23) [Quillen’s lm].** If $K$ is an alg.closed field of char 0 that $\mathfrak{g}$ is a f.d. Lie algebra over $K$. If $U = U(\mathfrak{g})$ is its universal enveloping algebra, then for any irreducible $U$-module $M$, $\text{End}_U(M) = K$.

**Miscellaneous**

**Prop. (2.5.8.24) [Grading on $U(\mathfrak{sl}_2(\mathbb{C}))$].** Let $H, R, L$ be a basis of $\mathfrak{sl}_2(\mathbb{C})$(2.5.2.11), if we define a grading as $\text{deg } R = 1, \text{deg } H = 0, \text{deg } L = -1$, then this is descends to a grading on $U(\mathfrak{g})$, and the degree 0 part is the ring $\mathcal{R} = \mathbb{C}[\Delta, H]$. Also, there is a decomposition:

$$U(\mathfrak{g}) = \bigoplus_{i \geq 0} L^i \mathcal{R} \oplus \bigoplus_{i > 0} R^i \mathcal{R}.$$  

9 Representations

**Def. (2.5.9.1) [Representations].** A representation of a Lie algebra $\mathfrak{g}$ over a vector space $V$ is a Lie homomorphism $\mathfrak{g} \rightarrow \mathfrak{gl}_V$.

**Def. (2.5.9.2) [Tensor Product of Representations].** Let $(V_1, \pi_1), (V_2, \pi_2)$ be two representations of a Lie algebra $\mathfrak{g}$, then $(V_1 \otimes V_2, \pi_1 \otimes \pi_2)$ is a representation of $\mathfrak{g}$ given by

$$(\pi_1 \otimes \pi_2)(g)(v_1 \otimes v_2) = \pi_1(g)v_1 \otimes v_2 + v_1 \otimes \pi_2(g)v_2.$$  

**Def. (2.5.9.3) [Representation on Tensor Algebras].** If $(V, \rho)$ is a representation of $\mathfrak{g}$, then $\mathfrak{g}$ acts on $T(V)$ via (2.5.9.2). Also, the ideals $I, J$ are invariant under action of $\mathfrak{g}$, thus the representation extends to $\text{Sym}(V)$ and $\wedge(V)$. Also it preserves degree, thus it induces representations on $\text{Sym}^k(V)$ and $\wedge^k(V)$.

**Proof:**

$$g(a \otimes a) = g(a) \otimes a + a \otimes g(a) = (a + g(a)) \otimes (a + g(a)) - a \otimes a - g(a) \otimes g(a)$$

and

$$g(a \otimes b - b \otimes a) = g(a) \otimes b + a \otimes g(b) - g(b) \otimes a - b \otimes g(a) = g(a) \otimes b - b \otimes g(a) + a \otimes g(b) - g(b) \otimes a$$  

□
Def. (2.5.9.4) [Dual Representation]. If \((\varphi, V)\) is a representation of \(g\), we define the **dual representation** \((\varphi^*, V^\vee)\) as
\[
(\varphi^*(g)(v^*), v) = (v^*, \varphi(g)v).
\]

Def. (2.5.9.5) [Trace Form]. The **trace form** of a representation \((V, \rho)\) of a Lie algebra \(g\) is an invariant symmetric form \(\beta_\rho\) defined by \((x, y) \mapsto \text{tr}(\rho(x) \circ \rho(y))\).

**Proof:** It is invariant because
\[
\text{tr}(\rho([x, y]) \circ \rho(z)) = \text{tr}(\rho(x)\rho(y)\rho(z)) - \text{tr}(\rho(y)\rho(x)\rho(z)) = \text{tr}(\rho(x)\rho(y)\rho(z)) - \text{tr}(\rho(x)\rho(z)\rho(y)) = \text{tr}(\rho(x)\rho([y, z])).
\]

Prop. (2.5.9.6). If \(\rho\) is a faithful representation of \(g\) and \(g\) is semisimple, then \(\beta_\rho\) is non-degenerate.

**Proof:** The Cartan’s criteria (2.5.1.27) shows \(g^\perp\) is a solvable sub-Lie algebra, so it must be 0 as \(g\) is semisimple (2.5.1.23). □

Prop. (2.5.9.7). Let \(L\) be a simple lie algebra, then any two non-degenerate symmetric invariant bilinear forms on \(L\) is proportional. Because any of this form corresponds to a \(L\)-morphism from \(L\) to \(L^*\). In particular, when \(L \subset gl_n\), the usual trace is proportional to the Killing form.

**Remark (2.5.9.8) [Rep(\(g\)].** Let \(g\) be a Lie algebra over a field \(k\), let Rep(\(g\)) denote the category of f.d. representations of \(g\).

Prop. (2.5.9.9) [Schur’s Lemma]. Let \(g\) be a finite Lie algebra, \(M\) be an irreducible \(g\)-module, then \(\dim M\) is countable. In particular, Shur’s lemma holds by (15.1.1.9).

**Proof:** It is of countable dimensional because \(\dim U(g)\) is countable. □

Prop. (2.5.9.10) [Generalized Eigenspace Decomposition for Nilpotent Lie Algebras]. Assume \(k\) is alg.closed, and \(g\) is a nilpotent algebra, and \((V, \rho)\) is a representation of \(g\), then there is a generalized eigenspace decomposition
\[
V = \bigoplus_{\lambda \in g^*} V^\lambda,
\]
where \(V^\lambda\) are the generalized eigenspaces, and they are stable under action of \(g\).

**Proof:** We use an induction argument:

If each \(a \in \mathfrak{h}\) has only one eigenvalue, then \(V\) is the generalized eigenspace \(V^\lambda\) for some function \(\lambda\) on \(\mathfrak{h}\). Then it suffices to show that \(\lambda\) is linear. But this is because by Lie’s theorem elements of \(\mathfrak{h}\) has a common eigenvector.

If for some \(a_0\), \(\text{ad}(a_0)\) has two eigenvalues. Now \(\mathfrak{h}\) is nilpotent, so \(\mathfrak{h} \subset \mathfrak{h}^0\), and hence \(\pi(h)V^{a_0}_\lambda \subset V^{a_0}_\lambda\) for any \(\lambda\) by (2.5.1.12).

As \(k\) is alg.closed, \(V\) can be written as a sum of generalized eigenspaces of \(a_0\), and each generalized eigenspace is a subrepresentation of \(\mathfrak{h}\), thus we can use induction. □
Def. (2.5.9.11) [Casimir Operator]. Let \( g \) be a semisimple Lie algebra of dimension \( n \), and \( \beta : g \times g \to k \) a non-degenerate invariant bilinear form on \( g \). Let \( e_i \) be a basis of \( g \) and \( e'_i \) be the dual basis under \( \beta \), then \( c = \sum e_i e'_i \in U(g) \) is independent of the basis, and lies in the center of \( U(g) \).

Now the trace form \( \beta_V \) for a faithful representation \( g \to gl_V \) of \( g \) is non-degenerate and invariant \((2.5.9.6)\), then the corresponding elements \( c'_\rho \) is called the Casimir element of \((V, \rho)\), and the action \( c_V \) of \( c'_\rho \) on \( V \) is called the Casimir operator of \((V, \rho)\).

The Casimir operator \( c_V \) is a \( g \)-module homomorphism, and has trace \( n \).

\( \square \)

Def. (2.5.9.12) [Unimodular Lie Algebras]. A f.d Lie algebra \( g \) is called unimodular if \( \wedge \text{ad} \) is a trivial representation of \( g \).

Prop. (2.5.9.13).

- If \( g = [g, g] \), then \( g \) is unimodular.
- If \( g \) is nilpotent, then \( g \) is unimodular.
- If \( g_1, g_2 \) is nilpotent, then \( g_1 \oplus g_2 \) is unimodular.
- If \( g \) is reductive, then \( g \) is unimodular.

Lemma (2.5.9.14) [Zassenhaus]. Let \( g \) be a Lie algebra and \( g' \) an ideal of \( g \). A representation \( \rho' \) of \( g' \) extends to a representation \( \rho \) of \( g \) that \( n_{\rho'}(g') \subset n_{\rho}(g) \) if there exists a Lie subalgebra \( h \) of \( g \) that \( g = g' \oplus h \) and \( [h, g'] \subset n_{\rho'}(g') \). If moreover \( \text{ad}_g(x)|_{g'} \) is nilpotent for all \( x \in h \), then \( \rho \) can be chosen that \( h \subset n_{\rho}(g) \).

\( \square \)

Prop. (2.5.9.15) [Nilpotent Representation Extension]. Let \( g \) be a Lie algebra, \( \alpha \) a nilpotent ideal of \( g \), and \( \rho \) a representation of \( \alpha \) that \( \rho(x) \) is nilpotent for all \( x \in \alpha \). Then \( \rho \) extends to a representation \( \rho' \) of \( g' \) that \( \rho'(x) \) is nilpotent for all \( x \in n \) the largest nilpotent ideal of \( g \).

\( \square \)

Thm. (2.5.9.16) [Ado]. Let \( g \) be a Lie algebra over a field \( k \) of char\(0\), then there exists a faithful representation \( \rho \) of \( g \) that \( \rho(n) \) consists of nilpotent endomorphisms, where \( n \) is the largest nilpotent radical. If \( g \) is of f.d., then this representation can be chosen to be of f.d.. In particular, any finite dimensional Lie algebra can be embedded in some \( gl(n, k) \).

\( \square \)
Remark (2.5.9.17). In fact, this is true for Lie algebras over a field of char $p$, too, Cf.[JACOBSON, N. 1962. Lie algebras.] Chap 6.3.

**Semisimple Representations**

For representations of a semisimple Lie algebra, See 15.15.

10 Lie Algebra Cohomology

Main references are [Wei94] and [Eti21].

**Prop. (2.5.10.1)** [Chevalley-Eilenberg resolution].

11 Amitsur-Levitski

**Preliminary**

Notice that in this paper, Kostant considers **reductive** lie groups. But in the range of this paper, the abelian part makes no contribution in the alternative part because they commutes with all elements. So We well just consider a **semisimple** Lie algebra in order to get a non-degenerate Killing form.

**Prop. (2.5.11.1).**

\[
\Gamma(\wedge^{2k}(\mathfrak{g})) = R^k \subset S^k(\mathfrak{g})
\]

\[
\Gamma(x_1 \wedge \cdots \wedge x_k) = \sum_{v \in \Pi_k} [x_v(1), x_v(2)] \cdots [x_v(2k-1), x_v(2k)]
\]

**Proof:** The proof is in fact simple, just notice that for every $v \in \Pi_k$ a representative of the subgroup $\Sigma_{2k,2}$ permuting the unordered pairs $\{(1,2), (3,4), \ldots, (2k-1,2k)\}$, the element in $v\Sigma_{2k,2}$ in fact combine in pairs to $[x_{v(2i-1)}, x_{v(2i)}]$ and together the $k!$ permutation of them compose a $[x_{v(1)}, x_{v(2)}] \cdots [x_{v(2k-1)}, x_{v(2k)}]$. \hfill \Box

Later he finds the dual of $\Gamma$, that is:

**Prop. (2.5.11.2).** $\gamma$ is $B$ dual to $\Gamma$,

\[
(\Gamma(\zeta), y_1 \cdots y_r) = (-1)^r (\zeta, dy_1 \wedge \cdots \wedge dy_r) \quad \forall \zeta \in \wedge^{2r}\mathfrak{g} \text{ and } y_i \in \mathfrak{g}.
\]

In particular,

\[
\Gamma(\zeta)(x) = \frac{(-1)^r}{r!} (\zeta, (dx)^r) \quad \forall \zeta \in \wedge^{2r}\mathfrak{g} \text{ and } x \in \mathfrak{g}.
\]

For the proof just notice that $(-dw, x_i \wedge x_j) = (w_i, [x_i, x_j])$ and

\[
(x_1 \otimes \cdots \otimes x_r, y_1 \otimes \cdots \otimes y_r) = \sum_{\sigma} (x_1, y_{\sigma(1)}) \cdots (x_r, y_{\sigma(r)})
\]

So dim of $R^k$ equals the dim of image of $\gamma_r$, that is, spanned by $(dx)^k$(because they are dual).

We say that a representation of $\mathfrak{g}$ satisfies m-fold standard identity if the alternating sum of any m elements of image of $\mathfrak{g}$ is 0. Obviously, this is equivalent to:

\[
\tau(R^k(\mathfrak{g})) \subset \ker \pi_V
\]
Now let \( o(g) \) be the maximum rank of \( dw, w \in g \), then by the discussion of the first paper, when \( g \) is semisimple, \( o(g) = r \). So the \( 2r \)-identity is satisfied by any representation of \( g \).

Furthermore, a prop of [Harish-Chandra] assert for any nonzero element \( u \in U(g) \), there is a representation such that \( \pi(U) \neq 0 \). So this is a sharp bound for general representations.

But one might naturally ask: Can we find the specific bound for a particular representation of a specific \( g \)? The answer is YES.

**Prop. (2.5.11.3).** \( \gamma \) vanishes on the ideal \( J_+ \cdot S(g) \).

**Proof:** The proof comes from the observation \( \pi \) is a \( G \)-map and by Cartan-Koszul theory, invariant elements in \( \wedge g \) are naturally isomorphic to the cohomology of \( g \) and \( \gamma(w) = -dw \) is clearly exact, thus \( \gamma(w_1 w_2 \ldots w_i) = \gamma(w_1) \wedge \cdots \wedge \gamma(w_i) \) is exact too. So \( \gamma(w) = 0 \).

**Cor. (2.5.11.4).** \( M = R^r \in H^r \), so it consists of harmonic functions.

**Proof:** \( (u, \Gamma(y)) = (\gamma(u), y) = 0 \) \( \forall u \) invariant, by Thm; so \( R^k = \text{Image} \Gamma \) is harmonic.

**Generalized Amitsur-Levitski**

Let \( E^k \subset U(g) \) be spanned by \( y^k, y \) nilpotent in \( g \), and \( Z \) the center.

In [Kos97] Kostant proved that the PBW isomorphism \( \delta : S(g) \to U(g) \) induces \( J, \delta(H) = E \).

So \( \tau : T(g) \to U(g) \) induces

\[
\tau(A^{2k}(g)) = \delta(R^k(g)) \subset E^k.
\]

Define \( \epsilon(\pi) \) the minimum integer \( k \) that \( \pi(y)^k = 0, \forall y \) nilpotent in \( g \). Then clearly:

**Prop. (2.5.11.5)[Generalized Amitsur-Levitski].** \( \pi \) satisfies the \( 2\epsilon(\pi) \)-fold standard identity.

**Prop. (2.5.11.6).** If \( \pi \) satisfies the \( m \)-identity, it satisfies the \( m + 1 \)-identity (By taking a summation on a fixed first element \( \sigma(1) \)).

**Prop. (2.5.11.7).**

- Let \( \pi \) be the natural representation of \( gl_n \) on \( \mathbb{C}^n \) then \( \epsilon(\pi) = n \).

- If \( n \) even and \( \pi \) the natural representation of skew-symmetric matrices on \( \mathbb{C}^n \) then \( \epsilon(\pi) = n - 1 \).

From this one derives the classical Amitsur-Levitski prop that \( GL_n(\mathbb{C}) \) satisfies the \( n \)-fold standard identity.

**Proof:**

1: the abstract Jordan decomposition which assures \( x \) is nilpotent in \( gl_n \) if \( \pi(x) \) is nilpotent.

2: comes from the Lacobson-Morosov Thm that any nilpotent element of \( g \) is contained in a \( sl_2 \)-triple. Thus we only need to show that \( W \) is reducible considered as this \( sl_2 \)-triple-module.

But then an irreducible representation of \( sl_2 \) preserves a non-degenerate bilinear form it must be odd dimensional cause a non-degenerate bilinear form is equivalent to a \( g \)-map from \( V \) to \( V^* \).

And there can be constructed an anti-symmetric form defined on the \( sl_2 \)-representation on \( \text{Sym}_{2k}[x, y] \) by (2.5.11.9), so there can’t exist symmetric \( g \)-invariant form. So this representation must be reducible.
Cor. (2.5.11.8) [Classical Amitsur-Levitski]. By (2.5.11.5),

\[ [[x_1, x_2, \ldots, x_n]] = \sum_{\sigma} \text{sgn}(\sigma)x_{\sigma(1)}x_{\sigma(2)}\cdots x_{\sigma(k)} = 0 \quad \forall x_i \in \mathfrak{gl}_n \]

called \textit{n-fold standard identity}.

Prop. (2.5.11.9). For a construction of the anti-symmetric form, notice

\[ \pi(g)f(x_1, x_2) = f(g_{11}x_1 + g_{12}x_2, g_{21}x_1 + g_{22}x_2). \]

Set

\[ v_k = \left(\begin{array}{c} m \\ k \end{array}\right)x_1^{m-k}x_2^k, \quad \Omega(v_k, v_{m-k}) = (-1)^k \left(\begin{array}{c} m \\ k \end{array}\right). \]

One verifies:

\[ \Omega(g \cdot u, g \cdot v) = (\det g)^m \Omega(u, v) \quad \forall g \in GL(2, \mathbb{C}) \]

So when \( m = n - 1 \) is odd, this is a symplectic form preserved by \( \mathfrak{sl}_2 \).

A computable Formula

Finally, Kostant gave a computable formula for determining \( \epsilon(\pi) \). Clearly we just need to consider irreducible representation.

Let \( \pi_\lambda \) be the irreducible representation of highest weight \( \lambda \), then the dual representation \( \pi_\lambda' \) has highest weight the negative of the lowest weight of \( \pi_\lambda \), that is, \( -w_0(\gamma) \).

But then \( \lambda + \lambda' \) is a sum of simple positive roots. \( \lambda + \lambda' = \sum_{i=1}^n m_i \alpha_i \). Put \( \epsilon(\lambda) = 1 + \sum_{i=1}^n m_i \). Then:

Prop. (2.5.11.10). \( \epsilon(\pi_\lambda) = \epsilon(\lambda) \).

\textit{Proof:} Just choose a \( \mathfrak{sl}_2 \)-triple \( \{e, x, f\} \) with \( \alpha(x) = 2 \ \forall \alpha \) simple root. Then \( \lambda(x) \) and \( -\lambda'(x) \) are respectively the maximal and minimal eigenvalues of \( \pi(x) \). \( (\lambda + \lambda')(x) = 2(\epsilon(\lambda) - 1) \). Thus \( f \) has nilpotent degree \( \epsilon(\lambda) \). And any nilpotent element action increases the eigenvalue of an eigenvector of \( x \) by at least 2, the prop follows. \( \square \)

Further Work

(cf. [Pro76]) Another different proof of the Amitsur-Levitski theorem is given by Kostant using techniques related to \textit{trace identities}. It turns out that method sheds more light. Later is studied the polynomial of matrices invariant under the conjugation action.

Artin conjectured that all the invariants is polynomials of the Trace polynomial \( Tr(A_1A_2\cdots A_n) \) (Proved)

And further, the relations among these invariant all turned out to be consequences of the prop of Hamilton-Cayley. All this is made into the \textit{Invariant Theory}.

Prop. (2.5.11.11) [Interesting results].

1. If an algebra over a field of characteristic 0 satisfies the identity \( X^n = 0 \), then it satisfies all the identities of \( n \times n \) matrices.

2. The space of multilinear identities of degree \( m \) of \( n \times n \) matrices can be described completely in terms of Young diagrams.
12 Lie $p$-Algebras

Remark (2.5.12.1). In this subsection, let $k$ be a field of characteristic $p$.

Def. (2.5.12.2) [Lie $p$-Algebras]. Let $x_0, x_1$ be elements of a Lie algebra over $k$ of characteristic $p$, then for $0 < r < p$, let $s_r(x, x_1)$ denote $\frac{1}{r}$ times coefficient of $t^{r-1}$ in the expression of $\text{ad}^{p-1}_{x+y}(x)$.

Then a Lie $p$-algebra is a Lie algebra $\mathfrak{g}$ over $k$ equipped with a map $x \mapsto x[p]: \mathfrak{g} \rightarrow \mathfrak{g}$ such that

- $(cx)^{[p]} = c^px^{[p]}$ where $c \in k$.
- $\text{ad}(x^{[p]}) = (\text{ad}(x))^{p}$.
- $(x+y)^{[p]} = x^{[p]} + y^{[p]} + \sum_{i=1}^{p-1} s_r(x, y)$.

Example (2.5.12.3). If $L$ is an Abelian Lie algebra, then it can be regarded as a Lie $p$-algebra by assigning $x[p] = 0$.

If $A$ is an associative algebra, then it can be given a Lie $p$-algebra structure by assigning $x[p] = x^p$.

Proof: To show $A$ is a Lie $p$-algebra, we check $\text{ad}(x)^p(y) = (l_x - r_x)^p(y) = l^p_x - r^p_x(y) = \text{ad}(x^p)(y)$.

Prop. (2.5.12.4) [Representations]. A representation of a Lie $p$-algebra $\mathfrak{g}$ over a $k$-vector space $V$ is a homomorphism $\mathfrak{g} \rightarrow \mathfrak{gl}_V$ of Lie $p$-algebras.

Def. (2.5.12.5) [Universal Enveloping $p$-Algebra]. The universal enveloping $p$-algebra of a Lie $p$-algebra $\mathfrak{g}$ is defined to be

$$U[p](\mathfrak{g}) = T(\mathfrak{g})/J[p], \quad T(\mathfrak{g}) = \bigoplus_{n=0}^{\infty} \mathfrak{g}^\otimes n$$

which is a graded algebra $T(\mathfrak{g})$ quotients the ideal $J = \{x \otimes y - y \otimes x - [xy], x^\otimes p - x^{[p]}\}$.

There is a natural linear map $\sigma: \mathfrak{g} \rightarrow U[p](\mathfrak{g})$.

Prop. (2.5.12.6). The universal enveloping $p$-algebra $U[p]: \mathfrak{g} \mapsto U[p](\mathfrak{g})$ defines a functor LieAlg $\rightarrow$ AssAlg that is left adjoint to the canonical functor $\text{AssAlg}_k \rightarrow \text{LieAlg}_k(2.5.12.3)$.

Proof: For any associative algebra $A$ and a morphism of Lie $p$-algebras $\mathfrak{g} \rightarrow [A]$, there is easily seen a morphism $U[p](\mathfrak{g}) \rightarrow A$, and it is unique.

Cor. (2.5.12.7) [Representation as Modules]. A representation of $\mathfrak{g}(2.5.12.4)$ is same as a representation of $U[p](\mathfrak{g})$.

Prop. (2.5.12.8). Let $e_i$ be a $k$-vector space basis of $\mathfrak{g}$, then the monomials

$$\{e_{i_1}^{n_1} e_{i_2}^{n_2} \cdots e_{i_r}^{n_r} | i_1 < i_2 < \ldots < i_r, 0 < n_{i_k} < p\}$$

for different $r$ form a basis of $U[p](\mathfrak{g})$.

Proof: This is a consequence of PBW theorem (2.5.8.4).

Cor. (2.5.12.9). If $\mathfrak{g}$ is of finite dimensional over $k$, then so does $U[p](\mathfrak{g})$, and the map $i: \mathfrak{g} \rightarrow U[p](\mathfrak{g})$ is injective.
2.6 Infinite Dimensional Lie Algebras

References are [What is moonshine?], [Vertex Operator Algebras and the Monster], [Infinite-Dimensional Lie Algebras, Kac], [Car05].

1 Kac-Moody Algebras
2 Vertex Operator Algebras
3 Moonshine Conjectures

Thm. (2.6.3.1) [Monstrous Moonshine]. There is a naturally defined graded infinite dimensional module, called the Monstrous module $V = \bigoplus_{n \in \mathbb{Z}} V_n$ of the monster group $M$ s.t. for any $g \in M$, the Mckay-Thompson series

$$T_g(\tau) = \sum_{n \geq -1} \text{tr}(g|V_n)e^{2\pi inr}$$

is a Hauptmodul for a discrete subgroup $\Gamma \subset SL(2,\mathbb{Z})$ of genus 0 and period $r$ at the cusp.

Proof: Cf.[Borcherds, 1992]

Prop. (2.6.3.2) [Duncan-Mertens-Ono, 2017]. There exists an infinite dimensional module $V = \bigoplus_{n>0, n \equiv 0, 3 \mod 4} V_n$ of the O'Nan group (2.1.13.5) ON s.t. for any $g \in ON$, the Mckay-Thompson series

$$F_g(\tau) = q^{-4} + 2 + \sum_{n>0} \text{tr}(g|V_n)e^{2\pi inr}$$

is a meromorphic modular form of weight $\frac{3}{2}$ on $\Gamma_0(4N)$, where $N$ is the order of $g$.

Proof:
2.7 Reflection Groups and Coxeter Groups

Main references are [Hum90], [Ser87], [Kna96].

Notations (2.7.0.1).
- Let $k \in \text{Field}$, char $k = 0$, $V \in \text{Vect}_k$.

1 Reflection Groups

Def. (2.7.1.1) [Reflections]. Let $V \in \text{Vect}^d / k$, a reflection on $V$ is a linear transformation $s \in \text{End}(V)$ that has $d - 1$ eigenvalues 1 and one eigenvalue $-1$.

Prop. (2.7.1.2). Let $\alpha \in V$ and $\alpha^\vee \in V^\vee$ that $(\alpha, \alpha^\vee) = 2$, then

$$s_\alpha : x \mapsto x - (x, \alpha^\vee)\alpha$$

is a reflection, and every reflection with vector $\alpha$ is of this form.

Proof: Clearly $s_\alpha$ is a reflection, and if $s$ is any reflection, then $\alpha^\vee$ is the composition of the quotient map $V \to V/H$ with the map $V/H \to F$ sending $\alpha + H$ to 1. □

Lemma (2.7.1.3). Let $R \subset V$ be a set s.t. span$\{R\} = V$, then for any $\alpha \in V$, there exists at most one reflection $s$ with vector $\alpha$ that $s(R) \subset R$.

Proof: Let $s, s'$ be two such reflections, then $t = ss'$ is an automorphism that is identity on both $F\alpha$ and $V/F\alpha$. So $(t - 1)^2 = 0$ on $V$. So the minimal polynomial of $T$ divides $(T - 1)^2$. Also because $R$ is finite there exists an $m$ that $t^m = 1$ on $R$ thus on $V$, so $t = 1$ as the greatest divisor of $(T - 1)^2$ and $T^m - 1$ is $T - 1$. □

Lemma (2.7.1.4). Let $V$ be an inner product space, then for any vector $\alpha$, there exists a unique reflection $s_\alpha$ that respects the inner product, which is

$$s_\alpha(x) = x - 2\frac{(x, \alpha)}{(\alpha, \alpha)}\alpha.$$

Def. (2.7.1.5) [Reflection Groups]. $\Gamma \leq \text{GL}(n, k)$ is called a reflection group if it is generated by reflections.

Thm. (2.7.1.6) [Shephard-Todd-Chevalley]. Let $\Gamma \leq \text{GL}(n, k)$, then $\Gamma$ is a reflection group iff $k[X_1, \ldots, X_n]^\Gamma$ is a polynomial ring. And in this case,
- There are homogenous alg.ind polynomials $p_1, \ldots, p_r$, $d_i = \deg(p_i)$, $d_1 \leq d_2 \leq \ldots \leq d_r$ s.t. $k[X_1, \ldots, X_n]^\Gamma = k[p_1, \ldots, p_r]$.
- $\frac{1}{\# \Gamma} \sum_{\gamma \in \Gamma} \frac{\text{tr}(\gamma)}{\det(1 - \gamma T)} = \prod_{i=1}^r \frac{1}{1 - Td_i} \in k(T)$.
- $(d_1, \ldots, d_r)$ are determined by $\Gamma$.
- $\# \Gamma = \prod_i d_i$, and $\Gamma$ contains $\sum_i (d_i - 1)$ reflections.
- If $\Gamma$ is an irreducible subgroup of $\text{GL}(n, k)$, then it is an abstractly irreducible group, and $Z(\Gamma)$ is cyclic of order $\text{pgcd}(d_1, \ldots, d_r)$.

Proof: □
2 Root Systems

Def. (2.7.2.1) [Root System]. A subset $R$ of a vector space $V$ over $F$ is called a root system if
- $R$ spans $V$ and doesn’t contain 0.
- For each $\alpha \in R$, there exists a unique reflection $s_\alpha = \text{id} - \alpha^\vee \otimes \alpha$ with vector $\alpha$ that $s_\alpha(R) \subset R$.
- For any $\alpha, \beta \in R$, $s_\alpha(\beta) - \beta$ is a multiple of $\alpha$, or equivalently $\alpha^\vee(\beta) \in \mathbb{Z}$.

Elements of $R$ are called the roots of $R$, and dimension of $V$ is called the dimension of the root system. And the subgroup of $GL(V)$ generated by all $s_\alpha$ is called the Weyl group of $R$. The Weyl subgroup is a finite group, as a subgroup of the group of permutations of $R$.

A root system is called indecomposable iff it cannot be written as a direct sum of two root systems.

Def. (2.7.2.2) [Reduced Root System]. Let $\alpha, \beta$ be roots that are multiples of each other, then $\beta = c\alpha$ for some $c \in F$, then $2(\beta, \alpha^\vee) = 2c \in \mathbb{Z}$, also $2c^{-1} \in \mathbb{Z}$, so $c \in \{-1, -1/2, 1/2, 1\}$. A reduced root system is a root system that there are no roots $\alpha, \beta$ that $\alpha = 2\beta$.

Prop. (2.7.2.3) [Invariant Quadratic Form]. Let $R$ be a root system in $V$, then there is a positive bilinear form in $V$ that is invariant under the action of the Weyl group of $R$.

Notice that for such a bilinear form, the reflection must be of the form given in (2.7.1.4), or in other words, $\alpha^\vee(\beta) = \left(\frac{2\alpha}{(\alpha, \alpha)}, \beta\right)$.

Proof: This follows entirely because the Weyl group of $R$ is finite, as we can take the average of any positive bilinear form under the action of reflections.

Def. (2.7.2.4) [Dual Root System]. Let $R$ be a root system in $V$, the set of dual vectors $\alpha^\vee$ for $\alpha \in R$ is also a root system in $V^\vee$, called the dual system of $R$. And it has the same Weyl group as $R$.

Moreover, $R^\vee \cong R$.

Proof: Take an invariant quadratic form on $V(2.7.2.3)$, then it gives an isomorphism $V \rightarrow V^\vee$. Then $\alpha^\vee$ corresponds to $\frac{2\alpha}{(\alpha, \alpha)}$ under this isomorphism, and there obviously generates $V$. If $\alpha^\vee \in R^\vee$, we can take the corresponding reflection to be $s_{\alpha^\vee} = 1 - \alpha \otimes \alpha^\vee$. Then

$$s_{\alpha^\vee}(\beta^\vee)(x) = (\beta^\vee - \beta^\vee(\alpha)\alpha^\vee)(x)$$

$$= (x, 2\beta/(\beta, \beta)) - \frac{(\alpha, \beta)}{(\beta, \beta)}(x, 2\alpha/(\alpha, \alpha))$$

$$= (x, \frac{2(\beta - \alpha(\alpha, \beta)/(\alpha, \alpha))}{(\beta, \beta)})$$

$$= (x, \frac{2s_\alpha(\beta)}{(\beta, \beta)}) = (s_\alpha(\beta))^\vee(x).$$

So $s_{\alpha^\vee}(\beta^\vee) = (s_\alpha(\beta))^\vee \in R^\vee$. In this way, we see $\alpha^\vee \vee = \alpha$, and $s_{\alpha^\vee}(\beta^\vee) - \beta^\vee = \beta^\vee(\alpha)\alpha^\vee$ is an integral multiple of $\alpha^\vee$. Also it can be seen easily from the formula above that the Weyl group is the same as the Weyl group of $R$.

Prop. (2.7.2.5) [Real Root Systems]. Let $R$ be a roots system in a vector space $V$ over a field $F$, and let $V_0$ be the $\mathbb{Q}$-vector space spanned by $R$, then $R$ is a root system in $V_0$ and $V_0 \otimes_{\mathbb{Q}} F \cong V$.

So from now on we focus on a real root system.
Proof: The non-trivial part is that the isomorphism $V_0 \otimes \mathbb{Q} \mathbb{F} \cong V$. The natural map $i : V_0 \otimes \mathbb{Q} \mathbb{F} \to V$ is surjective because $R$ generates $V$, and consider its transpose

$$i^* : V^\vee \to V_0^\vee \otimes \mathbb{Q} \mathbb{F},$$

then we can see that this maps $\alpha^\vee$ to $\alpha_0^\vee$, and $R_0^\vee$ is a root system in $V_0^\vee$, thus $\alpha_0^\vee$ generates $V_0^\vee$, and $i^*$ is surjective, showing $i$ is injective. \qed

**Def. (2.7.2.6)** [Base]. A subset $S \subset R$ is called a base of $R$ if every elements of $R$ can be written uniquely as a linear integral combination of elements of $S$ with the same sign.

If $S$ is a base of $R$, then we let $R^+$ denote the set of $R$ that is non-negative integral combinations of elements of $S$, called the positive roots of $R$, and $R^-$ the set of $R$ that is non-positive integral combinations of elements of $S$, called the negative roots of $R$. $R = R^+ \sqcup R^-.$

**Prop. (2.7.2.7)** [Base exists]. Let $t \in V^\vee$ be an element that $t(\alpha) \neq 0$ for all $\alpha \in R$. Let $R_t^+(R_t^-)$ be the set of all $\alpha \in R$ that $t(\alpha) > 0(<0)$, then $R = R_t^+ \cup R_t^-$. An element of $R_t^+$ is called indecomposable if it cannot be written as the sum of two elements in $R_t^+$. Let $S_t$ be the set of indecomposable elements of $R_t^+$, then $S_t$ is a base of $R$.

In particular, every root system $(R,V)$ contains a base. And if $S$ is a base and $t \in V^\vee$ that $t(S) > 0$, then $S = S_t$.

**Proof:** Cf.[Ser87]P38. \qed

**Cor. (2.7.2.8).** If $t \in V^\vee$ and $S_t$ is a basis of $V$ contained in $R_t^+$ that attains the minimal value of $t$ in $R_t^+$, then $S_t$ is a base of $R$.

**Prop. (2.7.2.9).** Let $S$ be a base of a root system $(R,V)$, then every positive root $\beta$ can be written as

$$\beta = \alpha_1 + \ldots + \alpha_k$$

in such a way that all the partial sums are roots.

**Proof:** Cf.[Ser87]P40. \qed

**Prop. (2.7.2.10).** Let $R$ be a reduced root system and $S$ a base, then for any $\alpha \in S$,

$$s_\alpha(R^+ \setminus \{\alpha\}) = R^+ \setminus \{\alpha\}.$$ 

In particular if $\rho = \frac{1}{2}(\sum_{\alpha \in R^+} \alpha)$, then $s_\alpha \rho = \rho - \alpha$.

**Proof:** If $\beta \in R^+$, then $s_\alpha(\beta) = \beta - c\alpha$ for some $c > 0$, Thus $s_\alpha(\beta) \in R^-$ iff $\beta = \alpha$. \qed

**Prop. (2.7.2.11)** [Base and Dual System]. Let $R$ be a reduced system and $S$ a base, then $S^\vee$ is a base of $R^\vee$.

**Proof:** By the isomorphism between $V$ and $V^\vee$, it suffices to show the vectors $\{\alpha^\vee, \alpha \in S\}$ is a base for $R^* = \{\alpha^\vee, \alpha \in R\}$. But it is clear if $S$ is a base corresponding to a vector $t \in V^*$, then $\{\alpha^\vee, \alpha \in S\}$ is the extremal vectors corresponding to $t$ too, so it is a base by(2.7.2.7). \qed
2.7. REFLECTION GROUPS AND COXETER GROUPS

Property of the Weyl Group

Prop. (2.7.2.12) [Weyl Group and Bases]. Let \( W \) be the Weyl group of a reduced root system \( R \) and \( S \) a base of \( R \), then
1. For any \( t \in V^* \), there exists \( w \in W \) that \( (w(t),\alpha) \geq 0 \) for all \( \alpha \in S \).
2. \( W \) acts transitively on the set of bases of \( R \).
3. For each \( \beta \in R \), there exists some \( w \in W \) that \( w(\beta) \in S \).
4. The group \( W \) is generated by \( s_\alpha \) where \( \alpha \in S \).
5. \( W \) acts simply transitively on the set of bases of \( R \).

Proof: We can in fact prove this for \( W_S \) the group generated by \( s_\alpha \) where \( \alpha \in S \).

1. Let \( \rho \) be defined in (2.7.2.10), and choose an element \( w \in W_S \) that \( w(t)(\rho) \) is maximal, then \( w(t)(\rho) \geq w(t)s_\alpha(\rho) = w(t)(\rho) - w(t)(\alpha) \). So \( (w(t),\alpha) \geq 0 \).
2. Let \( S' \) be a base and \( t' \in V^* \) that \( t'(S') > 0(2.7.2.7) \). Also by 1 we can find \( w \in W \) that \( w(t)(\alpha) \geq 0 \) for all \( \alpha \in S \). And in fact \( w(t)(\alpha) > 0 \) for all \( \alpha \in S \). So \( S = S t, S' = S_{w(t)} \). Thus \( w \) sends \( S' \) to \( S \).
3. Finally we prove that \( W_S = W \): because for any \( \beta \in R \), there exists \( w \in W_S \) that \( w(\beta) \in S \), so \( s_\beta = w^{-1}s_{w(\beta)}w \in W_S \).
4: See [Ser87]P70.

Def. (2.7.2.13) [Length]. Let \( w \in W \), define the length of \( w \) to be the minimal number \( m \) that \( w \) can be written as a product of \( m \) simple reflections \( s_i \).

Prop. (2.7.2.14). Let \( R \) be a root system with Weyl group \( W \), \( w \in W \).
- Let \( n(w) \) be the number of elements \( \alpha \in R^+ \) that \( w(\alpha) \in R^- \), then \( n(w) = l(w) \).
- There is a unique element \( w_0 \in W \) with length \( |R^+| \).
- \( w_0(R^+) = R^- \), and \( w_0^2 = \text{id} \).

Proof: 1: Cf.[Carter, P63].
2: By (2.7.2.12) there is a unique element \( w_0 \in W \) mapping \( S \) to \( -S \), and it has maximal length \( |R^+| \) by item1.
3: \( w_0^2(R^+) = R^- \), thus \( l(w_0^2) = 0 \) and \( w_0^2 = \text{id} \).

Def. (2.7.2.15) [Weyl Chambers]. Let \( (V,R) \) be a real root system, then a Weyl chamber is a connected component of \( V \setminus \bigcup_{\alpha \in R} H_\alpha \), where \( H_\alpha \) is the fixed hyperplane of vectors fixed by \( s_\alpha \).

Prop. (2.7.2.16). The Weyl group \( W \) acts transitively on the set of Weyl chambers of \( R \).

Proof: To show the action is transitive, if two Weyl chambers \( C, C' \) are adjacent with a common face \( F \subset H_\alpha \), then clearly \( s_\alpha(C) = C' \). In general, choose two generic vector in \( C, C' \) and connect them, then \( C, C' \) can be connected by adjacent chambers.
If \( w \in W \) satisfies \( w(C) = C \), we may assume \( C \) is the fundamental Weyl chamber, then \( w(S) = S \), so by (2.7.2.14), \( l(w) = 0 \), so \( w = \text{id} \).

Def. (2.7.2.17) [Height of Weights]. Let \( \alpha = \sum n_i\alpha_i \in R \), then the height of roots \( \alpha \) is denoted by \( \text{ht}(\alpha) = \sum n_i \).
Prop. (2.7.2.18) [Highest Root]. Let \((R, V)\) be a root system and \(S\) a base. If \(S\) is indecomposable, then there exists a root \(\bar{\alpha} = \sum_{\alpha \in S} n_\alpha \alpha\) that for any other root \(\sum_{\alpha \in S} m_\alpha \alpha, n_\alpha \geq m_\alpha\).

Proof: □

Def. (2.7.2.19) [Kostant’s Partition Function]. Let \(R\) be a root system, the Kostant’s partition function \(\Psi\) is a function on \(Q(R)\) that \(\Psi(\alpha)\) equals the number of ways to write \(\alpha\) as an unordered sum of positive roots in \(R^+\).

**Cartan Matrix and Dynkin Diagrams**

Prop. (2.7.2.20) [Angles Between Roots]. Let \(\alpha, \beta\) be two non-propositional roots in a root system \(R\), then we can put \(n(\alpha, \beta) = \alpha^\vee(\beta) = 2(\alpha, \beta)/(\alpha, \alpha)\). Then \(n(\alpha, \beta)\) are integers(2.7.2.1), and \(n(\alpha, \beta)n(\beta, \alpha) = 4 \cos^2 \varphi_{\alpha,\beta}\), where \(\varphi_{\alpha,\beta}\) is the angle between these two vectors. Then because \(4 \cos^2 \varphi_{\alpha,\beta}\) is an integer, it can only take values 0, 1, 2, 3. Then there are only 7 possibilities of the angles between \(\alpha, \beta\), and if \(\alpha, \beta\) are not orthogonal, their ration of lengths are determined also by the angle.

Prop. (2.7.2.21) [String of Roots]. If \(\alpha, \beta\) are not proportional and \(n(\beta, \alpha) > 0\), then \(\alpha - \beta\) is a root.

In particular, for \(\alpha, \beta \in S\) where \(S\) is a base of \(R\), \(n(\alpha, \beta) \leq 0\).

Proof: (2.7.2.20) shows \(n(\beta, \alpha) = 1\) or \(n(\alpha, \beta) = 1\). Now \(\alpha - \beta = s_\beta(\alpha)\) or \(-s_\alpha(\beta)\) is a root of \(R\). □

Def. (2.7.2.22) [Cartan Matrix]. Let \(R\) be a root system with a base \(S\). Then the Cartan matrix is \((n(\alpha, \beta))_{\alpha, \beta \in S}(2.7.2.20)\).

Prop. (2.7.2.23). The Cartan matrix depends only on \((V, R)\) and not on \(S\), and if \(R\) is reduced, \(R\) is determined by its Cartan matrix up to isomorphisms.

Proof: The first assertion follows from(2.7.2.12) as every two bases are conjugate. The Cartan matrix determines \(R\) because it determined the inner product between roots in a basis of \(V\). □

Prop. (2.7.2.24). Let \(E\) be the group of automorphisms of \(S\) that leaves that Cartan matrix invariant, then it can be identified with the set of automorphisms of \(R\) that leave the base \(S\) invariant. Then the group \(\text{Aut}(R)\) is isomorphic to the semi-product \(E \ltimes W\).

Proof: Let \(W\) is generated by \(s_\alpha\) so invariant under \(\text{Aut}(R)\). Now if \(u \in \text{Aut}(R)\), then \(u(S)\) is a base of \(R\), so there exists some \(w \in W\) that \(w(u(S)) = S\), thus \(u \in EW\). Also if \(w \in W \cap E\), then □

Def. (2.7.2.25) [Coxeter graph]. A coxeter graph is a finite graph that each pair of distinct vertices are connected by 0, 1, 2 or 3 vertices.

Def. (2.7.2.26) [Coxeter Graph associated to a Root System]. Let \((R, V)\) be a root system and \(S\) a base of \(R\), then the associated coxeter graph is a graph whose nodes are indexed by the elements of \(S\), and two distinct nodes \(\alpha, \beta\) are connected by \(a(\beta, \alpha)a(\alpha, \beta) = 4 \cos^2 \varphi_{\alpha,\beta}\) edges(2.7.2.20). This is independent of the choice of \(S\), by(2.7.2.23).

Prop. (2.7.2.27). \(R\) is indecomposable iff the Coxeter graph is connected.

Proof: By the formula in(2.7.1.4), \(R\) is decomposable iff \(R = R_1 \sqcup R_2\) where \(R_1, R_2\) are orthogonal to each other. Then this is equivalent to \(\varphi_{\alpha,\beta} = \pi/2\) for any \(\alpha \in R_1, \beta \in R_2\). □
3 Simple Root System

Lemma (2.7.3.1) [Listing of Indecomposable Root Systems]. The coxeter graphs $\Gamma$ arising from indecomposable root systems are exactly the graphs $A_n(n \geq 1), B_n(n \geq 2), D_n(n \geq 4), E_6, E_7, E_8, F_4, G_2$. (graphs are given in [Etingod, Lie algebras]P109.)

Proof: The existence is these types are given by (2.7.3.2).

For the converse, notice first that for a graph with vertices $v_i$ and $v_j$, $v_i, v_j$ are connected with $A_{ij}$ edges, the quadratic form

$$Q(x_1, \ldots, x_n) = \sum_{i=1}^{n} x_i^2 - \sum_{1 \leq i < j \leq n} \sqrt{A_{ij}}x_ix_j = \| \sum x_i v_i \|^2$$

is positive definite.

Next we show some constraints on the graph:

- Any subgraph of the coxeter graph, it can be shown that the corresponding quadratic form is also positive definite, in particular non-degenerate.
- If it is a tree: If it contains a circle, consider the subgraph of the circle, then the corresponding quadratic form vanishes on $(1, 1, \ldots, 1)$, contradiction.
- It doesn’t contains subgraphs listed in P77 of [Car05].

Now if $\Gamma$ contains a triple edge, then it must be $G_2$, otherwise it must contain a $\hat{G}_2$. If $\Gamma$ contains no triple edges, then it contains at most one double edge, otherwise it contains some $\hat{C}_l, l \geq 2$. If it contains only one double edge, then it contains no branch points, otherwise it contains some $\hat{B}_l, l \geq 3$, so it is a chain with an edge added. If the double edge is in one end, then it is $B_l$ for some $l \geq 3$, otherwise it must by $F_4$, in order not to contain $\hat{F}_4$.

Now we assume $\Gamma$ contains only simple edges. If it contains no branch point, then it is $A_l$ for some $l \geq 1$. But $\Gamma$ contains at most one branch point, and only 3 edges, otherwise it contains some $\hat{D}_l, l \geq 4$. If $\Gamma$ has only one branch point, then the graph is a center with three branches. One of the branch must be a single vertex, otherwise it contains a $\hat{E}_6$. Then a second branch must has $\leq 2$ vertices, otherwise it contains a $\hat{E}_7$. If the second branch has a single vertex, then $\Gamma \cong D_l$ for some $l \geq 4$. If the second branch has two vertices, then the third branch has $\leq 4$ vertices, otherwise it contains some $\hat{E}_8$. So $\Gamma \cong E_6, E_7$ or $E_8$. \qed

Prop. (2.7.3.2) [Listing of Indecomposable Root Systems]. Let $e_n$ be the standard basis of $\mathbb{R}^n$ with the standard bilinear form, and let $L_n$ be the subgroup generated by $e_n$. Then

- $A_n$: Let $V$ be the hyperplane of $\mathbb{R}^{n+1}$ orthogonal to the vector $e_1 + \ldots + e_{n+1}$, and $R$ be the subset of $L_{n+1} \cap V$ consisting of vectors of length $\sqrt{2}$. Then $(R, V)$ is a root system, and the Weyl group is the permutation group $S_n$ of $e_1, \ldots, e_{n+1}$. The polarization with $t(e_i) = n+1-i$ gives a base consisting of $\{e_i - e_{i+1}, i = 1, \ldots, n\}$ by (2.7.2.8).

- $B_n$: Let $V = \mathbb{R}^n$ and $R$ be the subset of $L_n$ consisting of vectors of length 1 or $\sqrt{2}$. Then $(R, V)$ is a root system, and the Weyl group is the permutation and sign changes of the vectors $e_i$, isomorphic to $\mathbb{Z}_2^n \times S_n$. The polarization with $t(e_i) = n+1-i$ gives a base consisting of $\{e_1 - e_2, \ldots, e_{n-1} - e_n, e_n\}$ by (2.7.2.8).

- $C_n$: Let $C_n$ be the dual system of $B_n(2.7.2.4)$, which by the invariant form isomorphic to the set of $\mathbb{R}^n$ consisting of vectors $\pm e_i \pm e_j, \pm 2e_i$. It has the same Weyl group as $B_n$. It has a base consisting of $\{e_1 - e_2, \ldots, e_{n-1} - e_n, 2e_n\}$ by (2.7.2.8).
• $D_n$: Let $V = \mathbb{R}^n$ and $R$ be the set of all vectors of $L_n$ of length $\sqrt{2}$. The Weyl group consists of permutations and sign changes of an even number of the vectors $e_i$. The polarization with $t(e_i) = n - i$ gives a base consisting of $\{e_1 - e_2, \ldots, e_{n-1} - e_n, e_n - e_1 + e_{n-1}\}$.

• $G_2$: Let $V = \mathbb{R}[\omega]$ and $R$ be the subset of $\mathbb{Z}[\omega]$ of norm 1 or 3. The Weyl group is isomorphic to the dihedral group. It clearly has a base consisting of $\{1, \omega - 1\}$.

• $F_4$: Let $V = \mathbb{R}^4$, and let $R$ be the set of vectors $\{\pm e_i, \pm e_i \pm e_j, \frac{1}{2}(\pm e_1 \pm e_2 \pm e_3 \pm e_4)\}$. It can be shown this is a root system. The polarization with

$$t(e_1) = 8, t(e_2) = 3, t(e_3) = 2, t(e_3) = 1,$$


gives a base consisting of $\{e_2 - e_3, e_3 - e_4, e_4, \frac{1}{2}(e_1 - e_2 - e_3 - e_4)\}$.

• $E_8$: Let $V = \mathbb{R}^8$ and

$$R_{E_8} = \{\pm e_i \pm e_j, i \neq j\} \cup \left\{\frac{1}{2}\sum_{i=1}^{8} \pm e_i\right\} \text{with even number of minus signs}\}.$$

The polarization with

$$t(e_1) = 23, t(e_2) = 6, t(e_3) = 5, \ldots, t(e_8) = 0$$

gives a base consisting of $\{e_2 - e_3, \ldots, e_7 - e_8, e_7 + e_8, \frac{1}{2}(e_1 - e_2 - \ldots - e_7 + e_8)\}$.

• $E_7$: $E_7$ is the intersection of $E_8$ with the hypersurface $\sum x_i = 0$, so

$$R_{E_7} = \{\pm(e_i - e_j), i \neq j\} \cup \left\{\frac{1}{2}\sum_{i=1}^{8} \pm e_i\right\} \text{with 4 minus signs}\}.$$

The polarization with

$$t(e_1) = 18, t(e_2) = 7, t(e_3) = 6, \ldots, t(e_8) = 1$$

gives a base consisting of $\{e_2 - e_3, \ldots, e_7 - e_8, \frac{1}{2}(e_1 - e_2 - e_3 - e_4 - e_5 + e_6 + e_7 + e_8)\}$.

• $E_6$: $E_6$ is the intersection of $E_7$ with the hypersurface $x_7 + x_8 = 0$.

$$R_{E_6} = \{\pm(e_i - e_j)|i \neq j \leq 6\} \cup \{\pm(e_7 - e_8)\} \cup \left\{\frac{1}{2}(\pm e_1 \pm e_2 \pm \ldots \pm e_7) \pm \frac{1}{2}(e_7 - e_8)\right\} \text{with 3 minus signs before } v_i, i \leq 6\}.$$

The polarization

$$t(e_1) = 11, t(e_2) = 4, t(e_3) = 3, t(e_4) = 2, t(e_5) = 1, t(e_6) = 0, t(e_7) = 4, t(e_8) = 3$$

gives a base consisting of $\{e_2 - e_3, \ldots, e_5 - e_6, e_7 - e_8, \frac{1}{2}(e_1 - e_2 - e_3 - e_4 - e_5 + e_6 - e_7 + e_8)\}$.

$$A_n^\vee \cong A_n, B_n^\vee \cong C_n, D_n^\vee \cong D_n, G_2^\vee \cong G_2, F_4^\vee \cong F_4, E_8^\vee \cong E_8, E_7^\vee \cong E_7, E_6^\vee \cong E_6.$$  

Remark (2.7.3.3). The polarizations $t$ are intimately related to the averaged coroot $\rho^\vee(2.7.3.12)$.

Def. (2.7.3.4) [Dynkin Diagram]. The coxeter graph cannot determine the root system up to isomorphism, because it cannot distinguish between $n(\alpha, \beta)$, $n(\beta, \alpha)$. So there is a Dynkin diagram which is constructed from the coxeter diagram by adding a vector from the longer vector to the shorter vector when $n(\alpha, \beta)n(\beta, \alpha) = 2$ or 3.
Prop. (2.7.3.5) [Listing of Dynkin Diagrams]. The Dynkin diagrams arising from indecomposable root systems are exactly the diagrams $A_n (n \geq 1), B_n (n \geq 2), C_n (n \geq 3), D_n (n \geq 4), E_6, E_7, E_8, F_4, G_2$. (Graphs are given in [Etingof, Lie algebras] P109.)

Proof: This follows easily from (2.7.3.1) and (2.7.3.2). \hfill \Box

Prop. (2.7.3.6) [Non-Reduced Root Systems]. For any $n \geq 1$, there is exactly one non-reduced indecomposable root system of rank $n$, which is $BC_n$, the union of $B_n$ and $C_n$ in (2.7.3.2).

Cor. (2.7.3.7). Cf. [Kna96] P139.

Weight Lattices

Def. (2.7.3.8) [Weight Lattice]. Let $(R, V)$ be a root system, we can define the root lattice as the $\mathbb{Z}$-lattice $Q(R)$ generated by $R$, and also the weight lattice $P(R) = \{ x \in V | \alpha^\vee (x) \in \mathbb{Z}, \forall \alpha \in R \}$ $P(R)$ has a generator by fundamental weights $\omega_i$ that $(\omega_i, \alpha_j^\vee) = \delta_{ij}$. Then $Q(R) \subset P(R)$, and $[P(R) : Q(R)]$ is finite as they are both complete lattices.

Prop. (2.7.3.9). Let $\rho = 1/2 \sum_i \alpha_i$, then $\rho = \sum_i \omega_i$.

Proof: It follows from (2.7.2.10) that $s_\alpha \rho = \rho - \alpha$, so $(\rho, \alpha_i^\vee) = 1$, thus $\rho = \sum_i \omega_i$ by definition (2.7.2.10). \hfill \Box

Prop. (2.7.3.10) [Weight Lattices of Indecomposable Root Systems]. Let $R$ be a root system, notation as in (2.7.3.2),

- $A_n$: $\alpha_i^\vee = \alpha_i$ for $i \leq n$, so $\omega_i = \left(\frac{n+i}{n+1}, \ldots, \frac{n+1}{n+2}, \ldots, \frac{n+1}{n+1}\right)$ $(i \text{ terms})$ for $1 \leq i \leq n$. Then $P = \{ (x_i) \in \mathbb{R}^n | x_i - x_j \in \mathbb{Z} \sum x_i = 0 \}, Q = \{ (x_i) \in \mathbb{Z}^n | \sum x_i = 0, \}$ and $P/Q \cong \mathbb{Z}/(n+1)\mathbb{Z}$.

- $B_n$: $\alpha_i^\vee = \alpha_i$ for $i < n$ and $\omega_n = (\frac{1}{2}, \ldots, \frac{1}{2})$. Then $P = \mathbb{Z}^n$ and $Q = \mathbb{Z}^n \cup \left(\frac{1}{2}, \ldots, \frac{1}{2}\right) + \mathbb{Z}^{n}, P/Q \cong \mathbb{Z}/2\mathbb{Z}$.

- $C_n$: $\alpha_i^\vee = \alpha_i$ for $i < n$ and $\omega_n = (\frac{1}{2}, \ldots, \frac{1}{2})$. Then $P = \{ (x_i) \in \mathbb{Z}^n | \sum x_i = 2 \mathbb{Z} \}$ and $Q = \mathbb{Z}^n, P/Q \cong \mathbb{Z}/2\mathbb{Z}$.

- $D_n$: $\alpha_i^\vee = \alpha_i$ for $i \leq n$, so $\omega_i = (1, \ldots, 1, 0, 0, \ldots, 0) (i\ \text{ones})$ for $1 \leq i \leq n-2$, $\omega_{n-1} = (1, 2, 1, \ldots, 1), \omega_n = (1, 2, 1, \ldots, 1, 2)$. So $P/Q \cong (\mathbb{Z}/2\mathbb{Z})^2$ for even $n$ and $\mathbb{Z}/4\mathbb{Z}$ for $n$ odd.

- $G_2$: It is clear $\omega_1 = \omega + 1, \omega_2 = 2\omega + 1$. Then $P = Q = \mathbb{Z}[\omega]$.

- $F_4$: $\omega_1 = (1, 1, 0, 0), \omega_2 = (2, 1, 1, 0), \omega_3 = (\frac{1}{2}, \frac{1}{2}, \frac{1}{2}, \frac{1}{2}), \omega_4 = (1, 0, 0, 0)$. So $P = Q = \frac{1}{2}\mathbb{Z}^4$.

- $E_8$: $\omega_1 = (1, 1, 0, \ldots, 0), S = Q = \{ (x_1, \ldots, x_8) | x_i \in \mathbb{Z} \text{ or } x_i \in \frac{1}{2} \mathbb{Z}, \sum x_i \in 2\mathbb{Z} \}$.

- $E_7$: $P/Q \cong \mathbb{Z}/2\mathbb{Z}$.

- $E_6$: $\omega_1 = (1, 1, 0, \ldots, 0), P/Q \cong \mathbb{Z}/3\mathbb{Z}$.

Proof: \hfill \Box

Prop. (2.7.3.11) [Maximal Roots]. For $A_n$, the maximal root is $\theta = e_1 - e_{n+1} = \alpha_1 + \ldots + \alpha_n = \omega_1 + \omega_n$. For $C_n$, the maximal root is $\theta = 2e_1 = 2\alpha_1 + \ldots + 2\alpha_{n-1} + \alpha_n = 2w_1$.

But for any other indecomposable root system $R$, the maximal root $\theta$ is a fundamental root:

- $B_n$: $\theta = e_1 + e_2 = \alpha_1 + 2\alpha_2 + \ldots + 2\alpha_{n-1} = \omega_2$.

- $D_n$: $\theta = e_1 + e_2 = \alpha_1 + 2\alpha_2 + \ldots + 2\alpha_{n-2} + \alpha_{n-1} + \alpha_n = \omega_2$. 

• $G_2$: $\theta = 2\omega + 1 = 3\alpha_1 + 2\alpha_2 = \omega_2$.
• $F_4$: $\theta = e_1 + e_2 = 2\alpha_1 + 3\alpha_2 + 4\alpha_3 + 2\alpha_4 = \omega_1$.
• $E_8$: $\theta = e_1 + e_2 = 2\alpha_1 + 3\alpha_2 + 4\alpha_3 + 5\alpha_4 + 6\alpha_5 + 4\epsilon_6 + 3e_7 + 2e_8 = \omega_1$.
• $E_7$: $\theta = e_1 - e_8 = \alpha_1 + 2\alpha_2 + 3\alpha_3 + 4\alpha_4 + 3\alpha_5 + 2\alpha_6 + 2\alpha_7 = \omega_6$.
• $E_6$: $\theta = e_1 - e_8 = \alpha_1 + 2\alpha_2 + 3\alpha_3 + 2\alpha_4 + \alpha_5 + 2\alpha_6 = \omega_4$.

Prop. (2.7.3.12) [$\rho$ and $\rho^\vee$]. $\rho^\vee$ is $\rho$ of the dual system $R^\vee$. Under the identification of $V$ and $V^*$, If $(R, S)$ is simply laced, then $R \cong R^\vee$ via $\alpha \mapsto \alpha^\vee$, so by (2.7.3.10),

- $A_n: \rho_{A_n} = \rho_{A_n}^\vee = (\frac{n}{2}, \frac{n-2}{2}, \ldots, -\frac{n}{2}) = \sum_i \frac{i(n+1-i)}{2} \alpha_i$.
- $B_n: \rho_{B_n} = \rho_{B_n}^\vee = (\frac{2n-1}{2}, \frac{2n-3}{2}, \ldots, \frac{1}{2}) = \sum_i \frac{i(n-i)}{2} \alpha_i$.
- $C_n: \rho_{C_n} = \rho_{C_n}^\vee = (n, n-1, \ldots, 1) = \sum_{i \leq n} \frac{i(2n+1-i)}{2} \alpha_i + \frac{n(n+1)}{4} \alpha_n$.
- $D_n: \rho_{D_n} = \rho_{D_n}^\vee = (n-1, n-2, \ldots, 0) = \sum_{i \leq n-2} \frac{i(2n-1-i)}{2} \alpha_i + \frac{1}{2} \alpha_{n-1} + \frac{n(n-1)}{4} \alpha_n$.
- $G_2: \rho_{G_2} = 3\omega + 2 = 5\alpha + 3\beta, \rho_{G_2}^\vee = \frac{10}{3}\omega + \frac{8}{3} = 6\alpha + \frac{10}{3}\beta$.
- $F_4: \rho_{F_4} = (\frac{11}{2}, \frac{5}{2}, \frac{3}{2}, \frac{1}{2}), \rho_{F_4}^\vee = (8, 3, 2, 1)$.
- $E_6: \rho_{E_6} = \rho_{E_6}^\vee = (23, 6, 5, 4, 3, 2, 1, 0)$.
- $E_7: \rho_{E_7} = \rho_{E_7}^\vee = (18, 7, 6, \ldots, 1) - (\frac{23}{4}, \ldots, \frac{23}{4})$.
- $E_8: \rho_{E_8} = \rho_{E_8}^\vee = (\frac{15}{2}, \frac{1}{2}, -\frac{1}{2}, -\frac{3}{2}, -\frac{5}{2}, -\frac{7}{2}, -\frac{1}{2}, -\frac{1}{2})$.

Def. (2.7.3.13) [Coxeter Numbers]. Let $(R, S)$ be an indecomposable root system, defined the Coxeter root to be $h_R = (\theta, \rho^\vee) + 1 = \text{ht}(\theta) + 1$, and the dual Coxeter number $h_R^\vee = (\rho, (\theta)^\vee) + 1$. Clearly if $(R, S)$ is simply laced, then $R \cong R^\vee$ via $\alpha \mapsto \alpha^\vee$, so if $\theta = \sum m_i \alpha_i$, then $\theta^\vee = \sum m_i \alpha_i^\vee$, so $h_R^\vee = h_R = \sum m_i + 1$.

Prop. (2.7.3.14) [Listing of Coxeter Numbers]. We can determine the Coxeter numbers and dual coxeter numbers of indecomposable root systems:

- $h_{A_n} = h_{A_n}^\vee = n + 1$.
- $h_{B_n} = 2n$, and $\theta^\vee = e_1 + e_2 = \alpha_1^\vee + 2\alpha_2^\vee + \ldots + \alpha_n^\vee$, so $h_{B_n}^\vee = 2n - 1$.
- $h_{C_n} = 2n$, and $\theta^\vee = e_1 = \alpha_1^\vee + \ldots + \alpha_n^\vee$, so $h_{C_n}^\vee = n + 1$.
- $h_{D_n} = h_{D_n}^\vee = 2n - 2$.
- $h_{G_2} = 6$, and $\theta^\vee = \frac{2}{3}(2\omega + 3) = \alpha_1^\vee + 2\alpha_2^\vee$, so $h_{G_2}^\vee = 4$.
- $h_{F_4} = 12$, and $\theta^\vee = e_1 + e_2 = 2\alpha_1^\vee + 3\alpha_2^\vee + 2\alpha_3^\vee + \alpha_4^\vee$, so $h_{F_4}^\vee = 9$.
- $h_{E_6} = h_{E_6}^\vee = 30$.
- $h_{E_7} = h_{E_7}^\vee = 18$.
- $h_{E_8} = h_{E_8}^\vee = 12$.

Minuscule Weights

Def. (2.7.3.15) [Minuscule Weights]. Let $(R, S)$ be a root system, then a dominant weight $\omega$ is called minuscule if $(\omega, \beta^\vee) \leq 1$ for any positive coroot $\beta^\vee$. 
Prop. (2.7.3.16) [Minuscule and Fundamental Weights]. Let $\theta^\vee = \sum m_i \alpha_i^\vee$ the maximal coroot, where $m_i$ are positive integers, and $m_i = (\omega_i, \theta^\vee)$. Then any minuscule weight is fundamental, and a fundamental weight $\omega_i$ is minuscule if $m_i = 1$.

Proof: The definition of minuscule weight requires $m_i \leq 1$, and any other coroot is of the form $\beta^\vee = \sum n_i \alpha_i^\vee$, where $n_i \leq m_i$, so $n_i = (\omega_i, \beta^\vee) \leq 1$. \hfill $\square$

Lemma (2.7.3.17). If $\omega \in Q$ and $|(\omega, \beta^\vee)| \leq 1$ for any coroot $\beta$, then $\omega = 0$.

Proof: If not, choose a counterexample $\omega = \sum m_i \alpha_i$ with $\sum |m_i| > 0$ minimum, then $(\omega, \omega) = \sum m_i (\omega, \alpha_i^\vee) > 0$, so changing $\omega$ to $-\omega$ if necessary, we can assume $m_i > 0$, $(\omega, \alpha_i^\vee) > 0$ for some $i$, so $(\omega, \alpha_i^\vee) = 1$, and $s_i \omega = \omega - \alpha_i$ is another counterexample with smaller $|m_i|$, contradiction. \hfill $\square$

Prop. (2.7.3.18). The following are equivalent for a dominant integral weight $\omega$ of a root system:

- $\omega$ is minuscule (2.7.3.15).
- If $\lambda$ is a dominant integral weight and $\omega - \lambda \in Q^+$, then $\lambda = \omega$.

Proof: Cf. [Etingof, P141]? \hfill $\square$

Prop. (2.7.3.19) [Number of Minuscule Roots]. Every coset in $P/Q$ contains a unique minuscule weight. This gives a bijection between the $P/Q$ and the set of minuscule weights. In particular, the number of minuscule weights equals the determinant of the Cartan matrix.

Proof: For any $a \in P$, let $C = a + Q$ be a coset, let $\omega \in C \cap P^+$ be an element with minimum $(\omega, \rho)$, then for any dominant weight $\lambda < \omega \in C$, $(\omega - \lambda, \rho) \geq 0$, so $\lambda = \omega$. Thus $\omega$ is minuscule (2.7.3.18).

Conversely, if $\omega_1 \neq \omega_2 \in C$ are minuscule, then by (2.7.3.17), there is a positive coroot $\beta^\vee$ that $|(\omega_1 - \omega_2, \beta)| > 2$. But then as $\omega_1, \omega_2$ are both dominant, $|(\omega_1 - \omega_2, \beta)| \leq 1$, contradiction. \hfill $\square$

Cor. (2.7.3.20) [Listing of Minuscule Weights]. By (2.7.3.19) and (2.7.3.2)(2.7.3.10), we can determine minuscule weights for indecomposable root system $(R, S)$,

- $A_n$: $P/Q \cong \mathbb{Z}/(n + 1)\mathbb{Z}$, so it has $n + 1$ minuscule weight, which are all the fundamental weights $\omega_i$ and 0.
- $B_n$: $P/Q \cong \mathbb{Z}/2\mathbb{Z}$, so there is exactly one non-zero minuscule weight, which is $\omega_n = (\frac{1}{2}, \ldots, \frac{1}{2})$, by (2.7.3.18).
- $C_n$: $P/Q \cong \mathbb{Z}/2\mathbb{Z}$, so there is exactly one non-zero minuscule weight, which is $\omega_n = (1, 0, \ldots, 0)$, by (2.7.3.18). The corresponding fundamental representation is the standard representation of $\mathfrak{sp}_{2n}$.
- $D_n$: $|P/Q| = 4$, so there are exactly 3 non-zero minuscule weights, which are $\omega_1, \omega_{n-1}$ and $\omega_n$, with corresponding fundamental representations of dimension $2n, 2^{n-1}, 2^{n-1}$. This is because the maximal coroot $\beta^\vee = \alpha_1^\vee + 2\alpha_2^\vee + \ldots + 2\alpha_{n-2}^\vee + \alpha_{n-1}^\vee + \alpha_n^\vee$.
- $G_2$: $|P/Q| = 1$, so there are no non-zero minuscule weights.
- $F_4$: There are no non-zero minuscule weights.
- $E_8$: There are no non-zero minuscule weights.
- $E_7$: $P/Q \cong \mathbb{Z}/2\mathbb{Z}$, so there is exactly one non-zero minuscule weight.
- $E_6$: $P/Q \cong \mathbb{Z}/3\mathbb{Z}$, so there are exactly two non-zero minuscule weights.
Prop. (2.7.3.21) \([w_0]\). Notice \(-w_0\) is an automorphism of \((R, S)\) that permutes fundamental weights and simple roots, so it induces an automorphism of the Dynkin diagram of \(R\). So if the Dynkin diagram of \(g\) has no non-trivial automorphism, \(w_0 = -1\). This is case for \(R = A_1, B_n, C_n, G_2, F_4, E_7\) and \(E_8\).

For \(D_n\), if \(n\) is even, then \(-1 \in W\) so \(w_0 = -1\). If \(n\) is odd, then \(w_0(e_i) = -e_i\) for \(i < n\) and \(w_0(e_n) = e_n\).

Notice also each \(s_i\) acts trivially on \(P / Q\), so \(-w_0\) acts by \(-1\) on \(P / Q\). For \(A_n, n \geq 2\), \(P / Q \cong \mathbb{Z} / (n + 1)\mathbb{Z}\), thus \(-w_0\) is the flip of the chain. Likewise for \(E_6\), \(P / Q \cong \mathbb{Z} / 3\mathbb{Z}\), thus \(-w_0\) flips the two minuscule weights. But for \(D_n\), \(P / Q \cong \mathbb{Z} / 2\mathbb{Z} \times \mathbb{Z} / 2\mathbb{Z}\) for \(n\) even and \(P / Q \cong \mathbb{Z} / 4\mathbb{Z}\) for \(n\) odd, so \(-w_0\) preserves the minuscule weights or flip \(w_{n-1}\) and \(w_n\).

4 Notations for a Root System

Def. (2.7.4.1) [Notations for a Root System]. Let \((R, S)\) be a root system, then

- \(R^+ / R^-\) is the positive/negative roots w.r.t. \(S\).
- \(S = \{\alpha_1, \ldots, \alpha_r\}\).
- \(s_i\) is the reflection w.r.t. \(\alpha_i\).
- \(\theta\) is the maximal root.
- \(\theta^\vee\) is the maximal coroot (maximal root of the dual root system). (It may not be dual to \(\theta\))
- \(\rho = \frac{1}{2} \sum_i \alpha_i = \sum \omega_i\).
- \(\rho^\vee\) is \(\rho\) of the dual system \(R^\vee\).
- The height of weights is defined as in (2.7.2.17).
- \(W\) is the Weyl group.
- \(w_0 \in W\) is the unique element with length \(|R^+|\) (2.7.2.14).
- \(n_{ij}\) is the Cartan number \(n(\alpha_i, \alpha_j)\).
- \(Q(R)\) is the root lattice (2.7.3.8).
- \(P(R)\) is the weight lattice, generated by the fundamental weights \(\omega_i\) (2.7.3.8).
- \(P^+(R)\) is the dominant integral weights.
- \(\mathcal{P}\) is the Kostant partition function on \(Q(R)\).
2.8 Algebraic K-Theory

Main references are [Algebraic K-Theory of Fields, Suslin, in Proc. ICM 1986, P222-244] and [G-S17].

1 Milnor K-Groups of Fields

Def.(2.8.1.1) $[K_0]$. The Grothendieck group $K_0(A)$ for a ring $A$ is the free group generated by f.g. projective module over $A$ modulo exact sequences. Then we have $P \sim Q$ iff $P \oplus A^n \cong Q \oplus A^n$ for some $n$. This is a functor $\mathcal{C}_{\text{Alg}} \to \mathcal{A}_{\text{Ab}}$.

Def.(2.8.1.2) [Milnor K-Groups]. For $k \in \text{Field}$, define the $n$-th Milnor K-group to be the groups

\[ K_0^{\text{Mil}}(k) = \mathbb{Z}, \quad K_1^{\text{Mil}}(k) = k^\times, \quad K_n^{\text{Mil}}(k) = (k^\times)^{\otimes n}/\{a_1 \otimes \ldots \otimes a_n \mid \exists 1 \leq i < j \leq n, a_i + a_j = 1\}, n \geq 2 \]

The elements in $K_n^{\text{Mil}}(k)$ are called symbols, and the class of $a_1 \otimes \ldots \otimes a_m$ is denoted by $\{a_1, \ldots, a_n\}$.

Prop.(2.8.1.3) [Total Milnor K-Groups]. For $m, n \in \mathbb{N}$, the tensor product $(k^\times)^{\otimes m} \times (k^\times)^{\otimes n} \to (k^\times)^{\otimes (m+n)}$ induces a surjective map

\[ K_m^{\text{Mil}}(k) \otimes K_m^{\text{Mil}}(k) \to K_{m+n}^{\text{Mil}}(k), \]

which induces a graded group structure on

\[ K_*^{\text{Mil}}(k) = \bigoplus_{n \in \mathbb{N}} K_n^{\text{Mil}}(k). \]

Then $K_*^{\text{Mil}}(k)$ is graded commutative.

Proof: Firstly we show that $\{x, -x\} = 0$: Because

\[ \{x, -x\} + \{x, -(1 - x)x^{-1}\} = \{x, 1 - x\} = 0, \]

Thus

\[ \{x, -x\} = -\{x, 1 - x^{-1}\} = \{x^{-1}, 1 - x^{-1}\} = 0. \]

Then the general case follows by induction. □

Prop.(2.8.1.4) [Finite Fields]. If $k \in \text{Field}$, $\# k < \infty$, for any $n \geq 2$, $K_n^{\text{Mil}}(k) = 0$.

Proof: By(2.8.1.3), it suffices to show that $K_2^{\text{Mil}}(k) = 0$. And if $\omega$ is a generator of the cyclic group $k^\times$, then it suffices to show that $\{\omega, \omega\} = \{\omega, -1\} = 0$. If $\# k = 2^m$, then

\[ 0 = \{1, \omega\} = \{\omega^{2^m-1}, \omega\} = (2^m - 1)\{\omega, \omega\}, \]

thus we are done. And if char $k \neq 2$, then we can find two non-squares in $k^\times$ s.t. $a + b = 1$. Then

\[ 0 = \{a, b\} = \{\omega^i, \omega^k\} = kl\{\omega, \omega\}, \]

so $\{\omega, \omega\} = 0$. □
Def. (2.8.1.5) [Residue Maps and Specialization Maps]. Let \((R, K, k)\) be a DVR, then for any \(n \in \mathbb{Z}_+\), there exists a unique homomorphism
\[ \partial^\text{Mil}_n : K_n^\text{Mil}(K) \to K_{n-1}^\text{Mil}(k) \]

s.t. for any uniformizer \(\varpi\) and units \(u_1, \ldots, u_{n-1} \in R^*\),
\[ \partial^\text{Mil}_n(\{\varpi, u_1, \ldots, u_{n-1}\}) = \{\overline{u}_1, \ldots, \overline{u}_{n-1}\}. \]

Moreover, for any uniformizer \(\varpi\) and \(n \in \mathbb{Z}_+\), there exists a specialization map
\[ s^\text{Mil}_{\varpi} : K_n^\text{Mil}(K) \to K_n^\text{Mil}(k) \]

s.t.
\[ s^\text{Mil}_{\varpi}(\{\varpi^1 u_1, \ldots, \varpi^n u_n\}) = \{\overline{u}_1, \ldots, \overline{u}_n\} \]

for any \(u_1, \ldots, u_n \in R^*\).


Cor. (2.8.1.6). \(\partial^\text{Mil}_n(\{a, b\}) = (-1)^{v(a)v(b)}a^{-v(b)}b^{v(a)}\).

Proof:

Thm. (2.8.1.7) [Berrick-Keating]. Let \(R, S \in \text{Ring} \) and \(U \in \text{Mod}_{R,S}\), let \(T = \begin{bmatrix} R & U \\ S & \end{bmatrix} \in \text{Ring}\), then the map
\[ \pi_i : K_i(T) \to K_i(T) \oplus K_i(S) \]

is an isomorphism for any \(i \in \mathbb{Z}\).


Prop. (2.8.1.8) [Matsumoto]. For \(k \in \text{Field}\), \(K_2^\text{Mil}(k) \cong K_2(k)\).

Proof:

2 Bloch-Kato Conjecture

Lemma (2.8.2.1) [Hilbert’s Theorem90 for \(K_2\)]. Let \(K/k\) be a cyclic Galois field extension with a generator \(\sigma \in \text{Gal}(K/k)\), then the complex
\[ K_2^\text{Mil}(K) \xrightarrow{\sigma^{-1}} K_2^\text{Mil}(K) \xrightarrow{\text{Nm}_{K/k}} K_2^\text{Mil}(k) \]

is exact.

Prop. (2.8.2.2) [Galois Symbols]. Let \( k \in \text{Field}, m \in \mathbb{Z} \cap k^\times, n \in \mathbb{Z}_+ \), the boundary map
\[
\partial k^\times \to H^1(k, \mu_m)
\]
induces a map
\[
\partial^n : (k^\times)^{\otimes n} \to (H^1(k, \mu_m))^{\otimes n} \cup H^n(k, \mu_m^{\otimes n}),
\]
and this map factors through \( K_n^{\text{Mil}}(k) \) and gives a Galois symbol map
\[
h_{k,m}^n : K_n^{\text{Mil}}(k) \to H^n(k, \mu_m^{\otimes n}).
\]

**Proof:** To show this map factors through \( K_n^{\text{Mil}}(k) \), it suffices to show for \( n = 2 \) and \( \partial^2(a \otimes (1-a)) = 0 \). Take an irreducible factorization
\[
x^m - a = \prod_l f_l \in k[x],
\]
and let \( \alpha_l \) be a root of \( f_l \) in \( k_{\text{sep}}, K_l = k(\alpha_l) \), then
\[
(1 - a) = \prod_l \text{Nm}_{K_l/k}(1 - \alpha_l).
\]
and
\[
\partial^2(a \otimes (1-a)) = \sum_l \partial^2(a \otimes \text{Nm}_{K_l/k}(1 - \alpha_l)).
\]
But
\[
\partial^2(a \otimes \text{Nm}_{K_l/k}(1 - \alpha_l)) = \partial(a) \cup \partial(\text{Nm}_{K_l/k}(1 - \alpha_l)) = \partial(a) \cup \text{cor}^K_{\alpha_l} \text{res}^K_{K_l}(a) \cup (1 - \alpha_l) = \text{cor}(\text{res}^K_{K_l}(a) \cup (1 - \alpha_l))
\]
But by definition \( a \in (K_l^\times)^m \), so \( \partial_{K_l}(a) = 0 \), by (10.1.3.9). Thus \( \partial^2(a \otimes (1-a)) = 0 \). \( \square \)

Thm. (2.8.2.3) [Bloch-Kato Conjecture, Voevodsky-Rost/Merkurjev-Suslin]. Situation as in (2.8.2.2), the Galois symbol (2.8.2.2) induces an isomorphism
\[
K_n^{\text{Mil}}(k)/mK_n^{\text{Mil}}(k) \xrightarrow{\cong} H^n(k, \mu_m^{\otimes n}).
\]

**Proof:** The \( n = 1 \) case follows from (10.1.3.9).
For the \( n = 2 \) case? \( \square \)


## 2.9 Hopf Algebras

Main references are [Quantum Groups, Drinfeld], [A Brief Introduction To Quantum Groups Pavel Etingof And Mykola Semenyakin].

### 1 Hopf Algebras

#### Coalgebras and Bialgebras

**Def.(2.9.1.1) [Coalgebras].** Let $R$ be a commutative ring, a **coalgebra** is a monoid object in the category $\text{Mod}^R_R$.

**Remark(2.9.1.2) [Yoneda Interpretation].** We do not need to verify all the relations defining a coalgebra $C$, whenever we have a functorial monoidal structure on all the set $\text{Hom}_R(H,T)$, we immediately recover the maps

- (Comultiplication): $\mu : C \to C \otimes_R C$ as $i_1 \cdot i_2$ in $\text{Hom}_R(C,C \otimes C)$,
- (Counit): $\varepsilon : C \to R$ as $1$ in $\text{Hom}_R(C,R) = C^\vee$.

by Yoneda lemma.

$C^\vee$ is an monoid by definition, and $C$ is called **cocommutative** iff $C^\vee$ is commutative.

**Def.(2.9.1.3) [Primitive Elements].** Let $H$ be a coalgebra over $R$, an element $x \in H$ is called **primitive** if $\mu(x) = 1 \otimes x + x \otimes 1$. It is called **group-like** if $\Delta(x) = x \otimes x$.

**Def.(2.9.1.4) [Bialgebras].** Let $R$ be a commutative ring, a **bialgebra** is a monoid object in the category of coalgebras over $R$. Equivalently, in the Yoneda interpretation, $C$ is an $R$-algebra that $\Delta$ is a homomorphism of algebras.

**Def.(2.9.1.5) [Hopf Algebra].** A **Hopf algebra** over a commutative algebra $R$ is a bialgebra $A$ together with a $R$-linear map $S : A \to A$ that satisfies:

$$m \circ (\text{id} \otimes S) \circ \mu = m \circ (S \otimes \text{id}) \circ \mu = \eta \circ \varepsilon : A \to A.$$ 

If $S^2 = \text{id}_A$, then $A$ is called an **involutive Hopf algebra**.

**Prop.(2.9.1.6).** In a Hopf algebra, $S$ is an anti-homomorphism both for the algebra structure and coalgebra structure.


**Example(2.9.1.7) [Group Algebras].** Let $\Gamma$ be a group, the group algebra $R[\Gamma]$ with the coalgebra structure

$$\mu : R[\Gamma] \to R[\Gamma] \times R[\Gamma] : g \mapsto g \otimes g, \varepsilon : R[\Gamma] \rightarrow R : \sum a_g g \mapsto \sum a_g$$

and

$$S : R[\Gamma] \to R[\Gamma] : g \mapsto g$$

is a Hopf algebra.

**Def.(2.9.1.8) [Dual Hoof Algebra].** Let $H$ be a Hopf algebra, matrix coefficients. $H^0$.

**Prop.(2.9.1.9).** $\text{Rep}(H) = \text{Mod}_{H^0}$. 


Co-modules

**Def. (2.9.1.10) [Co-Module].** Let $A$ be a coalgebra over a field $k$, then a right **co-module** is a $k$-vector space $V$ together with a $k$-linear map $\rho : V \to V \otimes A$ that satisfies

$$(\text{id}_V \otimes \mu) \circ \rho = (\rho \otimes \text{id}_A) \circ \rho, \quad (\text{id}_V \otimes \varepsilon) \circ \rho = \text{id}_V.$$

The map $\rho$ is called the **co-action**, and a $k$-subspace $W \subset V$ that $\rho(W) \subset W \otimes A$ is called a **sub-comodule** of $V$.

**Def. (2.9.1.11) [Tensor Product of Co-modules].**

Topologists’ Hopf Algebras

**Def. (2.9.1.12) [Topologist’s Hopf Algebra].** A **topologist’s Hopf algebra** over a commutative ring $R$ is a unital magma object in the dual category of graded algebras with $0$-degree term $R$, given by maps $\Delta : A \to A \otimes A$, and $\varepsilon : A \to R$ the canonical projection map. So in particular, $\Delta$ is of the form

$$\Delta(\alpha) = 1 \otimes \alpha + \alpha \otimes 1 + \sum_i \alpha'_i \otimes \alpha''_i, |\alpha'_i| > 0, |\alpha''_i| > 0.$$

**Prop. (2.9.1.13).** The tensor product of two topologists’ Hopf algebra is a topologists’ Hopf algebra.

**Prop. (2.9.1.14).** Let $F$ be a field, then $F[\alpha]/(\alpha^n)$, where $\alpha$ is placed at even dimension or $F$ has characteristic $2$, is a topologists’ Hopf algebra iff $F$ has positive characteristic $p$ and $n$ is a power of $p$.

**Proof:** By definition, it is easy to see that $\alpha$ is primitive, thus

$$\Delta(\alpha^n) = 0 = \sum_{0 < i < n} \binom{n}{i} \alpha^i.$$

Which then implies that $n$ is a $p$-power. □

**Prop. (2.9.1.15) [Hopf-Borel].** Let $A$ be a topologists’ Hopf algebra over a perfect field $K$, and $A$ is of f.d. in each degree, then:

- If $K$ has characteristic $0$, $A$ is isomorphic as an algebra to the tensor product of an exterior product of odd-dimensional generators and a polynomial ring of even-dimensional generators.
- If $K$ has characteristic $p$, then $A$ is isomorphic as an algebra to the tensor product of algebras of the following types:
  - $K[\alpha]$, where $\alpha$ is even-dimensional if $p \neq 2$.
  - $\wedge K[\alpha]$ where $\alpha$ is odd-dimensional.
  - $K[\alpha]/(\alpha^{p^i})$, where $\alpha$ is even-dimensional if $p \neq 2$.

**Proof:** We only prove the 0-characteristic case, Cf. [Hat02]P285. □
2 Commutative Hopf Algebras

Prop. (2.9.2.1) [Commutative Hopf Algebra]. Let $R$ be a commutative ring, a commutative Hopf algebra is equivalent to a cogroup object in $\mathcal{C}\text{Alg}_R$. A homomorphism of Hopf algebras is a morphism of algebras that represents a natural transformation of functors from $\mathcal{C}\text{Alg}_R$ to $\mathcal{S}\text{rp}$.

*Proof:* The critical point is to look at the definition of Hopf algebra. In this case, $S$ is a homomorphism of algebras (2.9.1.6), and notice tensor product is just the product in the dual category, and $m : A \otimes A \to A$ is the diagonal in the dual category, thus a cogroup object is a map $\Delta : A \to A \otimes A$ together with a map $\text{inv} : A \to A$ that

$$m \circ (\text{id} \otimes \text{inv}) \circ \Delta = m \circ (\text{inv} \otimes \text{id}) \circ \Delta = \text{id} : A \to A,$$

which is exactly the definition of the Hopf algebra (2.9.1.5).

Cor. (2.9.2.2) [Yoneda Interpretation]. We do not need to verify all the relations defining a Hopf algebra $H$, whenever we have a functorial commutative group structure on all the set $\text{Hom}(H,T)$, we immediately recover the maps:

- (Comultiplication): $\mu : H \to H \otimes R H$ as $i_1 \cdot i_2$ in $\text{Hom}(H,H \otimes H)$,
- (Antipode): $\iota : H \to H$ as inv in $\text{Hom}(H,H)$,
- (Counit): $\varepsilon : H \to R$ as 1 in $\text{Hom}(H,R) = H^\vee$.

by Yoneda lemma.

For convenience, we denote the structure maps $\eta_H : R \to H, \mu : H \times R H \to H, (-)^{-1} : H \to H$.

Prop. (2.9.2.3) [Group Algebras]. Let $\Gamma$ be a commutative group, then the group algebra $R[\Gamma]$ (2.9.1.7) represents the group functor that maps a commutative $R$-algebra $S$ to the commutative group $\text{Hom}(\text{grp} (\Gamma), S)$.

Cor. (2.9.2.4) [Multiplicative Groups]. $G_{m,R} = R[t,t^{-1}]$ is a Hopf algebra that represents the group functor of multiplicative groups on $\mathcal{C}\text{Alg}_R$.

Cor. (2.9.2.5) [Roots of Unity $\mu_{n,R}$]. Let $\Gamma \cong \mathbb{Z}/n\mathbb{Z}$, then $R[\Gamma] \cong R[t]/(t^n - 1)$ is a Hopf algebra that represents the group functor of multiplicative groups of $n$-th roots of unity on $\mathcal{C}\text{Alg}_R$.

Prop. (2.9.2.6) [Additive Groups]. $R[t]$ can be given a Hopf algebra structure that represents the group functor that maps a commutative $R$-algebra $S$ to the additive group $S^+$.

Def. (2.9.2.7) [$G_{(a,b),R}$]. Given elements $a, b \in R$ that $ab = 2$, for any commutative $R$-algebra $S$, the group $G_{(a,b),R}(S)$ of elements $x$ of $S$ that $x^2 + ax = 0$ is a group under the mapping $(m, n) \mapsto m + n + bmn$. Notice the inverse of $m$ is $m$ itself. Then $R[t]/(t^2 + at)$ can be given a Hopf algebra that represents the functor $S \mapsto G_{(a,b),R}(S)$.

Def. (2.9.2.8) [$V_\alpha$]. Let $V$ be a vector space over $k$, then $\text{Sym}(V^\vee)$ can be given a Hopf algebra structure representation the functor $V_\alpha : R \mapsto R \otimes_k V \cong \text{Hom}_k(V^\vee, R)$.

Def. (2.9.2.9) [Locally Constant Functions]. Let $\Gamma$ be a group, then $\Gamma_R = \prod_{\gamma \in \Gamma} R$ represents the group functor that maps an $R$-algebra $T$ to the group of locally constant functions on $\text{Spec} R$ with value in $\Gamma$. 
Remark (2.9.2.10). To illustrate the philosophy of (7.1.1.2), we figure out the Hopf structure of the local constant functions: a map \( \prod_{\gamma \in E} R \to T \) is equivalent to a set of idempotents \( e_\gamma \) of \( T \) that \( \sum e_\gamma = 1 \). This is equivalent to a locally constant function on \( \text{Spec} \, T \) that takes value \( \gamma \) on \( V(e_\gamma) \). Then the product takes values \( \gamma \delta \) on \( V(e_\gamma \otimes e_\delta) \subset \text{Spec} \, T \otimes T \), or equivalently takes values \( \gamma \) on \( V(\sum_{gg' = \gamma} e_g \otimes e_{g'}) \), so \( \Delta(e_\gamma) = \sum_{gg' = \gamma} e_g \otimes e_{g'} \).

Lemma (2.9.2.11) [Modulo \( \ker(\varepsilon) \)]. For a Hopf algebra \( A \) over \( R \), the comultiplication and counit are determined by \( \ker \varepsilon \):

- \( R \oplus \ker \varepsilon \to A : (a,b) \mapsto a + b \) is an isomorphism of \( R \)-modules.
- \( \mu(a) \equiv -\varepsilon(a) + a \otimes 1 + 1 \otimes a \mod \ker \varepsilon \otimes R \ker \varepsilon \).
- \( \iota(a) \equiv -a \mod (\ker \varepsilon)^2 \) for \( a \in \ker \varepsilon \).

Proof: 1: this is because the counit \( 0 \to \ker \varepsilon \to A \to R \to 0 \) has an inverse by the \( R \)-algebra map \( R \to S \).

2: item 1 allows us to write

\[ A \otimes_R A = R \oplus (\ker \varepsilon \otimes_R R) \oplus (R \otimes_R \ker \varepsilon) \oplus (\ker \varepsilon \otimes \ker \varepsilon) \]

so for \( a \in A \),

\[ \mu(a) = b + c \otimes 1 + 1 \otimes d + z \]

where \( b, c, d \in \ker \varepsilon, z \in \ker \varepsilon \otimes \ker \varepsilon \). Then \( a = (\varepsilon \otimes \text{id}_A)(b + c \otimes 1 + 1 \otimes d + z) = b + d \), and also \( a = b + c \). Applying \( \varepsilon \) shows \( b = \varepsilon(a) \), and thus

\[ \mu(a) = \varepsilon(a) + (a - \varepsilon(a)) \otimes 1 + 1 \otimes (a - \varepsilon(a)) + z = -\varepsilon(a) + a \otimes 1 + 1 \otimes a + z. \]

3: Let \( \iota(a) = b + c \) where \( b, c \in \ker \varepsilon \), then

\[ \varepsilon(a) = (\text{multi})(\iota \otimes \text{id})(-\varepsilon(a) + a \otimes 1 + 1 \otimes a + z) = -\varepsilon(a) + \iota(a) + a + (\text{multi})(\iota \otimes \text{id})(z) \]

so for \( a \in \ker \varepsilon \), \( \iota(a) \equiv -a \mod (\ker \varepsilon)^2 \), as \( (\text{multi})(\iota \otimes \text{id})(z) \in (\ker \varepsilon)^2 \), because \( \iota \) commutes with \( \varepsilon \).

Def. (2.9.2.12) [Hopf Ideal and Quotient Hopf Algebra]. Let \( A \) be a Hopf algebra, then a quotient Hopf algebra is a quotient \( A/I \) that has a Hopf algebra structure compatible with that of \( A \). In other words, there are commutative diagrams

\[
\begin{align*}
A \xrightarrow{\mu} A \otimes_R A & \quad \xrightarrow{\varepsilon} R \quad \xrightarrow{\iota} A \\
A/I & \xrightarrow{\text{proj}} A/I \otimes_R A/I & \xrightarrow{\text{restr}} A/I \\
\end{align*}
\]

In particular, quotient Hopf algebra corresponds to ideals of \( A \) that

\[ \mu(I) \subset \ker(A \otimes_R A \to A/I \otimes_R A/I), \quad \varepsilon(I) = 0, \quad \iota(I) \subset I, \]

called Hopf ideals of \( A \).

Remark (2.9.2.13) [Examples]. If \( \Gamma' \) is a subgroup of a commutative group \( \Gamma \), then \( R[\Gamma] \) has a quotient Hopf algebra \( R[\Gamma/\Gamma'] \). In particular, \( R[t]/(t^n - 1) \) is a quotient Hopf algebra of \( R[t,t^{-1}] \).
Prop. (2.9.2.14) [Hopf Ideals of Additive Groups]. Let \( f = \sum_{i=0}^{d} a_i t^i \in R[t] \) be a monic polynomial \( \neq t \), then \( (f) \) is a Hopf ideal of \( R[t] \) iff \( R \) is of char \( p > 0 \) and the derivative \( f' = 0 \).

**Proof:** We check conditions in (2.9.2.12), the first says \( \sum a_i (t \otimes 1 + 1 \otimes t)^i \) vanishes in \( R[t]/(f) \otimes_R R[t] \). But \( f \) is monic, so this is equivalent to \( a_i \binom{i}{j} = 0 \) for any \( 0 < j < i \leq d \). But we have \( \gcd_{0<j<i}(i) = p \) if \( i = p^r \) for some \( r \geq 1 \) and 1 otherwise, so \( a_d = 0 \) unless \( d \) is a power of \( p \), and \( p = 0 \in R \) because \( a_d = 1 \). In particular, \( f = \sum_{i=0}^{d} b_i t^{p^i} \), and it automatically satisfies the other two conditions. \( \square \)

Cor. (2.9.2.15) \([\alpha_{p', R}]\). Let \( R \) be a commutative ring of char \( p > 0 \), then the quotient Hopf algebra \( R[t]/(t^{p'}) \) corresponding to the Hopf ideal \( (t^{p'}) \) is denoted by \( \alpha_{p', R} \).

**WARNING:** \( \alpha_{p', R} \) is isomorphic to \( \mu_{p', R} \) as \( R \)-algebras, but they are not isomorphic as Hopf algebras.

Prop. (2.9.2.16) [Irreducibility of Hopf Algebras]. Let \( k \) be a field, then the following Hopf algebra contains no proper Hopf ideals:

- \( G_{a, k} \) if char \( R = 0 \).
- \( \alpha_{p, k} \) if char \( R = p > 0 \).

**Proof:** Any Hopf ideal to \( k[t] \) is principal, thus this proposition follows from (2.9.2.14). \( \square \)

Def. (2.9.2.17) [Cokernel Hopf Algebra]. Let \( A \to B \) be a homomorphism of Hopf Algebras over \( R \), then the **cokernel Hopf algebra** is the algebra \( B \otimes_A R = B/B \otimes_A \ker(\varepsilon_A) \), which represents the functor of kernels of \( \text{Hom}_R(B, T) \to \text{Hom}_R(A, T) \), thus is a Hopf algebra.

Lemma (2.9.2.18). A Hopf algebra over a field \( k \) is direct limit of Hopf algebra of f.t. over \( k \).

Def. (2.9.2.19) [Group-Like Elements]. Let \( A \) be a Hopf algebra, then a **group-like element** \( a \in A \) is an invertible element that satisfies \( \mu(a) = a \otimes a \in A \otimes A \).

If \( a \) is a group-like element in a Hopf algebra \( A \), then \( a = (\varepsilon, \text{id})\mu(a) = \varepsilon(a)a \), so \( \varepsilon(a) = 1 \).

Prop. (2.9.2.20) [Group-Like Elements are Linearly Independent]. Let \( A \) be a Hopf algebra over a field \( k \), then the set of group-like elements are linearly independent over \( k \).

**Proof:** If \( e = \sum a_i e_i \) that \( e, e_i \) are all group-like elements, then

\[
\mu(e) = e \otimes e = \sum c_i c_j e_i \otimes e_j = \sum c_i \mu(e_i) = \sum c_i e_i \otimes e_i
\]

so \( c_i^2 = c_i \) and \( c_i e_j = 0 \). Now also notice \( 1 = \varepsilon(e) = \sum c_i \varepsilon(e_i) = \sum c_i (2.9.2.19) \), contradiction. \( \square \)

Cor. (2.9.2.21). The set of group-like elements in the Hopf algebra \( k[\Gamma](2.9.2.3) \) are just the set \( \Gamma \subset k[\Gamma] \).

Prop. (2.9.2.22) [Cartier Theorem]. A Hopf algebra \( A \) over a field \( k \) of characteristic 0 is reduced.

**Proof:** We can base change to the algebraic closure \( \overline{k} \) of \( k \) and assume \( k \) is alg. closed. Because reducedness is stalkwise and Hilbert’s Nullstellensatz, it suffices to show \( A_s \) is reduced at each \( s \in G(k) \). The translation by \( g \in G(k) \) acts transitively on \( G(k) \), so it suffices to show it vanishes at the kernel of the counit map \( \ker(\varepsilon) \). Cf. [Jakob, Stix].

We may assume by taking direct limits that \( A \) is f.g. over \( k \). Let \( \mathfrak{m} \) be the kernel of the counit \( \varepsilon : A \to k \), then \( \mathfrak{m}/\mathfrak{m}^2 \) is a f.g. \( k \)-vector space with a basis lifting to \( x_1, \ldots, x_r \in \mathfrak{m} \).

We prove that \( \text{gr}_\mathfrak{m}(A) \) is a polynomial ring in \( x_i \), Cf. [Shatz]. \( \square \)
Prop. (2.9.2.23) [Faithfully Flatness]. If $A \subset B$ are f.g. Hopf algebras over a field $k$, then $B$ is f.f. over $A$.

Proof: Cf. [Milne, P73]. □

Cor. (2.9.2.24). If $A \subset B$ are Hopf algebras that $B$ is an integral domain, and let $K, L$ be their fraction field, then $B \cap L = A$. In particular, if $K = L$, then $A = B$.

Proof: Since $A \to B$ is f.f. by (2.9.2.23), $cB \cap A = cA$ for any $c \in A$ by (2.9.2.23). Thus if $a/c \in B$ for $a, c \in A$, then $a \in cB \cap A = cA$, so $a/c \in A$. □

3 Quiver Hecke Algebra

Cf. [Bru13].
3 Categories and Algebraic Topology

3.1 Categories

Main references are [?], [Coend Calculus, Fosco Loregian].

1 Basics

Def.(3.1.1.1)[Category]. A category $\mathcal{C}$ consists of the following data:

- A set $\text{Ob}(\mathcal{C})$ of objects of $\mathcal{C}$.
- For any $x, y \in \text{Ob}(\mathcal{C})$ a set $\text{Mor}(x, y)$ of morphisms from $x$ to $y$.
- For any $(x, y, z) \in \text{Ob}(\mathcal{C})$, a map of sets $\circ : \text{Mor}(y, z) \times \text{Mor}(x, y) \to \text{Mor}(x, z)$, called the composition law of $\mathcal{C}$.

that satisfies:
- (Identity) For any $x \in \text{Ob}(\mathcal{C})$, there exists an element $\text{id}_x \in \text{Mor}(x, x)$ s.t. $\text{id}_x \circ \varphi = \varphi$, $\psi \circ \text{id}_x = \psi$ whenever these compositions make sense. It is clear such an element is unique.
- (Associativity) $(\varphi \circ \psi) \circ \chi = \varphi \circ (\psi \circ \chi)$ whenever these compositions make sense.

Remark(3.1.1.2). Let $\mathcal{C}$ be a category, we will sometimes say $x \in \mathcal{C}$ to mean that $x$ is an element of $\text{Ob}(\mathcal{C})$ and $f : x \to y \in \mathcal{C}$ or $f$ is a morphism in $\mathcal{C}$ to mean: $x, y \in \text{Ob}(\mathcal{C})$ and $f \in \text{Mor}(x, y)$. Hopefully this won’t make any confusions.

Def.(3.1.1.3)[Dual Categories]. Let $\mathcal{C}$ be a category, then the dual category of $\mathcal{C}$ is a category $\mathcal{C}^{\text{op}}$ with

- $\text{Ob}(\mathcal{C}^{\text{op}}) = \text{Ob}(\mathcal{C})$.
- For $x, y \in \text{Ob}(\mathcal{C}^{\text{op}}) = \text{Ob}(\mathcal{C})$, $\text{Mor}_{\mathcal{C}^{\text{op}}}(x, y) = \text{Mor}_{\mathcal{C}}(y, x)$.
- The composition law of $\mathcal{C}^{\text{op}}$ is induced from that of $\mathcal{C}$.

Def.(3.1.1.4)[Isomorphisms]. Let $\mathcal{C}$ be a category, an isomorphism in $\mathcal{C}$ is a morphism $\varphi \in \text{Mor}(x, y)$ in $\mathcal{C}$ s.t. there exists a morphism $\psi \in \text{Mor}(y, x)$ s.t. $\varphi \circ \psi = \text{id}_y$ and $\psi \circ \varphi = \text{id}_x$. It is clear that such a $\psi$ is unique, and if it exists, it is called the inverse morphism of $\varphi$.

For $x, y \in \mathcal{C}$, if there exists an isomorphism in $\text{Mor}(x, y)$, $x, y$ are said to be equivalent objects.

Def.(3.1.1.5)[Functors]. Let $\mathcal{C}, \mathcal{C}'$ be categories, a functor $F$ from $\mathcal{C} \to \mathcal{C}'$ consists of the following data:

- a morphism of sets $\text{Ob}(\mathcal{C}) \to \text{Ob}(\mathcal{C}') : x \mapsto F(x)$.
- for any $x, y \in \text{Ob}(\mathcal{C})$, a morphism of sets $\text{Mor}(x, y) \to \text{Mor}(F(x), F(y)) : f \mapsto F(f)$.

that satisfies:
• $F(\text{id}_x) = \text{id}_{F(x)}$.

• $F(\varphi \circ \psi) = F(\varphi) \circ F(\psi)$ whenever $\varphi \circ \psi$ is defined.

A **contravariant functor** from $\mathcal{C}$ to $\mathcal{C}'$ is defined to be a functor from $\mathcal{C}^{\text{op}}$ to $\mathcal{C}'$.

**Def. (3.1.1.6)** [$\text{id}_\mathcal{C}$]. For any category $\mathcal{C}$, there exists a trivial functor $\text{id}_\mathcal{C} : \mathcal{C} \to \mathcal{C}$.

**Def. (3.1.1.7)** [Natural Transformations]. Let $\mathcal{C}, \mathcal{C}'$ be categories and $F, G : \mathcal{C} \to \mathcal{C}'$ be functors between categories, then a **natural transformation** $\eta$ from $F$ to $G$ consists of an element $\eta_x$ for each $x \in \text{Ob}(\mathcal{C})$ s.t. for any $f : x \to y \in \mathcal{C}$, the following diagram is commutative:

$$
\begin{array}{ccc}
F(x) & \xrightarrow{F(f)} & F(y) \\
\downarrow{\eta_x} & & \downarrow{\eta_y} \\
G(x) & \xrightarrow{G(f)} & G(y)
\end{array}
$$

Then for any two categories $\mathcal{C}, \mathcal{C}'$, there is a category $\text{Fun}(\mathcal{C}, \mathcal{C}')$ consisting of the set of functors from $\mathcal{C}$ to $\mathcal{C}'$, and natural transformations as morphisms between functors.

**Def. (3.1.1.8)** [Initial Objects]. An **initial object** in a category $\mathcal{C}$ is an object $\varnothing$ s.t. for any $X \in \mathcal{C}$, there exists a unique morphism $\varnothing \to X$. A **final object** is an initial object in $\mathcal{C}^{\text{op}}$. Initial and final objects are unique up to unique isomorphisms.

An object that is both initial and final is called a **zero object**.

**Def. (3.1.1.9)** [Filtered Categories]. A **filtered category** is a category $\mathcal{I}$ that:

- It is nonempty.

- for any $a, b \in \mathcal{I}$, there is some $c \in \mathcal{I}$ with morphisms $a \to c, b \to c$

- for any two morphisms $a, b : x \to y$, there is a morphism $c : y \to z$ that $c \circ a = c \circ b$.

**Def. (3.1.1.10)** [Fully Faithful Functors]. A functor of category $F : \mathcal{C} \to \mathcal{D}$ is called:

- a **full/faithful functor** if for any $x, y \in \text{Ob}(\mathcal{C})$, $F : \text{Hom}(X, Y) \to \text{Hom}(F(x), F(y))$ is surjective/injective.

- an **essentially surjective functor** if any object of $\mathcal{D}$ is equivalent to some $f(x)$, where $x \in \mathcal{C}$.

- an **equivalence** if there is a functor $G : \mathcal{D} \to \mathcal{C}$ that $F \circ G \cong \text{id}_\mathcal{D}$ and $G \circ F \cong \text{id}_\mathcal{C}$.

**Prop. (3.1.1.11)** [Category Equivalences]. A Functor $\mathcal{C} \to \mathcal{D}$ is an equivalence if and only if it’s fully faithful and essentially surjective.

**Proof:** There exist an object $G(X) \in \mathcal{C}$ and an isomorphism $\xi_X : FG(X) \to X$ for every $X \in \mathcal{D}$. Because $F$ is fully faithful, there exists a unique morphism $G(f) : G(X) \to G(Y)$ such that $F(G(f)) = \xi_Y^{-1} \circ f \circ \xi_X$ for every morphism $f : X \to Y$ in $\mathcal{D}$. Thus we obtain a functor $G : \mathcal{C} \to \mathcal{D}$ as well as a natural isomorphism $\xi : F \circ G \to \text{Id}_\mathcal{D}$. Moreover, the isomorphism $\xi_{F(Z)} : FGF(Z) \to F(Z)$ decides an isomorphism $\eta_Z : GF(Z) \to Z$ for every $Z \in \mathcal{C}$. This yields a natural isomorphism $\eta : G \circ F \to \text{Id}_\mathcal{C}$. $\square$

**Def. (3.1.1.12)** [Setoids]. A **setoid** is a category that is equivalent to a category that has only the identity morphisms.

**Def. (3.1.1.13)** [Groupoids]. A **groupoid** is a category that all morphisms are isomorphisms.
Prop. (3.1.1.14) [Equivalence Relations]. An equivalence relation is a groupoid that 
\( \# \text{Mor}_\mathcal{C}(x, y) \leq 1 \) for any \( x, y \in \mathcal{C} \).

Prop. (3.1.1.15). A category is equivalent to a setoid iff it is an equivalence relation.

Proof: \( \square \)

Def. (3.1.1.16) [Subcategories]. Let \( \mathcal{C} \) be a category, a subcategory \( \mathcal{C}' \) of \( \mathcal{C} \) is a category together 
with a functor \( F : \mathcal{C}' \to \mathcal{C} \) s.t. \( F : \text{Ob}(\mathcal{C}') \to \text{Ob}(\mathcal{C}) \) is injective and \( F \) is faithful. And it is called a 
full subcategory if \( F \) is fully faithful. It is called a strictly full subcategory if for any \( y \in \mathcal{C} \), 
\( y \) is equivalent to some \( F(x), x \in \text{Ob}(\mathcal{C}') \) iff \( y \in F(\mathcal{C}') \).

Def. (3.1.1.17) [Comma Categories]. For a category \( \mathcal{C} \) and an object \( S \), the 
comma category \( \mathcal{C} / S \) is defined to be the category of arrows \( T \to S \) with the arrows being compatible arrows over \( S \).

Def. (3.1.1.18) [Category of Arrows]. For a category \( \mathcal{C} \), the category of arrows \( \text{Arr}(\mathcal{C}) \) is a category 
whose objects are arrows in \( \mathcal{C} \) and a morphism \( f \to g \) is a commutative diagram

\[
\begin{array}{ccc}
A & \xrightarrow{h} & B \\
\downarrow f & & \downarrow g \\
A' & \xleftarrow{k} & B'
\end{array}
\]

Def. (3.1.1.19) [Twisted Arrow Category]. For a category \( \mathcal{C} \), the category of twisted arrows \( \text{TW}(\mathcal{C}) \) 
is a category whose objects are arrows in \( \mathcal{C} \) and a morphism \( f \to g \) is a diagram

\[
\begin{array}{ccc}
A & \xleftarrow{h} & B \\
\downarrow f & & \downarrow g \\
A' & \xrightarrow{k} & B'
\end{array}
\]

Def. (3.1.1.20) [Final Objects]. An object \( Z \) of a category is called a final object if 
\( \# \text{Hom}(X, Z) = 1 \) for any object \( X \). It is called weakly final if \( \text{Hom}(X, Z) \neq \emptyset \) for every object \( X \). 
Dually an object is called (weakly) initial if it is (weakly) initial as an object of \( \mathcal{C}^{\text{op}} \).

Def. (3.1.1.21) [Epimorphisms and Monomorphisms]. An epimorphism in a category is a morphism \( X \to Y \) that the map 
\( \text{Hom}(Y, Z) \to \text{Hom}(X, Z) \) induced by composition is injective. Dually, an 
monomorphism is an epimorphism in the dual category.

Def. (3.1.1.22) [Projective and Injective]. A projective object \( X \) in a category is an object that for any epimorphism \( (3.1.1.21) \) \( Y \to Z \), \( \text{Hom}(X, Y) \to \text{Hom}(X, Z) \) is surjective. Dually, an 
injective object \( X \) is a projective object in the dual category.

Def. (3.1.1.23) [Retract]. A morphism \( f \) in a category \( \mathcal{C} \) is called a retract of \( g \) if there are morphisms 
\( F, G : f \to g \) in \( \text{Mor}(\mathcal{C})(3.1.1.18) \) that \( G \circ F = \text{id}_f \).

Def. (3.1.1.24) [Equivalence relations]. For \( \mathcal{C} \in \text{Cat} \) has finite products, \( X_0 \in \mathcal{C} \), an equivalence 
relation on \( X_0 \) is a tuple \((X_1, u)\), where \( X_1 \in \mathcal{PSh}(\mathcal{C}) \) and \( u \in \text{Hom}(X_1, X_0 \times X_0) \) s.t for any 
\( X \in \mathcal{C} \), the map 
\[
\bar{X}_1(T) \xrightarrow{u} \bar{X}_0(T) \times \bar{X}_0(T)
\]
is a bijection of \( \bar{X}_1(T) \) onto the graph of an equivalence relation on \( \bar{X}_1(T) \). Similarly, we can define 
pre-relations on \( X_0 \), relations on \( X_0 \) and pre-equivalence relations on \( X_0 \).
Prop. (3.1.1.25) [Involutions]. Situation as in (3.1.1.24), then there is a morphism \( \sigma : F_0 \rightarrow F_0 \), \( \sigma^2 = \text{id}, u_0 \circ \sigma = u_1, u_1 \circ \sigma = u_0 \), by the symmetry in the definition of equivalence relations.

Def. (3.1.1.26) [Categorical Quotients]. Situation as in (3.1.1.24), for an equivalence relation \( u : X_1 \rightarrow X_0 \times X_0 \), a morphism \( v : X_0 \rightarrow X \) is called a categorical quotient if
- \( u \) factors through \( v : X_0 \rightarrow X \), and \( u : X_1 \rightarrow X_0 \times X_0 \) is an isomorphism.
- For any \( T \in \mathcal{C} \), there is a cokernel sequence
  \[
  \text{Mor}(X, T) \rightarrow \text{Mor}(X_0, T) \cong \text{Mor}(X_1, T)
  \]
  is exact.

Representable Functors

Def. (3.1.1.27) [Presheaves]. A presheaf on a category \( \mathcal{C} \) is defined to be a contravariant functor from \( \mathcal{C} \) to \( \text{Set} \). The category of presheaves on \( \mathcal{C} \) is denoted by \( \mathcal{P}\text{sh}(\mathcal{C}) \).

Prop. (3.1.1.28) [Representability Criterion]. Let \( \mathcal{C} \) be a complete category, \( F : \mathcal{C} \rightarrow \text{Set} \) be a functor. Assume that \( F \) commutes with limits, and the category \( \mathcal{I} \) of pairs \((x, f)\) where \( x \in \mathcal{C}, f \in F(x) \) has a cofinal family of objects indexed by a set \( I \), then \( F \) is representable, i.e. there is an object \( x \) that \( F(y) = \text{Mor}_\mathcal{C}(x, y) \), functorial in \( y \).

\[\text{Proof:} \quad \text{Because} \ \mathcal{C} \ \text{has small limits, let} \ \mathcal{I}' \ \text{be the full subcategory of} \ \mathcal{I} \ \text{generated by} \ (x_i, f_i), \ \text{set} \ x = \text{lim}_{(x_i, f_i) \in \mathcal{I}} x_i. \ \text{As} \ F \ \text{commutes with limits,} \ F(x) = \text{lim}_{(x_i, f_i) \in \mathcal{I}} F(x_i). \ \text{Hence there is a universal element} \ f \in F(x) \ \text{that maps to} \ f_i \ \text{under} \ F(x \rightarrow x_i). \ \text{f induces a natural transformation} \ \xi : \text{Mor}_\mathcal{C}(x, -) \rightarrow F(-).
\]

The assumption shows \( \xi \) is surjective. Now let \( x' \rightarrow x \) be the equalizer of all maps \( \varphi : x \rightarrow x \) that \( F(\varphi)f = f \), then there is a \( f' \in F(x') \) mapping to \( f \). Then the transformation \( \xi' \) defined by \( f' \) is also surjective. Now we also want to show it is injective: if \( a, b \in \text{Mor}_\mathcal{C}(x', y) \) mapsto the same element, then we consider the equalizer \( e' : x'' \rightarrow x' \) of \( a, b \), then the assumption and the fact \( F \) commutes with equalizer shows there is a \( f'' \in F(x'') \) mapping to \( f' \).

By universality consider a morphism \( \psi : x \rightarrow x'' \) that \( F(\psi)f = f'' \), then \( e \circ e' \circ \psi \) is a morphism \( x \rightarrow x \) that fixes \( f \), thus by construction \( ee'\psi e = e \), so \( e'\psi e = \text{id} \), because \( e \) is a monomorphism. Then \( e' \) is an epimorphism, thus \( a = b \).

\[\square\]

Adjunctions

Def. (3.1.1.29). Two functors \( f : \mathcal{C} \rightarrow \mathcal{D}, \ g : \mathcal{D} \rightarrow \mathcal{C} \) are called an adjunction pair iff there is a natural isomorphism of functors:

\[\mathcal{C}^{op} \times \mathcal{D} \rightarrow \text{Set} : \text{Hom}(f(-), -) \cong \text{Hom}(-, g(-)).\]

Equivalently this means that for any \( X_1 \rightarrow X_2 \in \mathcal{C}, Y_1 \rightarrow Y_2 \in \mathcal{D}, \)
\[
\begin{array}{ccc}
  f(X_1) & \longrightarrow & Y_1 \\
  \downarrow & & \downarrow \\
  f(X_2) & \longrightarrow & Y_2
\end{array}
\]

\[\square\]
is commutative iff its corresponding map

\[
\begin{array}{ccc}
X_1 & \longrightarrow & g(Y_1) \\
\downarrow & & \downarrow \\
X_2 & \longrightarrow & g(Y_2)
\end{array}
\]

is commutative.

Denoted an adjunction pair by \((f, g) : \mathcal{C} \rightleftarrows \mathcal{D}\).

**Prop. (3.1.1.30)**[Units and Counits]. If \(f, g\) are adjoints, then there are natural transformations \(u : \text{id} \to gf\), and \(v : fg \to \text{id}\), called the **unit/counit maps**. They satisfies \(f \overset{\sim}{\rightleftarrows} fgf \overset{\sim}{\rightarrow} f\) is id, and \(g \overset{\sim}{\rightleftarrows} gfg \overset{\sim}{\rightarrow} f\) is id.

Conversely, if there are natural morphisms \(u, v\) satisfying these two identities, then \((f, g)\) is an adjunction, by

\[
\text{Hom}(fX, Y) \to \text{Hom}(gfX, gY) \to \text{Hom}(X, gY) \to \text{Hom}(fX, fgY) \to \text{Hom}(fX, Y).
\]

**Proof:** 

\[\square\]

**Lemma(3.1.1.31).** Let \((f, g)\) be an adjunction pair, then

- If \(g \circ f\) is fully faithful, then \(f\) is fully faithful.
- If \(f \circ g\) is fully faithful, then \(g\) is fully faithful.

**Proof:** Cf.[Sta]0FWV. 

\[\square\]

**Prop. (3.1.1.32).** Let \((f, g)\) be an adjunction pair, then

- \(f\) is fully faithful iff \(u : \text{id} \to gf\) is an isomorphism.
- \(g\) is fully faithful iff \(v : fg \to \text{id}\) is an isomorphism.

**Proof:** 1: If \(\text{id} \cong gf\), then \(gf\) is fully faithful, so \(f\) is fully faithful by(3.1.1.31). If \(f\) is fully faithful, then for any \(X, Y\),

\[
\text{Hom}(X, Y) \xrightarrow{u} H(X, gfY) \cong H(fX, fY) \cong H(X, Y)
\]

is a canonical isomorphism, so \(u\) is an isomorphism.

2 is dual to 1. 

\[\square\]

**Cor. (3.1.1.33)**[Units and Equivalences]. Let \((F, G)\) be an adjunction pair, then the following are equivalent:

- \(F, G\) are both fully faithful.
- the unit and counit are both isomorphisms.
- \(F, G\) defines an equivalence of categories.

**Proof:** 1 \(\to\) 2 \(\to\) 3 follow from(3.1.1.32). And 3 \(\to\) 1 is clear. 

\[\square\]

**Prop. (3.1.1.34)**[Adjunction Preserves (Co)Limits]. A right adjoint functor is left exact and it preserves injectives if its left adjoint is exact.

A left adjoint functor is right exact and it preserves projectives if its right adjoint is exact.
Prop. (3.1.1.35) [Adjoint Functor Theorem]. Let \( G : \mathcal{C} \to \mathcal{D} \) be a functor, assume \( \mathcal{C} \) is complete and \( G \) commutes with colimits. Assume for every \( y \in \mathcal{D} \), the category of pairs \((x, f)\) where \( x \in \mathcal{C} \) and \( f \in \text{Mor}_\mathcal{D}(y, G(x)) \) has a cofinal family of objects indexed by a set \( I \), then \( G \) has a left adjoint. Similarly the dual statement holds.

Proof: The assumption shows that for any \( y \in \mathcal{D} \), the functor \( x \mapsto \text{Mor}_\mathcal{D}(y, G(x)) \) satisfies the condition of (3.1.1.28), thus it is representable by an object denoted by \( F(y) \). By Yoneda lemma, \( F \) underlies a functor, and this functor is a left adjoint of \( G \). □

Prop. (3.1.1.36) [Examples of Adjunction pairs].
- The valuation at \( k \)-th coordinate is left adjoint to the functor \( k^*(A) i = \prod_{\text{Hom}_i,k} A \) and is exact. So \( k_* \) preserves injectives.
- The sheaf \( \Gamma \) functor is right adjoint to the constant sheaf functor over arbitrary site.
- The inclusion functor is right adjoint to the shification functor over arbitrary site.
- The forgetful functor is right adjoint to the Shification functor, and shification is exact, so it preserves injectives.
- The stalk functor is left adjoint to the skyscraper sheaf operator.

Limits and Colimits

Prop. (3.1.1.37) [Products and Equalizers Implies Limits]. If a category admits arbitrary (resp. finite) products and equalizers, then it admits arbitrary (resp. finite) limits. Dually a category that admits coproducts and coequalizers admits all colimits.

Proof: The limits over a category \( \mathcal{C} \) is an equalizer of products over the category of arrows in \( \mathcal{C} \). □

Def. (3.1.1.38) [Exact Functor]. A functor \( F : \mathcal{C} \to \mathcal{D} \) is called an left exact functor if it maps finite limits to finite limits. It is called a right exact functor if it maps finite colimits to finite colimits. It is called an exact functor if it is both left exact and right exact.

Def. (3.1.1.39) [(Co)Complete Category]. A category is called (co)complete if it has all small (co)limits.

Def. (3.1.1.40) [Inverse System]. An inverse system in \( \mathcal{C} \) is a diagram \( Z^\text{op}_+ \to \mathcal{C} \), where \( Z_+ \) is the category of non-negative integers with a unique morphism \( n \to m \) iff \( n \leq m \).

Prop. (3.1.1.41) [Equivalent Inverse System]. Two inverse systems \( \{A_n\}, \{B_n\} \) are called equivalent if there are two non-decreasing unbounded maps \( \alpha, \beta : Z_+ \to Z_+ \) and maps \( \alpha : A_n \to B_{\alpha(n)}, \beta : B_n \to A_{\beta(n)} \) that is compatible with the transition maps and for any \( n \), there is a \( m \) large that \( A_m \to A_{\beta(m)} \to A_n \) coincide with the transition map \( A_m \to A_n \), and similar for \( B_n \). And similarly for colimits.

The limit for two inverse systems are the same, and similarly for colimits.

Prop. (3.1.1.42). Any presheaf on a small category is a colimit of representable sheaves \( h_X \). (Consider all \( h_X \to F \) and take colimit, prove it is isomorphism).

Prop. (3.1.1.43) [Filtered Colimit of Sets].
Prop. (3.1.1.44) [Cofiltered Limits of Sets]. A cofiltered limit of nonempty sets is nonempty.

Proof: Cf. [Sta]086J □

Def. (3.1.1.45) [Mittag-Leffler]. If \((A_i, \varphi_{ji})\) is a directed inverse system of sets over \(I\), then it is said to satisfy the Mittag-Leffler condition if \(\varphi_{ji}(A_j) \in A_i\) stabilizes. This is clearly true if \(\varphi_{ji}\) is surjective for any \(i, j\).

Prop. (3.1.1.46). If \((A_n)\) where \(n \in \mathbb{Z}\) is a Mittag-Leffler inverse system of nonempty sets, then \(\lim A_i\) is also nonempty.

Proof: Let \(A'_{j} = \cap_{j \geq i} \varphi_{ji} A_{j}\), then \((A'_{j})\) is a filtered system that the transition maps are all surjective, and clearly \(\lim A_{j} = \lim A'_{j}\), so it is nonempty by (3.1.1.44). □

Fiber Product

Prop. (3.1.1.47). For a category \(C\), the following are equivalent:

- It has arbitrary limits.
- It has arbitrary products and equalizer.
- It has arbitrary products and fibered products.

Proof: 1 \(\rightarrow\) 2, 1 \(\rightarrow\) 3 is trivial. 3 \(\rightarrow\) 2: The equalizer for \(f, g : X \rightarrow Y\) can be constructed as the base change of \(Y \rightarrow Y \otimes Y\) along \((f, g) : X \rightarrow Y \times Y\). 2 \(\rightarrow\) 1: for any diagram \(F : I \rightarrow C\), the fibered pullback can be constructed as the equalizer of two morphisms:

\[
\begin{align*}
  s, t : & \prod_{i \in Ob(I)} F(i) \rightarrow \prod_{f : i \rightarrow k \in Mor(I)} F(k) \\
  \text{where } \pi_{(f : j \rightarrow k)} s = \pi_{k}, \text{ and } \pi_{(f : j \rightarrow k)} t = (Ff)\pi_{j}.
\end{align*}
\]

\(□\)

Prop. (3.1.1.48) [Diagonal Base Change]. The diagonal commutes with base change:

\[
\begin{array}{ccc}
X \times_Y Z & \xrightarrow{\Delta} & (X \times_Y Z) \times_Z (X \times_Y Z) \\
\downarrow & & \downarrow \\
X & \xrightarrow{\Delta} & X \times_Y X
\end{array}
\]

Proof: □

Prop. (3.1.1.49). \((X \times_Y Z) \times_S (Z \times_F W) = (X \times_S Z) \times_{E \times_S F} (Y \times_S W)\).

Proof: □

Prop. (3.1.1.50). For \(f : X \rightarrow T\) and \(g : Y \rightarrow T\) and \(h : T \rightarrow S\), \(X \times_T Y = T \times_X S\) \((X \times_S Y)\). In particular, \(X \times_T Y \rightarrow X \times_S Y\) is a base change of \(T \rightarrow T \times_S T\).

Proof: For any object \(U\),

\[
\text{Hom}(U, X \times_T Y) = \{s : U \rightarrow X, t : U \rightarrow Y | f \circ s = g \circ t\},
\]

\[
\text{Hom}(U, T \times_T S(X \times_S Y)) = \{r : U \rightarrow T, s : U \rightarrow X, t : U \rightarrow Y | h \circ f \circ s = h \circ g \circ t, r = g \circ t, r = f \circ s\},
\]

so they are functorially isomorphic. Then by Yoneda lemma we have the desired isomorphism. □
Prop. (3.1.1.51). The diagonal map \( X \to X \times_Y X \) is an isomorphism iff \( X \to Y \) is monomorphism. (Because this is equivalent to \( \text{pr}_1 = \text{pr}_2 \)).

Def. (3.1.1.52) [Mapping graph]. Let \( f : X \to Y \) be a morphism in a category with fiber products and finite products, then the mapping graph \( \Gamma_f \) of \( f \) is defined to be the pullback

\[
\begin{array}{c}
\Gamma_f \to X \times Y \\
\downarrow \\
Y \to Y \times Y
\end{array}
\]

it can be seen that \( \Gamma_f \) is isomorphic to \( X \).

Localizations

Def. (3.1.1.53) [Localizing Categories]. Let \( \mathcal{C} \) be a category and \( S \) be a class of morphisms, then a functor \( F : \mathcal{C} \to \mathcal{D} \) is called the localizing category of \( \mathcal{C} \) w.r.t \( S \) if it maps morphisms in \( S \) to isomorphisms, and any other functor with this property factors uniquely through \( F \).

Def. (3.1.1.54) [Localizing Systems]. A class of morphisms \( S \) in a category is called a left (resp. right) localizing system if:

- (LS1): \( S \) is closed under composition and contains all the identities.
- (LS2): for every \( s \in S \) and \( f \) with the same source (resp. target), there is a \( t \in S \) and a \( g \), s.t. \( t \circ f = g \circ s \) (resp. \( f \circ t = s \circ g \)).
- (LS3): the existence of a \( t \in S \) s.t. \( ft = gt \) implies (resp. is implied by) the existence of a \( s \in S \) s.t. \( sf = sg \).

It is called localizing system if it is both left localizing and right localizing.

Def. (3.1.1.55) [Saturated Localizing Systems]. Let \( S \) be a localizing system, then it is called a saturated localizing system moreover it satisfies

- if \( f, g, h \in S \) and \( fg, gh \in S \), then \( g \in S \).

Def. (3.1.1.56) [Gabriel-Zisman Localization]. Cf. [Sta]04VD.

Cor. (3.1.1.57). If \( \mathcal{C} \) is a category and \( S \) is a left localizing system, then the rule \( X \mapsto X, (f : X \to Y) \mapsto \text{id}^{-1} f \) is a functor \( \mathcal{Q} : \mathcal{C} \to S^{-1}\mathcal{C} \) that represents \( S^{-1}\mathcal{C} \) as a localizing category of \( \mathcal{C} \) w.r.t \( S \)(3.1.1.53). And \( Q \) preserves finite colimits.

The dual is true for a right localizing system \( S \).

Proof: Cf.[[Sta]04VG], [[Sta]05Q2].

Cor. (3.1.1.58). If \( \mathcal{C} \) is a category and \( S \) is a localizing system, then the left localizing category and the right localizing category is canonically isomorphic, by the universal property(3.1.1.53).

Prop. (3.1.1.59) [Saturation]. If \( S \) is a localizing system in a category \( \mathcal{C} \), then the morphisms in \( \mathcal{C} \) that is mapped to an isomorphism in \( S^{-1}\mathcal{C} \) is the smallest saturated localizing system containing \( S \), called the saturation of \( S \).

Proof: Cf.[[Sta]05Q9].

Prop. (3.1.1.60) [Full Subcategories of Localized Categories]. If \( S \) is a left localizing system in a category \( \mathcal{C} \), \( \mathcal{C}' \) is a full subcategory of \( \mathcal{C} \) and \( S' \) is a left localizing system of \( \mathcal{C}' \) that \( S' \subset S \). If for any \( s : X \to Y \in S \) and \( X \in \mathcal{C}' \), there is a morphism \( t : Y \to Z \) that \( Z \in \mathcal{C}' \) and \( t \circ s \in S' \), then the natural functor \( (S')^{-1}\mathcal{C}' \to S^{-1}\mathcal{C} \) is fully faithful. And the dual is true for right localizing systems.

Proof: This is not hard from the Gabriel-Zisman localization description(3.1.1.56).
3.1. CATEGORIES

**Group Objects**

**Def. (3.1.1.61) [Group Object].** In a category \( C \) with finite products and a final object \( e \), a(n) **(Abelian)group object** is an object \( G \) that \( h_G \) is a functor from \( C \) to \( \mathcal{G} \text{rp} \) (resp. \( \mathcal{A} \text{b} \)). And a homomorphism of group objects is a natural transformation as a functor from \( C \) to \( \mathcal{G} \text{rp} \).

This is in fact equivalent to a morphism \( m_G : G \times G \to G \) and \( i_G : G \to G, e_G : e \to G \) that satisfy the desired commuting diagrams.

**Def. (3.1.1.62) [Group Action].** A **(left)action** of a group object \( G \) on an object \( X \) is a map of presheaves \( h_G \times h_X \to h_X \) that for any \( U \), \( h_G(U) \times h_X(U) \to h_X(U) \) is a group action. This is equivalent to a morphism \( \mu : G \times X \to X \) that satisfies the desired commuting diagrams.

**Prop. (3.1.1.63).** Let \( \mu : G \times X \to X \) be an action of a group object \( G \) on an object \( X \), there is a commutative diagram

\[
\begin{array}{ccc}
G \times X & \xrightarrow{(g,x)\mapsto(g,gx)} & G \times X \\
\downarrow{(g,x)\mapsto gx} & & \downarrow{\pi_2} \\
X & \xrightarrow{id} & X
\end{array}
\]

and the horizontal maps are isomorphisms.

**Cor. (3.1.1.64).** Considering the action of \( G \) on itself, we get

\[
\begin{array}{ccc}
G \times G & \xrightarrow{(g,h)\mapsto(g,gh)} & G \times G \\
\downarrow{m} & & \downarrow{\pi_2} \\
G & \xrightarrow{id} & G
\end{array}
\]

and the horizontal maps are isomorphisms.

**Prop. (3.1.1.65).** A unital magma object \( G \) in the category of groups is an Abelian group.

**Proof:** A unital magma object structure endows \( G \) with maps \( (\tilde{m}, \tilde{e}) \), and \( \tilde{m}(ab, cd) = \tilde{m}(a, c)\tilde{m}(b, d) \), because \( \tilde{m} \) is a morphism of groups. So we can use Eckmann-Hilton argument\(^2\) to show the category multiplication is the same as the group multiplication. So the commutativity of \( \tilde{m} \) with the inverse \( i \) implies that it is Abelian. \( \square \)

**Prop. (3.1.1.66).** A right-lax monoidal functor (3.1.4.10) between Cartesian monoidal structures maps a unital magma object to a unital magma object.

**Def. (3.1.1.67) [Categorical Quotient].** Let \( C \) be a category with finite products, \( G \) be a group object in \( C \), \( G \times X \to X \) is a left action (3.1.1.62), then a morphism \( X \to Y \) is called the **categorical quotient** of \( X \) iff \( Y \) is the coequalizer of \( G \times X \xrightarrow{\rho} X \). It is called the **universal categorical quotient** of \( X \) iff its product with \( S \) is the categorical quotient for each element \( S \in C \), in the category \( C/\Sigma \).
2 Ends and Coends

Def. (3.1.2.1) [Dinatural Transformation]. Given categories $\mathcal{C}, \mathcal{D}$ and functor $P, Q : \mathcal{C}^{op} \times \mathcal{C} \to \mathcal{D}$, then a dinatural transformation $\alpha : P \to Q$ is a family of arrows $\alpha_C : P(C, C) \to Q(C, C)$ where $C \in \mathcal{C}$ that for any arrow $C \to C' \in \mathcal{C}$, there is a commutative diagram

\[
P(C', C) \xrightarrow{\alpha_C} P(C, C) \xrightarrow{\alpha_{C'}} Q(C', C) \xrightarrow{} Q(C, C')
\]

Def. (3.1.2.2) [Wedge and Cowedge]. Let $P : \mathcal{C}^{op} \times \mathcal{C} \to \mathcal{D}$ be a functor, then a wedge for $P$ is a binatural functor $\Delta_D \to P$, where $D$ is an object of $\mathcal{C}$. Similarly a cowedge is a binatural functor $P \to \Delta_D$.

Def. (3.1.2.3) [End and Coend]. For a functor $P : \mathcal{C}^{op} \times \mathcal{C} \to \mathcal{D}$, the wedges and cowedges of $P$ form categories, and we define end of $P$ is just a terminal wedge, denoted by $\int^\mathcal{C} P(C, C)$, and the coend of $P$ is the initial cowedge, denoted by $\int_\mathcal{C} P(C, C)$.

Ends and coends are functorial w.r.t natural transformations.

Prop. (3.1.2.4) [Ends as Colimits]. There is a morphism

\[
F \mapsto \overline{F} : \text{Fun}(\mathcal{C}^{op} \times \mathcal{C}, \mathcal{D}) \to \text{Fun}(\text{Tw}(\mathcal{C}), \mathcal{D})
\]

where we maps $f : C \to C'$ to $F(C, C')$. Then it can be checked that

\[
\int^\mathcal{C} F(C, C) = \lim_{\text{Tw}(\mathcal{C})} \overline{F}, \quad \int_\mathcal{C} F(C, C) = \colim_{\text{Tw}(\mathcal{C})} \overline{F}.
\]

Cor. (3.1.2.5). A functor that preserves (co)limits preserves (co)ends.

Cor. (3.1.2.6). For an object $D \in \mathcal{D}$, we have isomorphisms:

\[
\text{Hom}(\int^\mathcal{C} F(C, C), D) \cong \int_C \text{Hom}(F(C, C), D),
\]

\[
\text{Hom}(D, \int_\mathcal{C} F(C, C)) \cong \int_C \text{Hom}(D, F(C, C)).
\]

Prop. (3.1.2.7) [Fubini]. Cf.[Coend Calculus, P20].

Prop. (3.1.2.8) [Natural Transformation as Ends]. Let $F, G : \mathcal{C} \to \mathcal{D}$ be functors, then the set of natural transformations is an coend.

\[
\text{Map}(F, G) \cong \int^\mathcal{C} \text{Hom}_{\mathcal{D}}(FC, GC)
\]

Kan Extension

Cf.[All Concepts are Kan Extensions].
Def. (3.1.2.9) [Kan Extensions]. Given functors $F : \mathcal{C} \to \mathcal{E}$ and $K : \mathcal{C} \to \mathcal{D}$, a left Kan extension of $F$ along $K$ is a functor $\text{Lan}_K F : \mathcal{D} \to \mathcal{E}$ together with a natural transformation $\eta : F \to \text{Lan}_K F \circ K$ that for any other pair $(G : \mathcal{D} \to \mathcal{E}, \gamma : F \to G \circ K)$, $\gamma$ factors uniquely through $\eta$.

Dually, a right Kan extension of $F$ over $K$ is equivalent to a left Kan extension of $F^{\text{op}}$ over $K^{\text{op}}$.

Prop. (3.1.2.10) [(Co)Limits as Kan Extensions]. If $\mathcal{D}$ is the final category 1, then the left Kan extension is just the colimit of the diagram defined by $F$, and the right Kan extension is just the limit of the diagram defined by $F$.

Prop. (3.1.2.11) [Yoneda Lemma]. $h_X : Y \mapsto \text{Hom}(Y, X)$ is a presheaf, and $\text{Hom}(h_X, F) \cong F(X)$ for any presheaf $F$.

So $X \to h_X$ is a fully faithful embedding from $\mathcal{C}$ to $\hat{\mathcal{C}} = \text{Func}(\mathcal{C}^{\text{op}}, \text{Set})$. In particular, if a $X \to Y$ induces isomorphism $\text{Hom}(W, X) \to \text{Hom}(W, Y)$ for every $W$, then $X \cong Y$.

So we can regard $C$ as a fully faithful subcategory of $\hat{\mathcal{C}}$.

Proof: The map $\text{Hom}(h_X, F) \to F(X)$ maps a $u$ to $u(X)(\text{id}_X)$. And the inverse map is defined to be $x \in F(X) \mapsto (s \in \text{Hom}(Y, X) \mapsto s^*(x) \in F(Y)) \in \text{Hom}(h_X, F)$.

Cor. (3.1.2.12). A universal object for a presheaf $F$ is a pair $(X, \zeta)$ that $\zeta \in F(X)$ with the property that for any $U$ and a $\sigma \in F()$, there is a unique arrow $U \to X$ that $Ff(\zeta) = \sigma$.

In fact, a universal object is equivalent to an isomorphism $h_X \cong F$, and this makes it easy to check whether a presheaf $F$ is representable.

Prop. (3.1.2.13) [Presheaves as Colimits of Presentable Presheaves]. Any presheaf of sets in $C$ is a colimit of presentable presheaves of $C$. More precisely, there is an isomorphism $F \cong \lim_{h_X \to F} h_X$.

From this we see that any morphism $\hat{C} \to D$ is determined by its restriction on $C$.

Proof: For any presheaf $G$, there is a morphism $\text{Hom}(F, G) \to \text{Hom}(\lim_{h_X \to F} h_X, G)$, i.e. a set of sections $f_s \in G(X)$ for every $h_X \to F$, that if $t \circ u = s$, then $u^*(f_t) = f_s$. Conversely, by Yoneda lemma, this just says that there is a morphism of presheaves $F \to G : F(X) \to G(X) : s \mapsto f_s$.

Cor. (3.1.2.14) [Kan Extension]. For a cocomplete category $\mathcal{D}$, there is a natural bijection between functor $\hat{\mathcal{C}} \to \mathcal{D}$ that commutes with colimits and functors $\mathcal{C} \to \mathcal{D}$ by Yoneda embedding.

Proof: For this, we only have to notice the functor $\mathcal{D} \to \hat{\mathcal{C}} : D \mapsto \text{Hom}(FX, D)$ is right adjoint to $F : \hat{\mathcal{C}} \to \mathcal{D}$ when $F$ is defined by colimit as in (3.1.2.13).

Cor. (3.1.2.15). Any contravariant functor $F : \hat{\mathcal{C}} \to \text{Set}$ that take colimits to limits, $F$ is representable. (Just use $G$ in the last proof, $F$ is representable by $G(\text{pt})$).

Def. (3.1.2.16) [$J$-Free Diagram]. For a cocomplete category $\mathcal{C}$ and a small category $J$, let $J^\delta$ be the subcategory of $J$ that has the same objects but only the identity morphisms, then an $J$-diagram in $\mathcal{C}$ is called $J$-free iff it is a left Kan extension of some diagram $J^\delta \to \mathcal{C}$. 
3 2-Categories

Remark (3.1.3.1)[2-Categories]. 2-categories are defined as in (3.13.2.25).

Def. (3.1.3.2) [(2, 1)-Categories]. A (2, 1)-category is a 2-category that all the 2-morphisms (corresponding to a 2-simplex) are isomorphisms.

Def. (3.1.3.3) [Final Objects]. A final object in a (2, 1)-category is an object \( x \) that for any object \( y \) there is a morphism \( y \to x \), and any two morphisms \( y \to x \) are isomorphic by a unique 2-morphism.

Lemma (3.1.3.4) [2-Commutative diagrams]. Let \( C \) be a 2-category, and \( g : y \to z, f : x \to z \) are arrows in \( C \), then the diagrams in \( C \):

\[
\begin{array}{ccc}
w & \xrightarrow{a} & x \\
\downarrow{b} & & \downarrow{f} \\
y & \xrightarrow{g} & z
\end{array}
\]

together with a 2-morphism from \( gb \) to \( fa \), naturally form a 2-category. A diagrams with invertible 2-morphisms are called 2-commutative diagram in \( C \).

Def. (3.1.3.5) [2-Fibered Products]. Let \( C \) be a 2-category, and \( g : y \to z, f : x \to z \) are arrows in \( C \), a 2-fibered product of \( f, g \) is a final object in the (2, 1)-category of 2-commutative diagrams as defined in (3.1.3.4), and it is denoted by \( x \times_z y \).

4 Monoidal Categories

Main references are [Tensor Categories, Etingof], [Lur09].

Def. (3.1.4.1) [Monoidal Category]. A monoidal category is a category \( \mathcal{C} \) with a functor \( \otimes : \mathcal{C} \times \mathcal{C} \to \mathcal{C} \) and a unit object 1 together with isomorphisms

\[
\eta_{A,B,C} : (A \otimes B) \otimes C \to A \otimes (B \otimes C), \quad \alpha_A : A \otimes 1 \to A, \quad \beta_A : 1 \otimes A \to A
\]

that satisfies the following commutative diagrams: Cf.[HTT, P791]. (Pentagon diagram)

Def. (3.1.4.2) [Dual and Opposed Category]. Let \( \mathcal{C} \) be a monoidal category, then the opposed category \( \mathcal{C}^{opp} \) is the same category as \( \mathcal{C} \) with the tensoring switched, which is also a monoidal category.

The dual category \( \mathcal{C}^{opp} \) with the same tensoring is also a monoidal category.

Def. (3.1.4.3). A strict monoidal category is a monoidal category that the isomorphisms above are all identities.

Prop. (3.1.4.4) [Mac Lane Coherence]. In a monoidal category, any two morphisms between two bracketings of a product \( X_1 \otimes \ldots X_n \) constructed using the isomorphisms \( \eta_{A,B,C} \) are equal. Also if some \( X_i \) are 1, then we can also use \( \alpha_A \) and \( \beta_A \).

Prop. (3.1.4.5) [Cartesian Monoidal Category]. For a category that has finite products, the product makes \( \mathcal{C} \) a symmetric monoidal category, called the Cartesian monoidal structure.

The Cartesian monoidal structure of the category of sets the default monoidal structure.

Prop. (3.1.4.6). For any category \( \mathcal{C} \), the category \( \mathcal{C}[\mathcal{C}, \mathcal{C}] \) of endofunctors has a natural monoidal structure.
Def. (3.1.4.7) [Closedness]. A monoidal category $(\mathcal{C}, \otimes)$ is called **left-closed** if for every $A \in \mathcal{C}$, the functor $N \mapsto A \otimes N$ has a right adjoint $Y \mapsto A^Y$ (or denoted by $\text{Hom}(A, Y)$ when $\mathcal{C}$ is symmetric). Dually it is called **right-closed** if $\mathcal{C}^{op}$ is left-closed. It is called **closed** if it is both left-closed and right-closed.

For a Cartesian monoidal category $\mathcal{C}$, $\mathcal{C}$ is called **Cartesian closed** if it is closed for the Cartesian monoidal structure.

Def. (3.1.4.8) [Reflexive Objects]. Let $(\mathcal{C}, \otimes)$ be a symmetric monoidal category that is closed, then we denote $\text{Hom}(Y, 1)$ by $Y^\vee$, then there is a natural map $Y \to (Y^\vee)^\vee$. If such a map is reflexive, then $Y$ is called a **reflexive object**.

Prop. (3.1.4.9). If $\mathcal{C}$ is closed, then

$$
\lim_{A_i} B \cong \lim \text{lim} (A_i B) \quad A (\lim_{B_i} A) \cong \lim \text{lim} (A B_i)
$$

**Proof:** Because $\mathcal{C}$ is closed, left and right tensor $A \otimes -$ and $- \otimes A$ are both left adjoints thus commutes with colimits. Now $B \mapsto A B$ is a right adjoint, thus it commutes with limits. And for any $C \in \mathcal{C}$,

$$
\text{Hom}(C, \lim_{A_i} B) \cong \text{Hom}(C \otimes (\lim_{A_i} B), B) \cong \lim \text{Hom}(C \otimes A_i, B)
$$

$$
\cong \lim B \text{Hom}(C \otimes A_i, B) \cong \lim \text{Hom}(A_i B) \cong \text{Hom}(C, \lim (A_i B))
$$

so $\lim_{A_i} B \cong \lim (A_i B)$ by Yoneda lemma.

Def. (3.1.4.10) [Monoidal Functor]. Let $(\mathcal{C}, \otimes), (\mathcal{D}, \otimes)$ be monoidal categories, then a **right-lax monoidal functor** from $\mathcal{C}$ to $\mathcal{D}$ is a functor $G$ together with morphisms $\gamma_{A,B}: G(A) \otimes G(B) \to G(A \otimes B)$ for any $A, B \in \mathcal{C}$ and a morphism $e : 1_{\mathcal{D}} \to G(1_\mathcal{C})$ that satisfies the following compatibility conditions: (Hexagon diagram).

Moreover, it is called a **monoidal functor** if $\gamma_{A,B}$ and $e$ are all isomorphisms.

Def. (3.1.4.11) [Equivalence of Monoidal Categories]. An equivalence of monoidal categories is a map that is an equivalence of categories as well as a monoidal functor.

Prop. (3.1.4.12) [Mac Lane Strictness]. Any monoidal category is equivalent to a strict monoidal category.

Prop. (3.1.4.13) [Examples]. For a monoidal category $(\mathcal{C}, \otimes)$, the functor $X \mapsto \text{Hom}(1, X)$ is a right-lax monoidal functor from $\mathcal{C}$ to $\text{Set}(3.1.4.5)$.

The morphism $\pi_0 : A \mapsto \pi_0(A)$ is a monoidal functor from the category of topological spaces $\text{Top}$ to the category $\text{Set}$ because it commutes with products.

**Proof:**

Symmetric Monoidal Categories

Def. (3.1.4.14) [Symmetric Monoidal Category]. A symmetric monoidal category is a monoidal category $(\mathcal{C}, \otimes)$ together with a natural transformation $\psi$ between $\otimes$ and $\otimes \circ \sigma : \mathcal{C} \times \mathcal{C} \to \mathcal{C}$ that $\psi^2 = \text{id}$ and the following commutative hexagon diagram is commutative:

A **symmetric monoidal functor** between symmetric monoidal categories are required to commutes with the braiding.
Rigid Monoidal Categories

Def. (3.1.4.15) [Duals]. Let \( C \) be a monoidal category and \( V \in C \), a left dual of \( V \) is an element \( V^* \) together with maps
\[
ev_V : V^* \otimes V \to 1, \quad coev_V : 1 \to V \otimes V^*
\]
that satisfies
\[
V \to V \otimes V^* \otimes V, \quad V^* \to V^* \otimes V \otimes V^* \to V^*
\]
are identities.

Similarly we can define right dual. if \( Y \) is a left/right dual to \( X \), then \( X \) is right/left dual to \( Y \).

Def. (3.1.4.16) [Dual Morphisms]. Let \( f : X \to Y \) be a morphism and \( X^*, Y^* \) the left duals of \( X \) and \( Y \), then there is a natural left dual map: \( f^* : Y^* \to X^* \) given by
\[
Y^* \to Y^* \otimes X \otimes X^* \to Y^* \otimes Y \otimes X^* \to X^*.
\]

Prop. (3.1.4.17). Let \( F : C \to D \) be a monoidal functor of monoidal categories, \( X \in C \) is an object with left dual \( X^* \). Then \( F(X^*) \) is a left dual of \( F(X) \) with evaluation and coevaluation maps
\[
ev_{F(X)} : F(X^*) \otimes F(X) \to F(X^* \otimes X) \to F(1_C) \to 1_D,
\]
\[
coev_{F(X)} : 1_D \to F(1_C) \to F(X \otimes X^*) \to F(X) \otimes F(X^*).
\]
and similarly for right duals.

Prop. (3.1.4.18) [Adjointness]. Let \( C \) be a monoidal category and \( V \in C \) with left dual \( V^* \), then there are natural adjunction maps
\[
\text{Hom}(U \otimes V, W) \cong \text{Hom}(U, W \otimes V^*), \quad \text{Hom}(V^* \otimes U, W) \cong \text{Hom}(U, V \otimes W).
\]

Proof: The first adjunction map is given by \( f \mapsto (f \otimes \text{id}_{V^*}) \circ (\text{id}_U \otimes coev_V) \), and the inverse given by \( g \mapsto (W \otimes ev_V) \circ (g \otimes \text{id}_{V^*}) \). The verification and the second one: \( \square \)

Cor. (3.1.4.19). In particular, we can use Yoneda lemma to show the left/right adjoints are unique if they exist.

Def. (3.1.4.20) [Rigid Tensor Categories]. Let \( C \) be a monoidal category, an element \( X \in C \) is called rigid if it has left and right duals. A rigid monoidal category is a monoidal category that every object is rigid. In particular, by (3.1.4.18), a rigid monoidal category is closed.

Prop. (3.1.4.21). If \( C \) is a rigid tensor category, then the functor
\[
\text{Equivalence of } C^{op} \text{ and } C^{opp}.
\]

Cor. (3.1.4.22). Any natural transformation of monoidal functors between rigid monoidal categories is an isomorphism.

Proof: Cf. [Milne, Tannakian Categories, P13]. \( \square \)

Prop. (3.1.4.23) [Trace and Rank]. Let \( C \) be a rigid symmetric monoidal category, we can define a trace morphism
\[
\text{tr}_X : \text{End}(X) \to \text{End}(1) : f \mapsto 1 \to X \otimes X^* \xrightarrow{f \otimes \text{id}} X \otimes X^* \to X^* \otimes X \to 1
\]
And the dimension of \( X \) is defined to be \( \text{tr}_X(\text{id}_X) \in \text{End}(1) \).
Invertible Objects and Grothendieck Categories

Def. (3.1.4.24) [Invertible Objects]. An invertible object in a monoidal category is a rigid object $L$ that the evaluation maps and coevaluation maps are all isomorphisms.

Tensor Categories

Def. (3.1.4.25) [Tensor Categories]. A tensor category over a field $k$ is an Artinian Abelian category over $k$ together with a rigid monoidal structure that is bilinear and satisfies $\text{End}(1) = k$.

A tensor functor is a functor between tensor categories that is additive and monoidal.

Prop. (3.1.4.26) [End(1)]. If $\mathcal{C}$ is a rigid additive tensor category, then $\text{End}(1)$ is a ring that acts on objects $X \in \mathcal{C}$ via $X \cong 1 \otimes X$. The action of $\text{End}(1)$ commutes with $\text{End}(X)$, in particular, $\text{End}(1)$ is commutative and $\mathcal{C}$ is $\text{End}(1)$-linear.

Prop. (3.1.4.27) [Abelian Rigid Tensor Category Exact]. If $\mathcal{C}$ is an rigid Abelian tensor category, then $\otimes$ commutes with inverse limits and direct limits in each variable.

Proof: It commutes with direct limits because it is left adjoint to the Hom functor, and it commutes with inverse limits by considering the opposite category (3.1.4.21).

Prop. (3.1.4.28). $\dim(X \otimes Y) = \dim X \cdot \dim Y$. If there is an exact sequence $0 \rightarrow X \rightarrow Z \rightarrow Y \rightarrow 0$, then $\dim(Z) = \dim(X) + \dim(Y)$.

Prop. (3.1.4.29) [Decompositions]. Let $(\mathcal{C}, \otimes)$ be a rigid Abelian tensor category and if $U$ is a subobject of 1, then $1 = U \oplus U^\perp$ where $U^\perp = \ker(1 \rightarrow U^\vee)$. Consequently, 1 is a simple object iff $\text{End}(1)$ is a field. And any rigid tensor category can be decomposed as rigid Abelian tensor categories $\mathcal{C}_I$ with $\text{End}(1_I)$ being fields.

Proof: Let $V = \text{Coker}(U \rightarrow 1)$, by tensoring $0 \rightarrow U \rightarrow 1 \rightarrow V \rightarrow 0$ with $U \hookrightarrow 1$, we get exact sequences

$$
\begin{array}{cccccc}
0 & \rightarrow & U & \rightarrow & 1 & \rightarrow & V & \rightarrow & 0 \\
\uparrow & & \uparrow & & \uparrow & & \uparrow \\
0 & \rightarrow & U \otimes U & \rightarrow & U & \rightarrow & V \otimes U & \rightarrow & 0
\end{array}
$$

thus $V \otimes U = 0$ and $U \otimes U = U$ via $1 \otimes 1 \cong 1$.

For the rest, Cf. [Tannakian Categories, Milne, P14].

Def. (3.1.4.30) [Associative Algebra in a Symmetric Tensor Category].

Prop. (3.1.4.31) [Fiber Functors]. If a symmetric tensor category admits an additive monoidal functor from $\mathcal{C} \rightarrow \text{Vect}_k$, then it is unique up to isomorphisms. Such a functor is called a fiber functor.

Def. (3.1.4.32) [Tannakian Categories]. A Tannakian category is a symmetric tensor category $\mathcal{C}$ over $k$ which admits a fiber functor $F : \mathcal{C} \rightarrow \text{Vect}_k$.

Prop. (3.1.4.33). An Tannakian category is equivalent to the symmetric tensor category $\text{Rep}(G)$ for an affine group scheme $G$, and $G$ is uniquely defined up to inner automorphisms.
5 Enriched Category

Def. (3.1.5.1) [Enriched Category]. Given a monoidal category \((\mathcal{C}, \otimes)\), an enriched category \(\mathcal{D}\) over \(\mathcal{C}\) consists of the following data:

- a collection of objects.
- For objects \(X, Y \in \mathcal{D}\), a mapping object \(\text{Map}_\mathcal{D}(X, Y) \subseteq \mathcal{C}\).
- For objects \(X, Y, Z \in \mathcal{D}\), a composite map \(\text{Map}(X, Y) \otimes \text{Map}(Y, Z) \to \text{Map}(X, Z)\) that is associative.
- For every \(X \in D\), a morphism \(1 \mapsto \text{Map}(X, X)\) that satisfies the commutative diagrams of the identity morphism.

Def. (3.1.5.2) [Category of Enriched Categories]. We can naturally define morphisms and natural transformations of categories enriched over a monoidal category \(\mathcal{C}\).

Prop. (3.1.5.3) [Transfer of Enriched Structure]. Given a right-lax monoidal functor between monoidal categories \(F : \mathcal{C} \to \mathcal{C}'\) and a category \(\mathcal{D}\) enriched over \(\mathcal{C}\), we may obtain a category \(F(\mathcal{D})\) enriched over \(\mathcal{C}'\) by asserting \(\text{Map}_{F(\mathcal{D})}(X, Y) = F(\text{Map}(X, Y))\). It is an enriched category just by the definition of right-lax monoidal functors.

Prop. (3.1.5.4) [Underlying Category]. For a category enriched \(\mathcal{D}\) over \(\mathcal{C}\), by (3.1.4.13), we can transfer the structure via \(\mathcal{C} \to \text{Set} : X \mapsto \text{Hom}(1, X)\), and the resulting category is called the underlying category of \(\mathcal{D}\).

Prop. (3.1.5.5).

- A category enriched in the Cartesian monoidal structure of the category of sets is just a usual category.
- A right-closed monoidal category is enriched over itself if we define \(\text{Map}(X, Y) = Y^X\). (Check).

Def. (3.1.5.6) [Tensored Category]. Let \(\mathcal{C}\) be a right-closed monoidal category and \(\mathcal{D}\) a category enriched over \(\mathcal{C}\), then \(\mathcal{D}\) is called tensored over \(\mathcal{C}\) if for any \(C \in \mathcal{C}\) and \(X \in \mathcal{D}\), there is an isomorphism of functors

\[
\eta : \text{Map}_\mathcal{D}(X, -)^C \cong \text{Map}_\mathcal{D}(X \otimes C, -).
\]

for some element \(X \otimes C \in \mathcal{D}\).

In particular, this implies \(\text{Hom}_\mathcal{C}(C, \text{Map}(X, Y)) \cong \text{Hom}_\mathcal{D}(X \otimes C, Y)\), thus \(X \otimes C\) is determined up to a unique isomorphism, and the map \((X, C) \mapsto X \otimes C\) defines a functor \(\mathcal{D} \times \mathcal{C} \to \mathcal{D}\) that there are natural morphisms

\[
X \otimes (C \otimes D) \cong (X \otimes C) \otimes D.
\]

Dually, if \(\mathcal{C}\) is left-closed and there is an object \(^C X\) that there is an isomorphism of functors

\[
^C \text{Map}(-, X) \cong \text{Map}(-, ^C X)
\]

then \(\mathcal{D}\) is called cotensored over \(\mathcal{C}\).

Proof: \(\square\)

Prop. (3.1.5.7). If \(\mathcal{C}\) is a right-closed monoidal category, then it is naturally tensored over itself, as defined in (3.1.5.5).
6 Others

Def. (3.1.6.1) [Compact Objects]. Fix a regular cardinal $\kappa$. Let $\mathcal{C}$ be a category that admits small colimits, and $J$ be a $\kappa$-filtered poset and a diagram $\{Y_\alpha\}$ indexed by $J$, then for $X \in \mathcal{C}$, there is a natural map

$$\lim \hom(X, Y_j) \to \hom(X, \lim Y_j).$$

$X$ is called $\kappa$-compact if this is an isomorphism for any $\kappa$-filtered diagram $J$. $X$ is called small if it is $\kappa$-compact for some small regular cardinal $\kappa$.

Def. (3.1.6.2) [Presentable Category]. Fix a regular cardinal $\kappa$, a regular category is a category $\mathcal{C}$ that satisfies:

- $\mathcal{C}$ admits all small colimits.
- $\mathcal{C}$ is generated by a small set $S$ of objects of $\mathcal{C}$ under small colimits.
- Any object of $\mathcal{C}$ is small.
- For $X,Y \in \mathcal{C}$, $\hom(X,Y)$ is small.

Remark (3.1.6.3). HTT Chap5.5 has a $\infty$-generalization of this notion.

Lifting Property and Small Object Argument

Def. (3.1.6.4) [lifting Properties]. Let $\mathcal{C}$ be a category and $p: A \to B, q: X \to Y$ be morphisms, then $p$ is said to have left lifting property w.r.t $q$ and $q$ is said to have right lifting property w.r.t $p$ if given any diagram

$$\begin{array}{ccc}
A & \to & X \\
\downarrow & & \downarrow \\
B & \to & Y
\end{array}$$

there is a dotted arrow completing the diagram.

For a set $A$ of morphisms of $\mathcal{C}$, let $l(A)$ denote the morphisms that have left lifting property w.r.t $A$ and $r(A)$ the morphisms that have right lifting property w.r.t $A$.

Def. (3.1.6.5) [Weakly Saturated Class]. Let $\mathcal{C}$ be a category with all small colimits, then a class of morphisms of $\mathcal{C}$ is called weakly saturated if it satisfies:

- Closed under pushout.
- Closed under transfinite composition: Let $\alpha$ be an ordinal and $\{D_\beta\}_{\beta<\alpha}$ be a system of objects in $\mathcal{C}_{C\downarrow}$ indexed by $\alpha$. For $\beta < \alpha$, let $D_{\leq \beta}$ be the colimit of system $\{D_\gamma\}_{\gamma<\beta}$ in $\mathcal{C}_{C\downarrow}$, then if each $D_{\leq \beta} \to D_\beta$ is in $S$, then $C \to D_{\leq \alpha}$ is in $S$.
- Closed under Retraction: In the category of morphisms of $\mathcal{C}$, if there is a morphism $F : f \to g, G : g \to f$ that $G \circ F = \text{id}$, and $g \in S$, then $f \in S$.

Cor. (3.1.6.6). The second condition implies all isomorphisms are in $S$, and $S$ is closed under composition.

Prop. (3.1.6.7) [Lifting and Retraction]. For a diagram $\begin{array}{ccc}
X & \to & X \\
\downarrow & & \downarrow \\
Z & \to & Y
\end{array}$ represents $p$ as a retraction of $u$, as the diagram $\begin{array}{ccc}
X & \to & Z \\
\downarrow & & \downarrow \\
Y & \to & Y
\end{array}$ shows.
Dually a diagram:

\[
\begin{array}{c}
X \xrightarrow{i} Y \\
\downarrow q \quad s \quad \downarrow f \\
Z \quad \quad Z \\
\end{array}
\]

represents \( q \) as a retraction of \( i \).

**Prop. (3.1.6.8) [Small Object Argument].** Let \( \mathcal{C} \) be a presentable category and \( A_0 = \{ \varphi_i : C_i \to D_i \} \) be a small collection of morphisms in \( \mathcal{C} \), then there is a morphism \( T : \mathcal{C}[1] \to \mathcal{C}[2] \) taking morphisms \( f : X \to Z \) in \( \mathcal{C} \) to the diagram

\[
\begin{array}{c}
Y \\
\downarrow f' \\
X \xrightarrow{f} Z
\end{array}
\]

That \( f' \) belongs to the weakly saturated class generated by \( A_0 \) and \( f'' \in r(A_0) \).

Moreover, if \( \kappa \) is a regular cardinal that each \( C_i, D_i \) is \( \kappa \)-compact, then \( T \) commutes with \( \kappa \)-filtered colimits.

**Proof:** Cf. [HTT, P788]. \( \square \)

**Lemma (3.1.6.9).** \( l(A) \) is weakly saturated for any set of morphisms \( A \)(Clear).

**Cor. (3.1.6.10) [Generated Weakly Saturated Class].** For any presentable category \( \mathcal{C} \) and \( A \) a set of morphisms in \( \mathcal{C} \), \( l(r(A)) \) is the smallest weakly saturated class of morphisms containing \( A \).

**Proof:** One direction of inclusion is by (3.1.6.9), for the other, if \( f : X \to Z \in l(r(A)) \), then there is a factorization \( X \xrightarrow{f'} Y \xrightarrow{f''} Z \), where \( f' \in A \) and \( f'' \in r(A) \), thus \( f \in l(f'') \), thus \( f \) is retraction of \( f' \):

\[
\begin{array}{c}
X \xrightarrow{f'} Y \\
\downarrow f' \quad g \quad f'' \quad \downarrow f'' \\
Z \quad \quad Z \quad Y \quad Z
\end{array}
\]

Thus \( f \in A \). \( \square \)

**Trees**

Cf. [HTT, Appendix]

**7 Fibered Categories**

**Categories of Categories**

**Def. (3.1.7.1) [2-Category of Categories over Categories].** There is a 2-category of categories over \( \mathcal{C} \), where the 1-morphisms are morphisms of categories over \( \mathcal{C} \) and the 2-morphisms are base-preserving natural transformations.

Two categories over \( \mathcal{C} \) are called **equivalent** if they are equivalent in this 2-category.

**Prop. (3.1.7.2) [2-Fibered Products in the Categories of Categories].** 2-fibered products exists in the categories of categories.

**Proof:** Let \( F : A \to \mathcal{C}, G : B \to \mathcal{C} \) be functors, then we can define a category \( A \times_\mathcal{C} B \) as follows:
3.1. CATEGORIES

- Objects are the triples \((A, B, f)\) where \(A \in \mathcal{A}, B \in \mathcal{B}\) and \(f : F(A) \rightarrow G(B)\) is an isomorphism in \(\mathcal{C}\).

- Morphisms from \((A, B, f)\) to \((A', B', f')\) are pairs \((a, b)\) where \(a : A \rightarrow A', b : B \rightarrow B'\) s.t. the diagram

\[
\begin{array}{ccc}
F(A) & \xrightarrow{f} & G(B) \\
\downarrow^{F(a)} & & \downarrow^{G(b)} \\
F(A') & \xrightarrow{f'} & G(B')
\end{array}
\]

is commutative.

\(\mathcal{A} \times_{\mathcal{C}} \mathcal{B}\) is a category both over \(\mathcal{A}\) and over \(\mathcal{B}\), and it fits into a 2-fiber products diagram

\[
\begin{array}{ccc}
\mathcal{A} \times_{\mathcal{C}} \mathcal{B} & \rightarrow & \mathcal{B} \\
\downarrow & & \downarrow \\
\mathcal{A} & \rightarrow & \mathcal{C}
\end{array}
\]

where the invertible 2-morphism is given by \(\psi_{(A,B,f)} = f : F(A) \rightarrow G(B)\).

The verification that this defines a final object in the 2-category of 2-commutative diagrams is in [Sta]02X9.

\(\square\)

Cor. (3.1.7.3). The 2-fibered product \(\mathcal{A} \times_{\mathcal{C}} \mathcal{B}\) is a groupoid iff \(\mathcal{A}, \mathcal{B}\) are all groupoids.

Prop. (3.1.7.4). Let \(\mathcal{A} \rightarrow \mathcal{C}, \mathcal{B} \rightarrow \mathcal{C}, \mathcal{C} \rightarrow \mathcal{D}\) be functors between categories, then there is a 2-fiber product diagram

\[
\begin{array}{ccc}
\mathcal{A} \times_{\mathcal{C}} \mathcal{B} & \rightarrow & \mathcal{A} \times_{\mathcal{D}} \mathcal{B} \\
\downarrow & & \downarrow \\
\mathcal{C} & \xrightarrow{\Delta_{\mathcal{C}/\mathcal{D}}} & \mathcal{C} \times_{\mathcal{D}} \mathcal{C}
\end{array}
\]

Proof: \(\square\)

Prop. (3.1.7.5) [2-Fibered Products of Categories]. The \((2,1)\)-category of categories over \(\mathcal{C}\) has 2-fiber products (3.1.3.5). More explicitly, suppose \(\mathcal{F} : \mathcal{X} \rightarrow \mathcal{S}, \mathcal{Y} \rightarrow \mathcal{S}\) be morphisms of categories over \(\mathcal{C}\), \(\mathcal{X} \times_{\mathcal{C}} \mathcal{Y}\) is given as follows:

- Objects of \(\mathcal{X} \times_{\mathcal{C}} \mathcal{Y}\) are quadruples \((U, x, y, f)\), where \(U \in \mathcal{C}, x \in \mathcal{X}_U, y \in \mathcal{Y}_U,\) and \(f : F(x) \rightarrow G(y)\) is an isomorphism in \(\mathcal{S}_U\).

- A morphism \((U, x, y, f) \rightarrow (U', x', y', f')\) is given by a pair \((a, b)\), where \(a : x \rightarrow x'\) is a morphism in \(\mathcal{X}\) and \(y \rightarrow y'\) is a morphism in \(\mathcal{Y}\) that
  - \(a, b\) induce the same morphism \(U \rightarrow U'\).
  - the diagram

\[
\begin{array}{ccc}
F(x) & \xrightarrow{f} & G(y) \\
\downarrow^{F(a)} & & \downarrow^{G(b)} \\
F(x') & \xrightarrow{f'} & G(y')
\end{array}
\]

is an isomorphism.
\(\mathcal{X} \times_S \mathcal{Y}\) is endowed with morphisms to \(\mathcal{X}\) and \(\mathcal{Y}\) over \(\mathcal{C}\) that the invertible 2-morphism giving the 2-commutativity is \(\psi_{(U,x,y,f)} : F(x) \to G(y)\).

The verification of the universal properties are similar to that of (3.1.7.2).

Cor. (3.1.7.6). There is an equivalence of fibre categories:

\[ (\mathcal{X} \times_S \mathcal{Y})_U \cong \mathcal{X}_U \times_{\mathcal{S}_U} \mathcal{Y}_U. \]

Fibered Categories

Def. (3.1.7.7) [(Co)Cartesian Arrows]. Let \(p : \mathcal{F} \to \mathcal{C}\) be a morphism, then a **Cartesian arrow** is an arrow \(\phi : C' \to C\) in \(\mathcal{F}\) that for any object \(C'' \in \mathcal{F}\) the map

\[ \text{Hom}(C'', C') \to \text{Hom}(C'', C) \times_{\text{Hom}(p(C''), p(C))} \text{Hom}(p(C''), p(C')) \]

is a bijection. A **coCartesian arrow** is an arrow that corresponds to a Cartesian diagram in \(\mathcal{F}^{\text{op}} \to \mathcal{C}^{\text{op}}\).

Prop. (3.1.7.8).

- If \(f\) is Cartesian, then \(f \circ g\) is Cartesian iff \(g\) is Cartesian.
- An arrow in \(\mathcal{F}\) whose image is an isomorphism is Cartesian iff it is itself an isomorphism.

Proof: Easy.

Def. (3.1.7.9) [Quasi-Fibration]. A functor \(F : \mathcal{C} \to \mathcal{D}\) is called a **quasi-fibration** if for any \(X \in \mathcal{C}\) and an isomorphism \(f : F(X) \cong Y\), there is an isomorphism \(\overline{f} : X \to Y\) mapping to \(f\).

Def. (3.1.7.10) [2-Category of Fibered Categories]. A **fibered category** over \(\mathcal{C}\) is a category over \(\mathcal{C}\) \(p : \mathcal{F} \to \mathcal{C}\) that for any \(\eta \in \mathcal{F}\) and an arrow \(f : U \to p(\eta)\), there is a Cartesian arrow \(\xi \to \eta\) in \(\mathcal{F}\) lifting \(f\). A **cofibered category** over \(\mathcal{C}\) is a category \(p : \mathcal{F} \to \mathcal{C}\) that the dual category \(p^{\text{op}} : \mathcal{F}^{\text{op}} \to \mathcal{C}^{\text{op}}\) is a fibered category.

A morphism of fibered categories over \(\mathcal{C}\) is a morphism of categories over \(\mathcal{C}\) that maps Cartesian morphisms to Cartesian morphisms. A 2-morphism of fibered categories is the same as a 2-morphism of categories over categories.

Def. (3.1.7.11) [Split Fibered Categories]. A **split fibered category** is a fibered category \(\mathcal{F} \to \mathcal{C}\) that comes from a functor \(\mathcal{C}^{\text{op}} \to \text{Cat}\).

Def. (3.1.7.12) [Cleavage]. A **cleavage** of a fibered category \(\pi : \mathcal{F} \to \mathcal{C}\) is a choice of Cartesian arrow \(f^*\) lifting \(f\) for any \(f \in \text{Arr}(\mathcal{C})\).

Lemma (3.1.7.13). Let \(F : \mathcal{F} \to \mathcal{G}\) be a morphism of fibered categories over \(\mathcal{C}\) that \(\mathcal{F}(U) \to \mathcal{G}(U)\) are fully faithful for any \(U \in \mathcal{C}\), then \(F\) is fully faithful.

Proof: To show \(F\) is fully faithful, it suffices to show for objects \(X, Y\) lying over \(U, V\), \(F\) induces a bijection of morphisms from \(x\) to \(y\) lying over a fixed \(f : U \to V\). Choose a Cartesian morphism \(f^*y \to y\) in \(\mathcal{S}_1\) lying over \(f\), then this induces a bijection between morphisms from \(x\) to \(y\) lying over \(f\) and \(\text{Hom}_{\mathcal{S}_1,U}(x, f^*y)\). Similarly, because \(F\) preserves Cartesian morphisms, we get a bijection between morphisms \(F(x) \to F(y)\) lying over \(f\) and \(\text{Hom}_{\mathcal{S}_2,U}(F(x), F(f^*y))\). Then the desired bijection follows from the hypothesis.
Prop. (3.1.7.14) [Equivalence of Fibered Categories]. Let \( F : \mathcal{F} \to \mathcal{G} \) be a morphism of fibered categories. Then \( F \) is an equivalence iff the restriction \( F_U : \mathcal{F}(U) \to \mathcal{G}(U) \) is an equivalence of categories for any object \( U \) of \( \mathcal{C} \).

Proof: One direction is trivial, for the other, the proof is similar to the fact essentially surjective+fully faithful implies equivalence.

Because \( F(U) \) are equivalences, for any object \( \xi \) of \( \mathcal{G} \) over \( U \), pick an object \( G\xi \) in \( \mathcal{F}(U) \) together with an isomorphism \( \alpha_\xi : \xi \cong F(G\xi) \). And for any morphism \( \xi \to \eta \), by (3.1.7.13), there is a unique arrow \( G\varphi : G\xi \to G\eta \) that \( F(G\varphi) = \alpha_\eta \circ \varphi \circ \alpha_\xi^{-1} \).

Thus clearly there is a 2-isomorphism \( \text{id}_\mathcal{G} \cong F \circ G \). It remains to construct an 2-isomorphism \( \text{id}_\mathcal{F} \cong G \circ F \): For any object \( \xi' \) over \( U \), since \( F(U) \) is fully faithful, there is a unique isomorphism \( \beta_{\xi'} : \xi' \cong G \circ F(\xi) \) in \( \mathcal{F}(U) \) that \( F\beta_{\xi'} = \alpha_{F\xi'} \). Then this is easily checked to be an 2-isomorphism \( \beta : \text{id}_\mathcal{F} \cong F \circ G \).

Prop. (3.1.7.15) [2-Fiber Products of Fibered Categories]. 2-fiber products exists in the category of fibered categories, and it coincides with that defined in (3.1.7.5).

Proof: it suffices to show for fibered categories \( \mathcal{X}, \mathcal{Y} \) over \( \mathcal{C} \), \( \mathcal{X} \times_\mathcal{C} \mathcal{Y} \) is also fibered over \( \mathcal{C} \). Let \((x,y,\varphi)\) be an object of \( \mathcal{X} \times_\mathcal{C} \mathcal{Y} \) mapping to \( U \in \mathcal{C} \) and \( f : V \to U \) is a morphism in \( \mathcal{C} \), choose Cartesian morphisms \( a : f^*x \to x \), \( b : f^*y \to y \) lying over \( f \), then \( F(a) \) and \( G(b) \) are Cartesian. Since \( \varphi : F(x) \to G(y) \) is an isomorphism, by the property of Cartesian morphisms, there exists a unique isomorphism \( f^*\varphi : F(f^*x) \to G(f^*y) \in \mathcal{S}_V \) that \( G(b) \circ f^*\varphi = \varphi \circ F(a) \). In other words, \( (F(a),F(b)) : (V,f^*x,f^*y,f^*\varphi) \to (U,x,y,\varphi) \) is a morphism in \( \mathcal{X} \times_\mathcal{S} \mathcal{Y} \).

The verification that this morphism is Cartesian is omitted.

Lemma (3.1.7.16). Let \( \mathcal{S} \to \mathcal{C} \) be a fibered category that factors through \( \mathcal{C}/U \) where \( U \in \mathcal{C} \), then \( \mathcal{S} \to \mathcal{C}/U \) is also a fibered category.

Proof: Cf.[[Sta]02XR].

Def. (3.1.7.17) [G-Equivariant Object]. Let \( G : \mathcal{C}^{op} \to (\text{Grp}) \) be a group functor and \( p_\mathcal{F} : \mathcal{F} \to \mathcal{C} \) a fibered category, and \( X \) an object of \( \mathcal{C} \) with an action of \( G \). A G-equivalent object of \( \mathcal{F}(X) \) is an object \( \rho \) of \( \mathcal{F}(X) \) that there is an action of \( G \circ p_\mathcal{F} \) on \( \rho \) and for any object \( U \) and \( \xi \in \mathcal{F}(U) \), the function \( p_\mathcal{F} : \text{Hom}_\mathcal{F}(\xi,\rho) \to \text{Hom}_\mathcal{C}(U,\rho) \) is \( G(U) \)-equivariant.

The category \( \mathcal{F}^G(X) \) of \( G \)-equivariant objects of \( \mathcal{F}(X) \) consisting of \( G \circ p_\mathcal{F} \)-equivariant morphism of \( G \)-equivariant objects.

Prop. (3.1.7.18). Let \( \pi_2 \) is the projection \( G \otimes X \to X \), \( \rho \) be an object of \( \mathcal{F}(X) \), then a \( G \)-equivariant structure on \( \rho \) is the same as a Cartesian arrow \( \beta : \pi_2^*\rho \to \rho \) that \( p_\mathcal{F}\beta = \alpha \), and satisfies the desired commutative diagram corresponding to \( (gh)x = g(h(x)) \). And a morphism of \( G \)-equivariant objects just corresponds to a morphism of pairs \( (\rho,\beta) \).

Proof: Cf.[Vistoli, P68].

Def. (3.1.7.19) [Presheaf of Arrows]. Let \( \mathcal{F} \) be a fibered category over \( \mathcal{C} \), and \( \xi,\eta \in \mathcal{F}(S) \), then we can define a quasi-functor \( \text{Hom}_S(\xi,\eta) \to (\mathcal{C}/S) \), where

\[
\text{Hom}_S(\xi,\eta)(U/S) = \{(\xi_1 \to \xi, \eta_1 \to \eta, \varphi)\}
\]
where $\xi_1 \to \xi, \eta_1 \to \eta$ are Cartesian arrows over $U \to S$, and $\varphi : \xi_1 \to \eta_1 \in \mathcal{F}(U)$. The arrows in $\text{Hom}_S(\xi, \eta)$ are uniquely defined by the property of Cartesian arrows. Then it is a quasi-functor, by (3.1.7.30).

Then it is equivalence to a presheaf $\text{Hom}_S(\xi, \eta)$, by (3.1.7.31). Equivalently, this presheaf can be defined by designating a choice of Cartesian arrows.

**Prop. (3.1.7.20)** [Splitting a Fibered Category]. Let $\mathcal{F} \to \mathcal{C}$ be a fibered category, then there exists a canonically defined split fibered category $\tilde{\mathcal{F}} \to \mathcal{C}$ with a canonical equivalence of fibered categories $\tilde{\mathcal{F}} \to \mathcal{F}$ over $\mathcal{C}$.

**Proof:** There is a functor $\mathcal{C}^{\text{op}} \to \text{Cat} : U \mapsto \text{Hom}(h_U, \mathcal{F})$, with corresponds to a split fibered category $\tilde{\mathcal{F}}$. There is an obvious morphism $\tilde{\mathcal{F}} \to \mathcal{F}$, sending an object $\varphi : h_U \to \mathcal{F}$ to $\varphi(\text{id}_U) \in \mathcal{F}(U)$. And for any $f : U \to V \in \mathcal{C}$ and a $\varphi : h_U \to \mathcal{F}$, we send $f^*\varphi \to \varphi \in \tilde{\mathcal{F}}$ to $\varphi(f : V/U \to U/U) \in \mathcal{F}$, Then we get a canonical map of fibered categories $\tilde{\mathcal{F}} \to \mathcal{F}$ over $\mathcal{C}$. It is an equivalence of categories by (3.1.7.14) and (3.1.7.33). □

**Categories Fibered in Groupoids, Sets and Equivalence Relations**

**Def. (3.1.7.21)** [Category Fibered in Groupoids]. A category (co)fibered in groupoids/setoids/equivalence relations over $\mathcal{C}$ is a category $\mathcal{F}$ (co)fibered over $\mathcal{C}$ that $\mathcal{F}(U)$ is a groupoid/setoids/equivalence relations for any $U \in \mathcal{C}$. Also we call a category fibered in equivalence relations over $\mathcal{C}$ a quasi-functor.

**Prop. (3.1.7.22)** [Characterization of Category Fibered in Groupoids]. Let $\mathcal{F}$ be a category over $\mathcal{C}$, then $\mathcal{F}$ is fibered over groupoids over $\mathcal{C}$ iff

- Every morphism in $\mathcal{F}$ is Cartesian.

- Given any $\eta \in \mathcal{F}, U \in \mathcal{C}$ and a morphism $f : U \to p_{\mathcal{F}}(\eta)$, there is an arrow $\varphi : \xi \to \eta \in \mathcal{F}$ mapping to $f$.

And dually for cofibered categories.

**Proof:** If these two holds, then $\mathcal{F}$ is clearly fibered over $\mathcal{C}$, and for any arrow $f : \xi \to \eta$ in $\mathcal{F}(U)$, there is a morphism $g : \eta \to \xi$ that is right inverse to $f$, then clearly it is the inverse.

Conversely, if $\mathcal{F}$ is fibered over $\mathcal{C}$, it suffices to check1: for any arrow $f$, the image in $\mathcal{C}$ can be lifted to a Cartesian diagram in $\mathcal{F}$, and differs $f$ by an isomorphism, thus $f$ is also Cartesian by (3.1.7.8). □

**Cor. (3.1.7.23).** if $\mathcal{A}$ is a category fibered in groupoids over $\mathcal{B}$ and $\mathcal{B}$ is a category fibered in groupoids over $\mathcal{C}$, then $\mathcal{A}$ is a category fibered in groupoids over $\mathcal{C}$.

**Prop. (3.1.7.24)** [Associated Category Fibered in Groupoids]. Let $\mathcal{F} \to \mathcal{C}$ be a fibered category, then the associated category fibered in groupoids $\mathcal{F}_{\text{cart}}$ is the category obtained by deleting all the non-Cartesian arrows. Then $\mathcal{F}_{\text{cart}}$ is a category fibered in groupoids over $\mathcal{C}$.

**Proof:** Firstly $\mathcal{F}_{\text{cart}}$ is a category by (3.1.7.8), and it is a category fibered in groupoids by (3.1.7.22). □

**Def. (3.1.7.25)** [Rigid Fibered Categories]. A rigid fibered category is a fibered category whose associated category fibered groupoids is fibered in setoids. Equivalently, there are no isomorphisms above any id$_U$. 


Prop. (3.1.7.26) [2-Fibered Products of Categories Fibered in Groupoids]. The 2-fibered products of categories fibered in groupoids over $\mathcal{C}$ is a category fibered in groupoids over $\mathcal{C}$.

Proof: The 2-fibered products exist by (3.1.7.15), and using (3.1.7.6), it is fibered in groupoids because the 2-fibered products of groupoids is a groupoid by (3.1.7.3). □

Prop. (3.1.7.27) [Characterization of Categories Fibered in Setoids]. Let $\mathcal{F}$ be a category over $\mathcal{C}$, then $\mathcal{F}$ is fibered in setoids over $\mathcal{C}$ iff for any object $\eta$ of $\mathcal{F}$ and an arrow $f : U \rightarrow p\mathcal{F}\eta \in \mathcal{C}$, there is a unique arrow $\xi \rightarrow \eta$ mapping to $f$.

Proof: Let $\mathcal{F}$ be a category fibered in sets, then pick a Cartesian arrow $\tilde{f}$ over $f$, then any other lifting factors through this lifting by the property of Cartesian, then it is identity, because $\mathcal{F}(U)$ is a setoid.

Conversely, if the hypothesis holds, then clearly $\mathcal{F}(U)$ is a setoid, and the fibered category condition holds, because of the uniqueness. □

Cor. (3.1.7.28) [Presheaves and Categories Fibered in Setoids]. Let $\mathcal{C}$ be a category, then categories fibered in setoids over $\mathcal{C}$ are exactly those equivalent to a presheaf over $\mathcal{C}$.

Cor. (3.1.7.29). In particular, for any object $X \in \mathcal{C}$, the presheaf $h_X$ determines a category fibered in sets, which is just the comma category $\mathcal{C}/X \rightarrow \mathcal{C}$.

Prop. (3.1.7.30) [Characterization of Quasi-Functors]. A category $\mathcal{F}$ over $\mathcal{C}$ is a quasi-functor iff:

- Given any object $\eta \in \mathcal{F}$ and an arrow $f : U \rightarrow p\mathcal{F}\eta$, there is a lifting $\xi \rightarrow \eta$ mapping to $f$. And given any two such extensions, there is a morphism $\xi' \rightarrow \xi$ commuting them.

- Given any two objects $\xi, \eta \in \mathcal{F}$ and an arrow $f : p\mathcal{F}\xi \rightarrow p\mathcal{F}\eta$, there is at most one arrow $\tilde{f} : \xi \rightarrow \eta$ lifting $f$.

Proof: □

Prop. (3.1.7.31). A fibered category over $\mathcal{C}$ is a quasi-functor iff it is equivalent to a presheaf.

Proof: If it is equivalent to a functor, then $\mathcal{F}(U)$ is equivalent to a setoid, thus it is an equivalent relation, by (3.1.1.15). Conversely, if $\mathcal{F}$ is a quasi-functor, then it is fibered in groupoids, thus by (3.1.7.22) every morphism is Cartesian, and if we denote $\Phi(U)$ the equivalence classes of $\mathcal{F}(U)$, then a morphism $U \rightarrow V$ will induce a morphism $\Phi(V) \rightarrow \Phi(V)$ by the property of Cartesian arrows. Then clearly this defines a presheaf that is equivalent to $\mathcal{F}$. □

Representability

Def. (3.1.7.32) [Representable Fibered Category]. A fibered category is called representable if it is equivalent to the fibered category $\mathcal{C}/X$ defined in (3.1.7.29) for some $X \in \mathcal{C}$.

Prop. (3.1.7.33) [2-Categorical Yoneda Lemma]. Let $\mathcal{F}$ be a fibered category over $\mathcal{C}$ and $X \in \mathcal{C}$, there is an equivalence of categories:

\[
\text{Hom}_{\mathcal{C}}((\mathcal{C}/X), \mathcal{F}) \cong \mathcal{F}(X) : \varphi \mapsto \varphi(\text{id}_X)
\]
Proof: To show this functor is essentially surjective, choose a choice of pullbacks of $\mathcal{F}$, for any $\xi \in \mathcal{F}(X)$, we define a $F : \mathcal{C}/X \rightarrow \mathcal{F}$ that maps a $\varphi : U \rightarrow X$ to $\varphi^*\xi$, and to any morphism in $\mathcal{C}/X$ an arrow in $\mathcal{F}$ induced by Cartesian property.

To show it is fully faithful, notice a natural transformation of $\varphi, \psi \in \text{Hom}_\mathcal{C}((\mathcal{C}/X), \mathcal{F})$ is determined by their value on $\text{id}_X$, and any map $\varphi(\text{id}_X) \rightarrow \psi(\text{id}_X)$ induces a natural transformation, by Cartesian properties. □

Cor.(3.1.7.34) [Characterization of Representability]. Translating the 2-Yoneda lemma and (3.1.7.14), we see that a fibered category $\mathcal{F}$ is representable by $X \in \mathcal{C}$ iff $\mathcal{F}$ is fibered in groupoids, and there is an object $\xi \in \mathcal{F}(X)$ that for any object $\rho \in \mathcal{F}$, there is a unique arrow $\rho \rightarrow \xi$.

Cor.(3.1.7.35). If $\mathcal{X}, \mathcal{Y}$ are fibered categories over $\mathcal{C}$ representable by $U, V$ resp., then there is an isomorphism of sets

$$\text{Hom}_\mathcal{C}(\mathcal{X}, \mathcal{Y})/2 \sim \text{Hom}_\mathcal{C}(U, V)$$

Proof: By Yoneda lemma there is an equivalence $\text{Hom}_\mathcal{C}(\mathcal{X}, \mathcal{Y}) \cong \text{Hom}_\mathcal{C}(U, V)$, and then $\text{Hom}_\mathcal{C}(\mathcal{X}, \mathcal{Y})$ is an equivalence relation by (3.1.1.15), so the isomorphism is clear. □

Def.(3.1.7.36) [Representable 1-Morphisms]. Let $\mathcal{C}$ be a category and $F : \mathcal{X} \rightarrow \mathcal{Y}$ be a morphism of categories fibered over $\mathcal{C}$, then $F$ is called representable if for any $U \in \mathcal{C}$ and a morphism $\mathcal{C}/U \rightarrow \mathcal{Y}$, the fibered category $(\mathcal{C}/U) \times_\mathcal{Y} \mathcal{X} \rightarrow \mathcal{C}/U$ is representable (3.1.7.32)(Notice it is a fibered category by (3.1.7.15) and (3.1.7.16)).

Prop.(3.1.7.37) [Diagonal and Representability]. Let $\mathcal{S}$ be a category fibered in groupoids over $\mathcal{C}$. Assume $\mathcal{C}$ has fibered product, then the following are equivalent:

- $\Delta_S : \mathcal{S} \rightarrow \mathcal{S} \times_\mathcal{C} \mathcal{S}$ is representable.

- For every $U \in \mathcal{C}$, any $G : \mathcal{C}/U \rightarrow \mathcal{S}$ is representable.

Proof: Cf.[[Sta]02YA].

The key to this proposition is the fibered product diagram (3.1.7.15)(3.1.1.48)

$$
\begin{array}{c}
X \times F Y \rightarrow \mathcal{F} \\
\downarrow \\
X \times S Y \rightarrow \mathcal{F} \times_\mathcal{S} \mathcal{F}
\end{array}
$$

which still holds in the 2-commutative sense.

So if $\Delta_\mathcal{F}$ is schematic, then $X \times F Y$ is a scheme, so $X \rightarrow \mathcal{F}$ is schematic, for any scheme $X$.

Conversely, consider the fibered products

$$
\begin{array}{c}
\mathcal{F} \times F \times S \mathcal{F} \rightarrow \mathcal{F} \\
\downarrow \\
X \rightarrow \mathcal{F} \times S \mathcal{F}
\end{array}
$$

induced by $h = f \times g : X \rightarrow \mathcal{F} \times S \mathcal{F}$. So in order to prove $\Delta_\mathcal{F}$ is schematic, it suffices to prove $\mathcal{F} \times F \times S \mathcal{F} X$ is a scheme, and for this, it suffices to prove $X \times F X$ is a scheme. But $X \times F X \rightarrow X$ is a pullback of $X \rightarrow F$, so it is a scheme. □
3.2 Categorical Logic

Main references are [Categorical Logic Notes, Jacob Lurie], [Coend Calculus, Fosco Loregian], [Harder-Narasimhan Filtrations, Huayi Chen], [Harder-Narasimhan Theory, Jonathan Pottharst], [Coend Calculus].

1 Monads and Categories

Def. (3.2.1.1)[Monad]. Let \( C \) be a category, a monad on \( C \) is an endofunctor \( C \to C \) together with two natural morphisms:

- (multiplication) \( \mu : T \circ T \to T \).
- (unit) \( \text{id}_C \to T \).

that satisfies associativity and unit diagrams.

Def. (3.2.1.2)[Algebras over Monads]. An algebra over a monad \( T \) is an object \( X \) together with a morphism \( \alpha : TX \to X \) that satisfies the diagrams for an algebra.

2 Group Formation

The goal of this subsection is to give a formation that encompass both the group theory and algebraic group theory.

Def. (3.2.2.1)[Group Formations]. A group formation is a small category \( C \) with a class of arrows \( S \in C \) consisting of monomorphisms, satisfying the following axioms:

- \( G \) is complete and cocomplete.
- \( G \) has a zero object \( e \).
- \( S \) is stable under pullbacks.
- If \( N \to H \to G \in S \) and \( H \to G \) is a monomorphism, then \( N \to H \in S \).
- Let \( N \to G \in S \), then \( N \) is called a normal subobject of \( G \), and \( N = \ker(G \to \text{Coker}(N \to G)) \).
- For \( G \in C \), coproducts exist in \( C/G \), and if \( N \to G, H \to G \in S \), then the coproduct is also in \( S \), denoted by \( NH \to G \).
- Let \( N \to G \in S \) and \( H \to G \) a monomorphism, then
  - there is a natural isomorphism: \( H/N \cap H \cong HN/N \).
  - If \( N \to G \in S \), then there is a natural isomorphism \( G/NH \cong (G/N)/(H/H \cap N) \).

Prop. (3.2.2.2).

3 Filtrations of a Category

Def. (3.2.3.1)[Filtrations in a Category]. Let \( C \) be a category with an initial object, a filtration of an object \( X \) in \( C \) is a family \( \mathcal{F} = (X_t)_{t \in \mathbb{R}} \) of subobjects of \( X \) indexed by \( \mathbb{R} \) that satisfies:

- (decreasing property) if \( s \leq t \), then \( X_s \to X \) factors through \( X_t \).
- (separation property) for sufficiently small \( t \), \( X_t \) is the initial object.
• (exhaustiveness) for sufficiently large $s$, $X_s = X$.

• (right locally constant property) for any $t \in \mathbb{R}$, there exists $\delta > 0$ that for any $s \in [t, t + \delta)$, the morphism $X_t \to X$ are isomorphisms.

• (finite jump) the jump set of $\mathcal{F}$ is finite.

Naturally, we define morphisms of filtrations.

Def.(3.2.3.2)[Pullback and Pushforward Filtrations]. Suppose fibered products exist in $\mathcal{C}$, for any morphism $f : X \to Y$ and a filtration $\mathcal{G} = (Y_t) \to Y$, then the family $f^* \mathcal{G} = (Y_t \otimes_Y X) \to X$ is a filtration on $X$, called the pullback filtration.

If $f : X \to Y$ and $\mathcal{F} : (X_t) \to X$ is a filtration on $X$, then if there is a filtration $f_* \mathcal{F}$ on $Y$ and a morphism of filtrations $\mathcal{F} \to f_* \mathcal{F}$ compatible with $f$, then $f_* \mathcal{F}$ is called the pushforward filtrations.

4 Harder-Narasimhan Formalism

Main references are[Jon20].

Def.(3.2.4.1)[Harder-Narasimhan Formalism]. A Harder-Narasimhan formalism consists of

• An exact category $\mathcal{C}$ (3.3.1.17).

• A function $\text{deg} : \text{Ob}(\mathcal{C}) \to \mathbb{Z}$ that is additive w.r.t. short exact sequences.

• An exact faithful generic fiber functor to an Abelian category $F : \mathcal{C} \to \mathcal{A}$ that induces for each object $F : \mathcal{E} \in \mathcal{C}$ a bijection

\[
\{\text{strict objects of } \mathcal{E}\} \cong \{\text{subobjects of } F(\mathcal{E})\}
\]

where a strict subobject is an object that can be prolonged to an exact sequence.

• An additive function rank: $\mathcal{A} \to \mathbb{N}$ on $\mathcal{A}$ that $\text{rank}(\mathcal{L}) = 0 \iff \mathcal{L} = 0$, and its composition with $F$ is also called rank.

• If $u : \mathcal{E} \to \mathcal{E}'$ is a morphism in $\mathcal{C}$ that $F(u)$ is an isomorphism, then $\text{deg}(\mathcal{E}) \leq \text{deg}(\mathcal{E}')$ with equality iff $u$ is an isomorphism.

Cor.(3.2.4.2).

• We are free to choose the "kernel" for $u$ that $F(u)$ is surjection.

• The subobjects of subobjects are subobjects, by axiom3.

Def.(3.2.4.3)[Saturation]. Let $X'$ be a subobject of $X$, then we let $\tilde{X}'$ denote the strict subobject of $X$ corresponding to the subobject $F(X')$ of $F(X)$, called the saturation of $X'$. The saturation satisfies:

• 

• 

•


Prop.(3.2.4.4). Every morphism $f : X \to Y$ has a kernel and a image in $\mathcal{C}$, and $0 \to \ker f \to X \to \text{Im } f \to 0$ is an exact sequence.
Prop. (3.2.4.5) [HN-Formalism on the Category of Filtered Vector Spaces]. If \( L/K \) is a field extension, there is a category \( \text{VectFil}_{L/K} \) consisting of \( (V, \text{Fil}) \) where \( V \) is a \( K \)-vector space and \( \text{Fil} \) is a finite filtration on \( V \otimes_K L \). It is an exact category by declaring exact sequences be those induce exact sequences on the graded.

The generic fiber functor is \( \text{VectFil}_{L/K} \to \text{Vect}_K \): \((V, \text{Fil}) \mapsto V\), and rank is as usual, the **Hodge-Tate degree** is defined to be \( t_H((V, \text{Fil})) = \sum i \dim_K gr^i(V \otimes_K L) \). This is a HN-filtration.

**Proof:** The axioms can be directly checked, notice a filtration \( W_n \) of a filtration \( V_n \) is a strict object iff \( W_k = W_n \cap V_k \).

\[ \square \]

Def. (3.2.4.6) [Slope]. In a HN-formalism, the **slope** is defined to be \( \text{slope}(E) = \frac{\deg(E)}{\text{rank}(E)} \).

\( E \) is called **semistable of slope** \( \lambda \) iff \( \text{slope}(E) = \lambda \), and \( \text{slope}(E') \leq \lambda \) for any nonzero strict subobject \( E' \subset E \).

Prop. (3.2.4.7). If \( 0 \to E' \to E \to E'' \to 0 \) be a short exact sequence in \( \mathcal{C} \), then:

- If two of them have the same slope, then so does the third.
- If two of them have different slope, then we know the ordering of these slopes.

**Proof:** Just notice that the degree and rank are all additive functions.

\[ \square \]

Prop. (3.2.4.8). If \( E \) is semistable of slope \( \lambda \), then for any morphism \( u: E \to E'' \) that \( F(u) \) is surjective, \( \mu(E'') \geq \lambda \).

**Proof:** Take the kernel of \( F(u) \) in \( \mathcal{A} \), which corresponds to a strict object \( E' \) of \( E \), and \( 0 \to E' \to E \to E'' \to 0 \) is exact, so we can use (3.2.4.19).

\[ \square \]

Cor. (3.2.4.9). If \( E, F \) are semistable of slopes \( \lambda > \mu \), then \( \text{Hom}_\mathcal{C}(E, F) = 0 \).

**Proof:** Notice \( F \) is faithful.

\[ \square \]

Prop. (3.2.4.10) [Semistable Objects]. If \( f: E \to F \) be a map of vector bundles of the same slope \( \lambda \), then \( \ker(f) \) and \( \text{Coker}(f) \) are all semistable vector bundles of slope \( \lambda \), and if \( 0 \to E' \to E \to E'' \to 0 \) is exact and \( E', E'' \) are semistable of slope \( \lambda \), then so does \( E \).

**Proof:** Use \( F(f) \) to find the "coimage" \( A \) and the "image" \( B \) of \( f \), then there is a map from \( F(A) \) to \( F(B) \) which is an isomorphism, but they have the same degree and rank, thus \( A \cong B \) by the last axiom. And the image must has slope \( \lambda \). Then \( \ker(f), \text{Coker}(f) \) all can be defined, and they have the same slope \( \lambda \) by (3.2.4.19).

\( \ker(f) \) is semistable because strict subobjects of \( \ker(f) \) are also strict subobjects of \( E \) (3.2.4.2).

And for \( \text{Coker}(f) \), if it is not semistable, choose \( F' \subset \text{Coker}(f) \) that has slope \( \lambda \), let \( F'' \) be the inverse image, then \( 0 \to \text{Im}(f) \to F' \to F'' \to 0 \), then by (3.2.4.19) slope \( F'' \) > \( \lambda \), contradicting the semi-stability of \( F \).

For the extension, \( \text{slope}(E) = \lambda \) by (3.2.4.19), and for a strict subobject \( F \) of \( E \), then we can find \( F', F'' \) be strict objects of \( E', E'' \) respectively that there is an exact sequence \( 0 \to F' \to F \to F'' \to 0 ? \), which shows \( \text{slope}(F) \leq \lambda \), so \( E \) is semistable.

\[ \square \]


**Harder-Narasimhan Filtration**

**Lemma (3.2.4.11)** [Final Subobjects of Maximal Slope]. Let \( X \) be an object of \( \mathcal{C} \) and \( X', X'' \) its subobjects of maximal slope, then \( X' + X'' \) and \( X' \cap X'' \) are also of maximal slope.

**Proof:** Cf. [Jon20] P8. \( \square \)

**Def. (3.2.4.12).** Given an object \( X \) of \( \mathcal{C} \), consider the following condition on a nonzero subobject \( X' \) of \( X \):

For all subobjects \( X'' \) of \( X \) properly containing \( X' \), \( \mu(X'') < \mu(X') \).

**Def. (3.2.4.13)** [SCSS]. Let \( X' \) be a subobject of \( X \), then the following conditions are equivalent:

- \( X' \) satisfies condition (3.2.4.12) and is semistable.
- \( X' \) satisfies condition (3.2.4.12) and is of maximal slope.
- \( X' \) is the final object of \( X \) of maximal slope.

If \( X' \) satisfies these equivalent conditions and \( X' \neq X \), then \( X \) is called a **strongly contradicting semi-stability** or SCSS of \( X \).

**Proof:** Cf. [Jon20] P8. \( \square \)

**Prop. (3.2.4.14).** Every object \( X \) of \( \mathcal{C} \) admits a SCSS.

**Def. (3.2.4.15)** [Harder-Narasimhan Filtration]. Let \( \mathcal{E} \in \mathcal{C} \), a chain of strict objects \( 0 \subset \mathcal{E}_0 \subsetneq \mathcal{E}_1 \subsetneq \ldots \subsetneq \mathcal{E}_m = \mathcal{E} \) is called a **Harder-Narasimhan filtration** iff each quotient \( \mathcal{E}_i/\mathcal{E}_{i-1} \) is semistable of slope \( \lambda_i \) and \( \lambda_1 > \lambda_2 > \ldots > \lambda_m \).

**Prop. (3.2.4.16).** Every object \( \mathcal{E} \in \mathcal{C} \) has a unique functorial Harder-Narasimhan filtration.

**Proof:** For uniqueness: if there are two filtrations, it suffices to show that \( \mathcal{E}'_1 = \mathcal{E}_1 \), because notice by (3.2.4.2) \( \mathcal{E}_i \) is a strict subobjects of \( \mathcal{E}_j \) for any \( i < j \), so we finish by induction on the length of the filtration and considering \( \mathcal{E}/\mathcal{E}_1 \).

For this, firstly \( \lambda_1 = \lambda'_1 \), suppose the contrary and \( \lambda_1 > \lambda'_1 \), then \( \lambda_1 > \lambda'_i \) for each \( i \), so \( \text{Hom}(\mathcal{E}_1, \mathcal{E}_i/\mathcal{E}_{i-1}) = 0 \) for each \( i \) by (3.2.4.32), so by induction \( \text{Hom}(\mathcal{E}_1, \mathcal{E}) = 0 \), contradiction.

Next by the same reason as in the proof above, \( \mathcal{E}_1 \hookrightarrow \mathcal{E} \) has image in \( \mathcal{E}_1' \), and the reverse is true for \( \mathcal{E}_1' \), so \( \mathcal{E}_1 \cong \mathcal{E}_1' \) in \( \mathcal{E} \).

For existence: Use induction on \( \text{rank}(\mathcal{E}) \). If \( \mathcal{E} \) is semistable, then we finish. Otherwise, there is a strict subobject \( \mathcal{F} \) and \( 0 \to \mathcal{F} \to \mathcal{E} \to \mathcal{G} \to 0 \) that \( \text{slope}(\mathcal{F}) > \text{slope}(\mathcal{E}) \), so \( \text{rank}(\mathcal{F}) < \text{rank}(\mathcal{E}) \). Now by induction \( \mathcal{F} \) and \( \mathcal{G} \) has HN-filtration, thus by argument as above, we see that \( \mathcal{E} \) cannot have strict subobject with slope bigger than slopes appearing in the HN-filtration of \( \mathcal{F}, \mathcal{G} \). So if we choose a strict subobject of \( \mathcal{E}_1 \) of maximal rank among the strict subobjects of maximal slope, we claim the subobjects of \( \mathcal{E}/\mathcal{E}_1 \) all have slopes smaller than \( \text{slope}(\mathcal{E}_1) \): if some \( \text{slope}(\mathcal{G}) \geq \text{slope}(\mathcal{E}_1) \), consider its inverse image \( \mathcal{G}' \), then \( 0 \to \mathcal{E}_1 \to \mathcal{G}' \to \mathcal{G} \to 0 \), thus \( \text{slope}(\mathcal{G}') \geq \text{slope}(\mathcal{E}_1) \) and has bigger rank, contradiction. So we can use induction on \( \mathcal{E}/\mathcal{E}_1 \). \( \square \)

**HN-Polygons**

**Harder-Narasimhan Categories**

This subsection is unnecessary. Main references are [Harder-Narasimhan Categories]
Def. (3.2.4.17) [Harder-Narasimhan Categories]. A **Harder-Narasimhan category** consists of a geometric exact category $\mathcal{C}$ that is additive w.r.t short exact sequences in $\mathcal{E}_A$.

1. A function $\deg : \text{Ob}(\mathcal{C}) \to \mathbb{R}$ that is additive w.r.t short exact sequences in $\mathcal{E}_A$.
2. A function $\text{rank} : \text{Ob}(\mathcal{C}) \to \mathbb{N}$ on $\mathcal{A}$ that is additive w.r.t short exact sequences in $\mathcal{E}$, $\text{rank}(X) = 0 \iff X = 0$.

The **slope** of a nonzero object $X$ is defined to be $\mu(X) = \deg(X)/\text{rank} X$. And $X$ is called **semistable** if $\mu(X) = \lambda$, and $\mu(X') \leq \lambda$ for any nonzero geometric subobject $X' \subset X$.

And the category satisfies the following axiom:

- **NH**: For any nonzero geometric object $X$, there exists a geometric subobject $X_{\text{des}} \subset X$ that
  \[
  \mu(X_{\text{des}}) = \sup\{\mu(Y) | Y \text{ is a non-zero geometric subobject of } X\}
  \]

  and moreover, any nonzero geometric subobject $Z$ of $X$ that $\mu(Z) = \mu(X_{\text{des}})$ is a geometric subobject of $X_{\text{des}}$.

Notice that $X_{\text{des}}$ is semistable and unique up to isomorphisms, called the **destablization** of $X$.

Cor. (3.2.4.18). A geometric object of rank 1 is semistable.

**Proof**: For any nonzero geometric subobject $X' \subset X$, rank $X' = \text{rank} X = 1$, so rank $X/X' = 0$ hence $X/X' = 0$ and $X' \cong X$. Then clearly $\mu(X') = \mu(X)$ and $X$ is semistable. \hfill $\square$

Cor. (3.2.4.19). If $0 \to \mathcal{E}' \to \mathcal{E} \to \mathcal{E}'' \to 0$ be a short exact sequence in $\mathcal{E}_A$, then:

- If two of them have the same slope, then so does the third.
- If two of them have different slope, then we know the ordering of these slopes.

**Proof**: Just notice that the degree and rank are all additive functions. \hfill $\square$

Prop. (3.2.4.20) [Abelian Categories as Harder-Narasimhan Categories]. Let $(\mathcal{C}, \mathcal{E}, \mathcal{A})$ be a geometric exact category with functions $\deg$ and $\text{rank}$, and $\mathcal{C}$ is an Abelian category, $\mathcal{E}$ is the set of short exact sequences, then $(\mathcal{C}, \mathcal{E}, \mathcal{A}, \deg, \text{rank})$ is a Harder-Narasimhan category.

**Proof**: We need to check HN: induct on rank $X$: The condition is clear when $X$ is semistable, in particular when rank $X = 1$ (3.2.4.18), and when $X$ is not semistable, let $Y$ be a geometric subobject of $X$ that $\mu(X') > \mu(X)$ and rank $X'$ is maximal, then by induction hypothesis, there is a destablization $Y_{\text{des}}$, and we want to show $X'_{\text{des}}$ is just $X_{\text{des}}$: Let $Y$ be a nonzero geometric subobject of $X$. If $Y$ is a geometric subobject of $X'$, then $\mu(Y) \leq \mu(X'_{\text{des}})$. If $Y$ is not a geometric subobject of $X'$, then $Y + X'$ is greater than $X'$, and rank$(Y + X') >$ rank $X'$, so by maximality, $\mu(Y + X') \leq \mu(X) < \mu(X')$. Moreover, there is an exact sequence

\[
0 \to Y \cap X' \to Y \oplus X' \to Y + X' \to 0
\]

so

\[
\deg Y = \deg(Y \cap X') + \deg(Y + X') - \deg(X')
\]

\[
< \mu(X'_{\text{des}}) \text{rank}(Y \cap X') + \mu(X')(\text{rank}(Y + X') - \text{rank}(X'))
\]

\[
\leq \mu(X'_{\text{des}})(\text{rank}(Y \cap X') + \text{rank}(Y + X') - \text{rank}(X'))
\]

\[
= \mu(X'_{\text{des}})\text{rank}(Y).
\]

In particular, if $\mu(Y) = \mu(X'_{\text{des}})$, then $Y$ must be a geometric subobject of $X'$ hence a geometric subobject of $X'_{\text{des}}$, so HN holds for $X$. \hfill $\square$
**Prop. (3.2.4.21) [Harder-Narasimhan Filtration].** Let \( X \) be a nonzero geometric object, a chain of admissible monomorphisms \( 0 = X_0 \to X_1 \to \ldots \to X_m = X \) is called a **Harder-Narasimhan filtration** of \( X \) iff each quotient \( \mathcal{E}_i/\mathcal{E}_{i-1} \) are all semistable of slope \( \lambda_i \) and \( \lambda_1 > \lambda_2 > \ldots > \lambda_m \), called the slopes associated to \( X \).

**Prop. (3.2.4.22) [Harder-Narasimhan Filtrations Exist].** Let \( (\mathcal{C}, \mathcal{E}, A, \text{deg}, \text{rank}) \) be a Harder-Narasimhan category, then the Harder-Narasimhan filtration exists for any nonzero geometric object \( X \).

**Proof:** We induct on the rank of \( X \): if \( X \) is semistable, this is clear, so we are done in the case \( \text{rank} X = 1 \) by (3.2.4.18). We choose \( X_1 = X_{\text{des}} \), then \( X_{\text{des}} \) is semistable and \( X' = X/X_{\text{des}} \neq 0 \). Now \( \text{rank} X' < \text{rank} X \), we can apply induction hypothesis to obtain a HN-filtration \( 0 = X'_1 \xrightarrow{f'_1} X'_2 \to \ldots \to X'_{n-1} \xrightarrow{f'_{n-1}} X'_{n} = X' \). Now let \( X_i = X \times_X X'_i \) (exists by Ex6 (3.3.1.17)), then \( X_1 = X_{\text{des}} \).

Since \( X \to X' \) is an admissible epimorphism, \( X_i \to X'_i \) are also admissible epimorphisms, and there are Cartesian diagrams

\[
\begin{array}{ccc}
X_i & \xrightarrow{f_i} & X_{i+1} \\
\downarrow{\pi_i} & & \downarrow{\pi_{i+1}} \\
X'_i & \xrightarrow{f'_i} & X'_{i+1}
\end{array}
\]

and \( f_i \) are monomorphisms, so \( f_i \) is the kernel of \( X_{i+1} \to X'_{i+1}/X'_i \), which is an admissible epimorphism, so \( f_i \) is admissible. There are natural isomorphisms \( \varphi_i : X_{i+1}/X_i \to X'_{i+1}/X'_i \). (Cf.[Harder-Narasimhan Filtrations]), and axiom A6 (3.3.1.20) shows \( \varphi \) is compatible with the geometric structure, so \( X_{i+1}/X_i \) are all semistable, and notice

\[
\mu(X_2/X_1) = \frac{\text{rank}(X_2)\mu(X_2) - \text{rank}(X_1)\mu(X_1)}{\text{rank}(X_2) - \text{rank}(X_1)} < \mu(X_1)
\]

so \( 0 \to X_1 \to X_2 \to \ldots \to X_m = X \) is a HN-filtration for \( X \). \( \square \)

**Prop. (3.2.4.23) [HN-Formalism for Filtrations in an Abelian Category].** Let \( \mathcal{C} \) be an Abelian category and \( \mathcal{E} \) the set of all short exact sequences in \( \mathcal{C} \), \( A(X) \) is the set of isomorphism classes of filtrations on \( X \), then \( (\mathcal{C}, \mathcal{E}, A) \) is a geometric exact category, by (3.3.1.24), given any additive rank function on \( \mathcal{C} \), and define a degree function for any filtration \( \mathcal{F} = (X_\lambda) \) as

\[
\text{deg}(\mathcal{F}) = \int_{\mathbb{R}} \lambda(d \text{ rank } X_{\lambda}),
\]

then \( \text{deg} \) is additive w.r.t short exact sequences of filtrations, and \( (\mathcal{C}, \mathcal{E}, A, \text{deg}, \text{rank}) \) is a Harder-Narasimhan filtration.

Then a filtration is semistable iff it has only one jump. Then the HN-filtration of a filtration is just the jump set ordered decreasingly.

**Prop. (3.2.4.24) [HN Formalism for Vector Spaces with Two Norms].** The vector spaces with two norms is a Harder-Narasimhan category, Cf.[Harder-Narasimhan Filtrations, P9].

**Prop. (3.2.4.25) [HN-Formalism for Torsion-Free Sheaves].** The category of torsion-free sheaves on a geometrically normal projective variety of dimension \( d \geq 1 \) over a field \( K \) is a Harder-Narasimhan category. Cf.[Harder-Narasimhan Filtrations, P10].
3.2. CATEGORICAL LOGIC

Prop. (3.2.4.26) [HH-Formalism for Hermitian Adelic Bundle]. Let $K$ be a number field, then the category of Hermitian adelic bundle over $K$ is a Harder-Narasimhan category. Cf. [Harder-Narasimhan Filtrations, P10].

Prop. (3.2.4.27) [HN Formalism for Filtered Vector Spaces Field]. If $L/K$ is a field extension, there is a category $VectFil_{L/K}$ consisting of $(V,Fil)$ where $V$ is a $K$-vector space and $Fil$ is a (finite) filtration of vector spaces over $L$ on $V \otimes_K L$ (3.2.3.1). It is a geometric exact category by (3.3.1.24) and a Harder-Narasimhan category by (3.2.4.20).

The rank is as usual, and the degree is defined to be

$$\deg((V,Fil)) = \int_R \lambda(d \text{rank } V)(3.2.4.23)$$

Slope Inequalities and Functoriality

Def. (3.2.4.28) [Additional Conditions]. In this subsubsection, we assume the Harder-Narasimhan filtration satisfies the following axiom that is

Def. (3.2.4.29) [Slope Inequality Axioms]. To show the functoriality of the Harder-Narasimhan filtration, we need the following axiom:

- (SI): If $X_1, X_2$ are two semistable geometric objects that $\mu(X_1) > \mu(X_2)$, then there are no non-zero morphism from $X_1$ to $X_2$ compatible with the geometric structures (3.3.1.21).

Prop. (3.2.4.30). If SI holds, then

Prop. (3.2.4.31). If $E$ is semistable of slope $\lambda$, then for any morphism $u : E \to E''$ that $F(u)$ is an isomorphism, slope($E''$) $\geq \lambda$.

Proof: Take the kernel of $F(u)$ in $A$, which corresponds to a strict object $E'$ of $E$, and $0 \to E' \to E \to E'' \to 0$ is exact, so we can use (3.2.4.19). □

Cor. (3.2.4.32). If $E, F$ are semistable of slopes $\lambda > \mu$, then $\text{Hom}_C(E, F) = 0$.

Prop. (3.2.4.33) [Semistable Vector Bundles Form a Weak Serre Subcategory]. If $f : E \to F$ be a map of vector bundles of the same slope $\lambda$, then $\ker(f)$ and $\operatorname{Coker}(f)$ are all semistable vector bundles of slope $\lambda$, and if $0 \to E' \to E \to E'' \to 0$ is exact and $E', E''$ are semistable of slope $\lambda$, then so does $E$.

Proof: Use $F(f)$ to find the "coimage" $A$ and the "image" $B$ of $f$, then there is a map from $F(A)$ to $F(B)$ which is an isomorphism, but they have the same degree and rank, thus $A \cong B$ by the last axiom. And the image must has slope $\lambda$. Then $\ker(f)$, $\operatorname{Coker}(f)$ all can be defined, and they have the same slope $\lambda$ by (3.2.4.19).

$\ker(f)$ is semistable because strict subobjects of $\ker(f)$ are also strict subobjects of $E$ (3.2.4.2). And for $\operatorname{Coker}(f)$, if it is not semistable, choose $F' \subset \operatorname{Coker}(f)$ that has slope $\lambda$, let $F''$ be the inverse image, then $0 \to \operatorname{Im}(f) \to F' \to F'' \to 0$, then by (3.2.4.19) slope($F'$) $> \lambda$, contradicting the semi-stability of $F$.

For the extension, slope($E$) $= \lambda$ by (3.2.4.19), and for a strict subobject $F$ of $E$, then we can find $F', F''$ be strict objects of $E'$, $E''$ respectively that there is an exact sequence $0 \to F' \to F \to F'' \to 0 ?$, which shows slope($F$) $\leq \lambda$, so $E$ is semistable. □
5 Tannakian Categories

Let $k$ be a field.

**Def.(3.2.5.1) [Fiber Functor].** Let $C$ be a $k$-linear Abelian tensor category, then a fiber functor on $C$ with values in a $k$-algebra $R$ is a $k$-linear exact faithful tensor functor $\eta : C \to \text{Mod}_R$ that takes values in the subcategory $\text{Proj}_R$.

**Def.(3.2.5.2) [Tannakian Category].** A Tannakian category is a rigid tensor category $C$ that $\text{End}(1) = k$ together with a fiber functor (3.2.5.1) with values in some $k$-algebra $R$.

**Def.(3.2.5.3) [Neutral Tannakian Categories].** A neutral Tannakian category is a Tannakian category that the fiber functor has values in $k$. By (15.3.2.9), such a category is equivalent to $\text{Rep}_k(G)$ for some affine group scheme $G$.

In particular, a Tannakian category can be thought of as an abstract version of the category of representations of an affine group scheme that has no distinguished “forgetful” functor, just as a vector space is an abstract version of $k^n$ that has no distinguished basis.
3.3 Homological Algebra

Main references are [Sta]Chap12 and ??.

1 Additive Category

Def. (3.3.1.1) [Preadditive Categories]. A category \( \mathcal{A} \) is called **preadditive** iff
- A1: \( \mathcal{A} \) is enriched over the Cartesian category of Abelian groups.

Def. (3.3.1.2) [Zero Element]. Let \( \mathcal{A} \) be a preadditive category and \( x \in \mathcal{A} \), then the following are equivalent:
- \( x \) is initial.
- \( x \) is final.
- \( \text{id}_x = 0 \in \text{Mor}(x, x) \).

Such an element is called a **zero element** in \( \mathcal{A} \), denoted by 0. If 0 exists, then a morphism \( \alpha : x \to y \) factors through 0 iff \( \alpha = 0 \).

Proof: Cf.[Sta]00ZZ.

Cor. (3.3.1.3). An additive functor transforms a zero object to a zero object.

Prop. (3.3.1.4) [Finite Direct Sums]. If \( \mathcal{A} \) is a preadditive category and \( x, y \in \mathcal{A} \). If one of \( x \times y \) and \( x \bigsqcup y \) exists, then so does the other, and they are isomorphic, called the **direct sum** of \( x, y \).

Proof: Cf.[Sta]0101.

Def. (3.3.1.5) [Additive Functors]. A functor between preadditive categories \( F : \mathcal{C} \to \mathcal{D} \) is called **additive** if it is a morphism of \( \text{Ab} \)-enriched categories.

Def. (3.3.1.6) [Kernels, Cokernels, Images and Coimages]. Let \( \mathcal{A} \) be a preadditive category and \( f : X \to Y \) is a map, then

- the **kernel** of \( f \) is the fiber product

\[
\begin{array}{c}
X \\
\downarrow f \\
0 \\
\rightarrow Y
\end{array}
\]

- the **cokernel** of \( f \) is the fiber pushforward

\[
\begin{array}{c}
X \\
\rightarrow f \\
\downarrow \\
0 \\
\rightarrow Y
\end{array}
\]

- the **image** of \( f \) is the cokernel of the kernel.
- the **coimage** of \( f \) is the kernel of the cokernel.

Cor. (3.3.1.7). If they exist, then kernel and coimage are monomorphisms, and cokernel and image are epimorphisms, by general non-sense.

Prop. (3.3.1.8). If the image and coimage of \( f \) exist, then there is a natural decomposition \( f : X \to \text{Im}(f) \to \text{Coim}(f) \to Y \), by the universal property.

Def. (3.3.1.9) [Exact Sequence]. A diagram \( X \overset{f}{\to} Y \overset{g}{\to} Z \) is an **exact sequence** if \( f \) is the kernel of \( g \) and \( g \) is the cokernel of \( f \).
Additive Categories

Def. (3.3.1.10) [Additive Categories]. A preadditive category $\mathcal{A}$ is called an additive category iff moreover it satisfies

- A2: There exists an element that is both initial and final, called the zero element.
- A3: There exists a canonical finite sums and finite products and they are equal, and the sum induce the Abelian structure of $\text{Hom}(X,Y)$.

Prop. (3.3.1.11) [Characterizing Direct Sum Decompositions]. If $\mathcal{A}$ is a preadditive category with zero object, $x, y, z \in \mathcal{A}$, then $z$ is the product and sum of $x, y$ in $\mathcal{A}$ iff there are four morphism that satisfies some identities.

Proof: Cf. [Sta]0102.

Cor. (3.3.1.12). An additive functor between additive categories transforms finite direct sums to direct sums.

Def. (3.3.1.13) [Kernel of an Additive Functor]. The kernel of an additive functor between additive categories is is the full subcategory of objects that are mapped to 0.

Def. (3.3.1.14) [Compact Object]. Let $\mathcal{D}$ be an additive category with arbitrary direct sums, then a compact object $K \in \mathcal{D}$ is an object that

$$\bigoplus_i \text{Hom}(K, E_i) \to \text{Hom}(K, \bigoplus_i E_i)$$

is bijective for any set $I$ and objects $E_i \in \mathcal{D}$.

Karoubian Categories

Def. (3.3.1.15) [Karoubian Categories]. A Karoubian category is an additive category $\mathcal{C}$ that satisfies the following equivalent conditions:

- Every idempotented endomorphism of an object of $\mathcal{C}$ has a kernel.
- Every idempotented endomorphism of an object of $\mathcal{C}$ has a cokernel.
- Every idempotented endomorphism $p : z \to z$ induces a direct sum decomposition $z = x \oplus y$(exists by A3) that $p$ corresponds to the projection $z \to x$.

Proof: 1 $\to$ 3: Let $p : z \to z$ be an idempotent, let $x = \ker(p), y = \ker(1-p)$, then there are maps $x \to z, y \to z$. Then $p : z \to z$ factors through $z \to y \to z$. Similarly $(1-p) : z \to z$ factors through $z \to x \to z$. Then it can be verified that $z = x \oplus y$ is a direct sum decomposition (3.3.1.11).

2 $\to$ 3 is dual.

3 $\to$ 1, 3 $\to$ 2 are easy by (3.3.1.11).

Prop. (3.3.1.16). Let $\mathcal{D}$ be a preadditive category,

- if $\mathcal{D}$ has countable products and kernels of morphisms that have a right inverse, then $\mathcal{D}$ is Karoubian.

- Dually, if $\mathcal{D}$ has countable coproducts and cokernels of morphisms that have a left inverse, then $\mathcal{D}$ is Karoubian.
Proof: Given any idempotented morphism \( e : X \to X \), \( e \) has a kernel iff \( W \mapsto \ker(\text{Mor}(M, X) \xrightarrow{e} \text{Mor}(M, X)) \) is representable. Notice that for any Abelian group \( A \),

\[
\ker(e : A \to A) = \ker(\Phi : \prod_Z A \to \prod_Z A)
\]

where

\[
\Phi(a_1, a_2, \ldots) = (ea_1 + (1 - e)a_2, ea_2 + (1 - e)a_3, \ldots)
\]

and it has a right inverse

\[
\Psi(a_1, a_2, \ldots) = (a_1, (1 - e)a_1 + ea_2, (1 - e)a_2 + ea_3, \ldots)
\]

thus the kernel exists. \( \square \)

### Exact Categories

**Def. (3.3.1.17) [Exact Categories].** Let \( \mathcal{C} \) be an small additive category and \( \mathcal{E} \) be a set of short sequences

\[
0 \to X \to Y \to Z \to 0
\]

in \( \mathcal{C} \). If \( 0 \to X \xrightarrow{\varphi} Y \xrightarrow{\psi} Z \to 0 \) is in \( \mathcal{E} \), then we call \( \varphi \) an admissible monomorphism and \( \psi \) an admissible epimorphism. then \( (\mathcal{C}, \mathcal{E}) \) is called an exact category if it satisfies:

- **Ex1:** For any complex \( 0 \to X \xrightarrow{\varphi} Y \xrightarrow{\psi} Z \to 0 \), \( \varphi \) is the kernel of \( \psi \) and \( \psi \) is the cokernel of \( \varphi \).
- **Ex2:** For any \( X, Y \in \mathcal{C} \), \( 0 \to X \to X \times Y \to Y \to 0 \) is in \( \mathcal{E} \).
- **Ex3:** \( \mathcal{E} \) is saturated in the category of short sequences.
- **Ex4:** if \( f, g \) are admissible monomorphisms, then so is \( gf \).
- **Ex5:** If \( f \) is an admissible monomorphism, then any pushout of \( f \) exists and is an admissible monomorphism.
- **Ex6:** If \( g \) is an admissible epimorphism, then any pullback of \( g \) exists and is an admissible epimorphism.

**Cor. (3.3.1.18).** If \( \mathcal{C} \) is an Abelian category and \( \mathcal{E} \) the set of all exact sequences in \( \mathcal{C} \), then \( (\mathcal{C}, \mathcal{E}) \) is an exact category.

**Cor. (3.3.1.19).** If \( (\mathcal{C}, \mathcal{E}) \) is an exact category, then

- **Ex7:** if \( f : X \to Y \in \mathcal{C} \) is a morphism having a kernel and there is a morphism \( g : Z \to X \) that \( fg \) is an admissible monomorphism, then so is \( f \). Dual argument holds for admissible epimorphisms.

**Proof:** Cf.[Bernhard Keller, Chain complexes and stable categories, P28]. \( \square \)

**Def. (3.3.1.20)[Geometric Exact Categories].** A geometric exact category consists of an exact category \( (\mathcal{C}, \mathcal{E}) \) and a mapping \( A \) from \( \text{Ob}(\mathcal{C}) \) to \( \text{Sets} \) together with morphisms

- a morphism \( f^* : A(X) \to A(Y) \) for any admissible monomorphism \( f : X \to Y \).
- a morphism \( g_* : A(X) \to A(Z) \) for any admissible epimorphism \( g : X \to Z \).

that satisfies the following axioms:
• A1: $A(0) = \text{pt}$.
• A2: If $i, j$ are admissible monomorphisms, then $(ji)^* = i^*j^*$.
• A3: If $p, q$ are admissible epimorphisms, then $(qp)_* = q_*p_*$.
• A4: $\text{id}_X^* = (\text{id}_X)_* = \text{id}_{A(X)}$.
• A5: If $f : X \to Y$ is an isomorphism, then $f^*f_* = f_*f^* = \text{id}$.
• A6: For any Cartesian and Cocartesian diagram $\xymatrix{X \ar[r]^u \ar[d]^p & Y \ar[d]^q \ar[r]^v & Z \ar[r]^w & W}$, if $u$ is admissible monomorphism or $q$ is admissible epimorphism, then $v^*q_* = p_*u^*$.
• A7: If $X \xrightarrow{u} Y \xrightarrow{v} Z$ is a diagram in $\mathcal{C}$ that $u$ is an admissible epimorphism and $v$ is an admissible monomorphism, and if $h_X \in A(X), h_Z \in A(Z)$ satisfy $u_*(h_X) = v^*(h_Z)$, then there exists $h \in A(X \oplus Z)$ that $(\text{id}, vu)^*(h) = h_X$ and $\pi_2(h) = h_Z$. (Notice $(\text{id}, vu)$ is an admissible monomorphism because it is composition of $X \to X \oplus Z$ with the isomorphism $(\pi_1, vu\pi_1 + \pi_2) : X \oplus Z \to X \oplus Z$.
For any $X \in \mathcal{C}$, an element of $A(X)$ is called a geometric structure on $X$.

Exact categories can be viewed as geometric exact categories by asserting $A(X) = \text{pt}$ for all $X \in \mathcal{C}$.

**Def. (3.3.1.21)** [Morphisms compatible with the Geometric Structure]. Let $(\mathcal{C}, \mathcal{E}, A)$ be a geometric exact category, if $(X', h'), (X'', h'')$ are two geometric objects, then a morphism $f : X' \to X''$ is said to be a morphism compatible with the geometric structure if there exists a geometric object $(X, h)$ and an admissible monomorphisms $u : X' \to X$ and an admissible epimorphism $v : X \to X''$ that $h' = u^*(h)$ and $h'' = v_*(h)$ and $f = vu$.

The composition of two morphisms compatible with the geometric structure is also a morphism compatible with the geometric structure.

We denote $\mathcal{C}_A$ the category of geometric objects of $\mathcal{C}$, and $\mathcal{E}_A$ the set of diagrams of geometric objects $0 \to X' \xrightarrow{\phi} X \xrightarrow{\pi_1} X'' \to 0$ that the underlying diagram is in $\mathcal{E}$ and $u, v$ are compatible with the geometric structures.

**Prop. (3.3.1.22)** [Hermitian Spaces]. The f.d. Hermitian spaces over $\mathbb{C}$ or f.d. normed vector spaces over $\mathbb{R}$ form a geometric exact category.

**Proof:** Cf. [Harder-Narasimhan Categories, P4].

**Prop. (3.3.1.23)** [F.D. Ultranormed Banach Spaces]. Let $K$ be a complete valued field, then the category of f.d. ultranormed Banach spaces over $K(12.1.2.4)$ is a geometric exact category.

**Proof:** It suffices to check axiom A7, but $vu$ has norm $\leq 1$, and for any $\varphi : E \to F$ of norm $\leq 1$, we can endow $E \oplus F$ with the maximum norm, then in the decomposition $E \xrightarrow{(\text{id}, \varphi)} E \oplus F \xrightarrow{\pi_2} F$, we have $(\text{id}, \varphi)^*(h) = h_E$ and $(\pi_2)_*(h) = h_F$.

**Prop. (3.3.1.24)** [Filtrations in an Abelian Category]. The filtrations (3.2.3.1) in an Abelian category form a geometric exact category.

**Proof:** Cf. [Harder-Narasimhan Categories, P5].
Def. (3.3.1.25) [K₀ Group]. Let \( \mathcal{A} \) be an exact category, then the \( K₀ \)-group \( K₀(\mathcal{A}) \) is defined to be the quotient Abelian group
\[
\bigoplus_{[0 \to A \to B \to C \to 0] \in \mathcal{E}} \mathbb{Z} \to \bigoplus_{A \in \mathcal{C}} \mathbb{Z} \to K₀(\mathcal{A}) \to 0,
\]
where \( e_{0 \to A \to B \to C \to 0} \) is mapped to \( e_B - e_A - e_C \).

2 Abelian Categories

Def. (3.3.2.1) [Abelian Categories]. An Abelian category \( \mathcal{A} \) is an additive category that satisfies the following axiom:
- A4: The kernels and cokernels exist for any \( f \), and the natural map \( \text{Im}(f) \to \text{Coim}(f) \) are isomorphisms.

Remark (3.3.2.2). WARNING: An additive category that epimorphism+monomorphism is isomorphism need not be an Abelian category. Cf. [https://mathoverflow.net/questions/41722/is-every-balanced-pre-abelian-category-abelian] for a counter-example.

Prop. (3.3.2.3). In an Abelian category, the functor \( X \mapsto \text{Hom}(X,Y) \) and \( X \mapsto \text{Hom}(Y,X) \) is both left exact. (Note that left and right is seen on the image).

Def. (3.3.2.4) [Injectives and Surjectives]. A morphism \( f \) is an Abelian category \( \mathcal{A} \) is called an injection if \( \ker f = 0 \). It is called a surjection if \( \text{Coker} f = 0 \). \( f \) is an injection iff it is a monomorphism, it is a surjection iff it is an epimorphism.

Prop. (3.3.2.5). Axiom A3 asserts the good existence of product and sum of objects as we wanted, and it can be used to prove that monomorphism and epimorphism are stable under pushout and pullback.

But this uses A4 strongly, Cf. [MacLane Categories for working mathematicians P203]. (For epimorphism, first prove \( 0 \to X \times_Y Y \to X \times Y \to U \to 0 \) is exact when \( X \to U \) is epi).

Prop. (3.3.2.6). equalizer and finite product derives finite limit, thus finite limits and finite colimits exists in Abelian categories.

Prop. (3.3.2.7) [Mitchell’s embedding theorem]. If \( \mathcal{A} \) is a small Abelian category, then there exists a unital ring \( R \), not necessary commutative and a fully faithful and exact functor \( \mathcal{A} \to R - \text{Mod} \) that preserves kernel and cokernel. WARNING: it may not preserve sum and product, let alone limits and colimits.

Proof: □

Prop. (3.3.2.8). If \( \mathcal{C}, \mathcal{A} \) are categories and \( \mathcal{A} \) is Abelian, then \( \text{Hom}(\mathcal{C}, \mathcal{A}) \) is an Abelian category. In particular, \( \text{Ch}(\mathcal{A}) \) is Abelian.

Localization

Prop. (3.3.2.9) [Localization Category]. If \( \mathcal{C} \) is a preadditive category and \( S \) is a left or right localizing system of \( \mathcal{C} \), then there exists a natural additive structure on \( S^{-1}\mathcal{C} \) and a localizing functor \( \mathcal{C} \to S^{-1}\mathcal{C} \) that is additive.

Proof: Cf. [Sta]05QD. □
Lemma (3.3.2.10). If \( \mathcal{C} \) is additive and \( S \) is localizing, let \( X \) be an element of \( \mathcal{C} \), then: \( Q(X) = 0 \) iff there is a morphism \( 0 : X \to Y \) that is an element of \( S \) iff there is a morphism \( 0 : Z \to X \) that is an element of \( S \) iff there is a morphism \( 0 : Z \to X \) that is an element of \( S \).

Proof: If such \( 0 : X \to Y \in S \), then it maps to isomorphisms in \( S^{-1}(\mathcal{C}) \) by (3.1.1.57), so \( Q(X) = 0 \). If \( Q(X) = 0 \), then the morphism \( 0 \to X \) is mapped to an isomorphism, so by (3.1.1.59), there are \( g, h \) that \( fg = hf = 0 \), so \( Z \to 0 \to X \in S \). Dually for the other direction. \( \square \)

Prop. (3.3.2.11) [Localized Abelian Categories]. If \( \mathcal{A} \) is Abelian and \( S \) is localizing, then \( S^{-1} \mathcal{A} \) is an Abelian category and \( \mathcal{A} \to S^{-1} \mathcal{A} \) is exact.

Proof: By (3.1.1.57) and its dual, \( \mathcal{A} \to S^{-1} \mathcal{A} \) preserves finite limits and colimits. \( \square \)

Serre Subcategory

Def. (3.3.2.12) [Serre Subcategories]. A Serre subcategory of an Abelian category is a non-empty full subcategory \( \mathcal{C} \) that if

\[
A \to B \to C
\]

is exact and \( A, C \in \text{Ob}(\mathcal{C}) \), then \( B \in \text{Ob}(C) \).

A weak Serre subcategory of an Abelian category is a non-empty full subcategory \( \mathcal{C} \) that if

\[
A \to B \to C \to D \to E
\]

is exact and \( A, B, D, E \in \mathcal{C} \), then \( C \in \mathcal{C} \).

Prop. (3.3.2.13).

- A Serre category is equivalent to a full subcategory \( \mathcal{A} \) that contains 0, all the subobjects and quotient objects of \( \mathcal{A} \), and extensions of objects of \( \mathcal{A} \) are in \( \mathcal{A} \).
- A weak Serre category is equivalent to a full subcategory \( \mathcal{A} \) that contains 0, and all the kernels, cokernels of objects in \( \mathcal{A} \), and all the extensions of objects in \( \mathcal{A} \).

In these cases, \( \mathcal{A} \) is an Abelian category and the functor \( i : \mathcal{A} \to \mathcal{C} \) is exact.

Proof: One direction of these two are trivial, it suffices to prove the converse. For the first, \( 0 \to \text{Im}(A) \to B \to \text{Im}(B) \to 0 \), so \( B \in \mathcal{C} \). For the second, \( 0 \to \text{Coker}(A \to B) \to C \to \text{ker}(D \to E) \to 0 \), so \( C \in \mathcal{C} \). \( \square \)

Prop. (3.3.2.14) [Quotients by Serre Subcategory]. For an exact functor \( F \) between Abelian categories, the kernel of \( F \) is a Serre subcategory. Any Serre subcategory is the kernel of an essentially surjective exact functor \( Q : \mathcal{A} \to \mathcal{A}/\mathcal{C} \), and this functor satisfies the universal property that any exact functor between Abelian categories \( F : \mathcal{A} \to \mathcal{C} \) that \( \mathcal{C} \subset \text{ker}(F) \) factors uniquely through \( \mathcal{A}/\mathcal{C} \).

Proof: The full subcategory of \( \text{ker}(F) \) is clearly a Serre subcategory by checking the definition. Conversely, consider \( S = \)all the morphisms that has kernel and cokernel in \( \mathcal{C} \), first we prove it is a localizing system (3.1.1.54).

The long exact sequence (3.3.4.4) shows that if \( f, g \in S \), then \( gf \in S \). For other verifications, Cf. [Sta] 02MS?

Next we construct \( \mathcal{C}/\mathcal{A} \) as \( S^{-1} \mathcal{C} \). Consider which objects are mapped to 0 in \( \mathcal{C}/\mathcal{A} \), use (3.3.2.10) and consider the kernel and cokernel, it is easy to see that \( \text{ker}(Q) = \mathcal{C} \). If another category \( \mathcal{D} \) and \( F : \mathcal{C} \to \mathcal{D} \) satisfies \( \mathcal{C} \) is mapped to 0, then it is clear that elements in \( S \) is mapped to isomorphism, so it factors through \( \mathcal{C}/\mathcal{A} \) by universal property (3.1.1.57). \( \square \)
Prop. (3.3.2.15)[K₀ Group of Serre Subcategory]. Let $\mathcal{A}$ be an Abelian category and $\mathcal{C}$ a Serre subcategory, with $\mathcal{A}/\mathcal{C} = \mathcal{B}$. Then

- The exact functors $\mathcal{C} \to \mathcal{A} \to \mathcal{B}$ induces an exact sequence

$$K_0(\mathcal{C}) \to K_0(\mathcal{A}) \to K_0(\mathcal{B}) \to 0,$$

- The kernel of $K_0(\mathcal{C}) \to K_0(\mathcal{A})$ is generated by elements of the form

$$\ker(\psi) \left/ \text{Im}(\varphi) \right. - \ker(\varphi) \left/ \text{Im}(\psi) \right.$$  

where $\varphi, \psi : M \to M$ are pairs of maps that $\varphi \circ \psi = \psi \circ \varphi = 0$.

Proof: Cf.[Sta]02MX. □

Artinian Abelian Categories

Def. (3.3.2.16)[Artinian Abelian Categories]. An Artinian Abelian category is an Abelian category that

- $\text{Hom}(A, B)$ are all f.d. vector spaces over $k$.
- Then length of any filtrations $0 = X_0 \subset X_1 \subset \ldots \subset X_l = X$ for any object $X$ is bounded. The maximal length is called the length of $X$.

Prop. (3.3.2.17)[Jordan-Holder]. Let $\mathcal{C}$ be an Artinian category, then any maximal length filtration of an element $X$ has the same length, and the set of quotients $X_{k+1}/X_k$ is the same, up to order.

Proof: □

Others

Def. (3.3.2.18)[Essential Morphism]. In an Abelian category, an injection $A \to B$ is called essential iff every non-zero subobject of $B$ intersects $A$. A surjection is called essential iff every proper subobject of $A$ is not mapped to $B$.

Def. (3.3.2.19)[Noetherian Abelian Category]. In a Grothendieck Abelian category $\mathcal{A}$, an object $M$ is called finitely generated if for every ascending chain

$$M_1 \subset M_2 \subset \ldots \subset M$$

with $\bigcup_i M_i = M$, we have $M_i = M$ for some $i$.

$\mathcal{A}$ is called Noetherian iff a subobject of a f.g. object is f.g.. $\mathcal{A}$ is called Artinian iff every f.g. object has finite length.

Def. (3.3.2.20)[Compact Objects]. An object $M$ in an additive category $\mathcal{C}$ with arbitrary direct sum is called compact if Hom($M, -$) commutes with arbitrary direct sums.
Grothendieck Abelian Category

Def. (3.3.2.21) [Grothendieck Abelian Category]. A Grothendieck Abelian category is an Abelian category \( \mathcal{A} \) satisfying the following axioms:

**AB3**: It is an Abelian category and arbitrary direct sums exists. (Thus colimits over small categories exists.)

**AB5**: Filtered colimits over small categories are exact. This is equivalent to \{ for any family of subobjects \( \{ A_i \} \) of \( A \) to \( B \) indexed by inclusion can induce a morphism \( \sum A_i \to B \) (internal sum) \}?.

**GEN**: It has a generator, which is an object \( U \in \mathcal{A} \) s.t. for any proper subobject \( N \subseteq M \), there is a map \( U \to M \) that doesn’t factor through \( N \).

Def. (3.3.2.22) [Further Grothendieck Axioms]. For a Grothendieck Abelian category \( \mathcal{A} \), we can also formulate the following axioms:

**AB4**: Arbitrary direct sums are exact.

**AB6**: For any index set \( J \) and filtered categories \( I_j, j \in J \) and diagrams indexed over \( I_j \), the natural map

\[
\lim_{i_j \in I_j} \prod_{j \in J} M_{ij} \to \prod_{j \in J} \lim_{i_j \in I_j} M_{ij}
\]

is an isomorphism.

**Dual Axioms**: Axioms with an * meaning that the dual category satisfies something.

Prop. (3.3.2.23). The presheaf category \( \mathcal{A}^C \) is a Grothendieck Abelian category if \( \mathcal{A} \) is Grothendieck Abelian.

**Proof**: For the presheaf, the only problem is the existence of generator, for that, just construct a family of presheaves and sum them. Take \( Z_X = i_f(U) \), where \( U \) is the generator of \( \mathcal{A} \) and \( f = pt \to A^C : pt \to U \). Then \( F(X) = \text{Hom}(Z_X, F) \) by adjointness (5.1.2.9). So they are a family of generators. \( \square \)

Prop. (3.3.2.24). Any Grothendieck Abelian category has a functorial injective embedding.

**Proof**: Cf. [Sta]079H. \( \square \)

Prop. (3.3.2.25) [Representability on Grothendieck Category]. A contravariant functor from a Grothendieck category to \( \text{Sets} \) is representable iff it takes colimits to limits.

**Proof**: \( M \oplus M \to M \) with induce a map \( F(M) \times F(M) \to F(M) \) thus \( F(M) \) is a semigroup, and the inverse of \( \text{id}_M \) in \( \text{Hom}(M, M) \) maps to a \( F(M) \to F(M) \) which is the inverse, Thus in fact \( F \) is a left adjoint functor to \( A_b \).

Let \( U \) be a generator, \( A = \sum_{s \in F(U)} U \), let \( s_{\text{univ}} = (s) \in F(A) = \prod_{s \in F(U)} F(U) \). Let \( A' \) be the largest objects that \( s_{\text{univ}} \) restrics to 0 in \( A' \), let \( \sigma_{\text{univ}} \) be in \( F(A/A') \) that maps to \( s_{\text{univ}} \) in \( F(A) \) (because \( F \) is left exact). Then we claim \( (A/A', \sigma_{\text{univ}}) \) represents \( F \). Cf. [Sta]07D7. \( \square \)

Cor. (3.3.2.26). Grothendieck Category satisfies \( AB3^* \). (because \( F = \prod_i \text{Hom}(-, M_i) \) commutes with colimits).
Examples of Grothendieck Category

**Prop. (3.3.2.27)[Modules].** For $R \in \text{Alg}$, $\text{Mod}_R$ is a Grothendieck Abelian category. More generally, for $R, S \in \text{Alg}$, $\text{Mod}_{R-S} = \text{Mod}_{R \otimes S^{op}}$ is a Grothendieck Abelian category.

**Proof:** This is clear, by (4.1.1.24).

**Prop. (3.3.2.28)[Sheaf of Modules].** $\text{Sh}(\mathcal{O})$ for a ringed site $(\mathcal{C}, \mathcal{O})$ is a Grothendieck Abelian category.

**Proof:** It is obviously an Abelian category and have filtered colimits as presheaves, which are exact because colimits in the category of Abelian groups are exact, and for a family of generators, take $j_U\mathcal{O}_U$ as the representative for $\Gamma(U, -)$, which is the sheaf associated to the sheaf $Z_U$ in the proof of (3.3.2.23).

**Cor. (3.3.2.29).** Let $\mathcal{C}$ be a site, the categories $\text{PSh}(\mathcal{C})$ and $\text{Sh}(\mathcal{C})$ are Grothendieck Abelian categories.

**Proof:** For the presheaf, Cf.(3.3.2.23). For the sheaf, it follows from (3.3.2.28).

**Remark (3.3.2.30).** The category of Abelian sheaves doesn’t satisfy AB4*, i.e. not every limit of epimorphisms is epimorphism.

**Proof:** Consider the constant sheaf $\prod_{\xi \in [0, 1]} B(\frac{\xi}{2}, \frac{1}{4})$ on $[0, 1]$.

**Prop. (3.3.2.31)[Quasi-Coherent Sheaves].** For $X \in \text{Sch}$, $\text{QCoh}(X)$ is Grothendieck category, and there is a coherentor left adjoint to the forgetful functor.

**Proof:** Firstly by (5.5.1.3), $\text{QCoh}(X)$ is an Abelian category, and on affine open set, the colimit is an Qco sheaf, thus the colimit exists in Qco and equals the colimit in the category of sheaves, thus filtered colimits is exact because $\text{Mod}(\mathcal{O}_X)$ is Grothendieck (3.3.2.28). The generator exists, Cf.[Sta]077P.

The coherentor exists by the fact that $h_F$ commutes with colimits and by the property of Grothendieck category (3.3.2.25).

3 Chain Complexes

**Def. (3.3.3.1)[Chain Complex].** A chain complex over an additive category $A$ is $\cdots \rightarrow C_{n+1} \rightarrow C_n \rightarrow C_{n-1} \rightarrow \cdots$. The category of complexes over $A$ is denoted by $\text{Comp}(A)$.

**Prop. (3.3.3.2).** For any Abelian category $A$, $\text{Comp}(A)$ is an Abelian category.

**Prop. (3.3.3.3).** The natural inclusion $A \subset \text{Comp}(A)$ embeds $A$ as a full subcategory of $D(A)$, and $H^0$ is just the left adjoint.

An object $K \in D(A)$ is called discrete if it is in the essential image of this embedding.

**Def. (3.3.3.4)[Shifting of Complexes].** Remember the translation operator $K[n]$ makes the complex lower $n$ dimensions.

**Def. (3.3.3.5) [Truncation of Complexes].** Let $A$ be an Abelian category and $A^*$ be a complex, there are several ways to truncate $A^*$:

- The stupid truncation $\sigma_{\leq n} A = \cdots \rightarrow A_{n-1} \rightarrow A_n \rightarrow 0 \rightarrow \cdots$. There is a morphism $A \rightarrow \sigma_{\leq n} A$. 
• The stupid truncation $\sigma_{\geq n}A = \ldots \to 0 \to A_n \to A_{n+1} \to \ldots$. There is a morphism $\sigma_{\geq n}A \to A$.

• The canonical truncation $\tau_{\leq n}A = \ldots \to A_{n-1} \to \ker(d_n) \to 0 \to \ldots$. There is a natural morphism $\tau_{\leq n}A \to A$ that induces isomorphism on cohomology groups on degree $\leq n$.

• The canonical truncation $\tau_{\geq n}A = \ldots \to 0 \to \coker(d_{n-1}) \to A_{n+1} \to \ldots$. There is a natural morphism $A \to \tau_{\geq n}A$ that induces isomorphism on cohomology groups on degree $\geq n$.

Cor. (3.3.3.6). There are exact sequences of complexes

$$0 \to \tau_{\leq n}A^\bullet \to A^\bullet \to \tau_{\geq n+1}A^\bullet \to 0$$

$$0 \to \sigma_{\geq n+1}A^\bullet \to A^\bullet \to \sigma_{\leq n}A^\bullet \to 0$$

Def. (3.3.3.7) [Cone & Cylinder]. The mapping cone of $f : K^\bullet \to L^\bullet$ is the complex $C(f)^\bullet$ that:

$$C(f) = K[1]^\bullet \oplus L^\bullet, \quad d(k^{i+1}, l^i) = (-d_K k^{i+1}, f(k^{i+1}) + d L l^i)$$

The mapping cylinder of $f : K^\bullet \to L^\bullet$ is the complex $\text{Cyl}(f)$ that:

$$\text{Cyl}(f) = K^\bullet \oplus K[1]^\bullet \oplus L^\bullet, \quad d(k^i, k^{i+1}, l^i) = (d_K k^i - k^{i+1}, -d_K k^{i+1}, f(k^{i+1}) + d L l^i)$$

It is a shame I haven’t see clearly the similarity of this with the topological cone and cylinder, should study it further.

Def. (3.3.3.8) [Double Complexes]. A double complex over an Abelian category is a complex over $\text{Comp}(\text{A})$.

Def. (3.3.3.9) [Totalization]. Given a double complex $K^{\bullet \bullet}$ over an Abelian category $\text{A}$, the associated total complexes is defined to be

$$(\text{Tot}^\Pi(K))^n = \prod_{n=p+q} K^{p,q}, \quad d^n = \prod_{n=p+q} (d^{p,q} + (-1)^p d_2^{p,q})$$

$$(\text{Tot}^\oplus(K))^n = \bigoplus_{n=p+q} K^{p,q}, \quad d^n = \sum_{n=p+q} (d^{p,q} + (-1)^p d_2^{p,q})$$

Def. (3.3.3.10) [Hom Complexes]. Let $\text{A}$ be an Abelian category and $P^\bullet, Q^\bullet \in K(\text{A})$, we define Hom complex $\text{Hom}^n(P^\bullet, Q^\bullet)$ to be

$$\text{Hom}^n(P^\bullet, Q^\bullet) = \prod \text{Hom}_i(P^i, Q^{n+i}),$$

with the differential giving by $d(\{f_k\})_i = \{df_i - (-1)^i f_{i+1}d\}$ and suitable signatures.

It is clear that $H^n(\text{Hom}^n(P^\bullet, Q^\bullet)) = \text{Hom}_{K(\text{A})}(P^\bullet, Q^\bullet[n])$.

Homotopy Category $K(\text{A})$

Def. (3.3.3.11) [Homotopies of Complexes].

Def. (3.3.3.12) [$K(\text{A})$]. Let $\text{A}$ be an additive category, the homotopy category of complexes $K(\text{A})$ is the category whose objects are complexes in $\text{A}$ and whose morphisms are homotopy classes of morphism between complexes.
Prop. (3.3.3.13) [Distinguished Triangle of $K^*(A)$]. For any morphism $K^* \to L^*$, there exists a termwise-splitting exact sequence of Complexes commuting in $K(A)$.

\[
\begin{array}{ccccccccc}
K^* & \longrightarrow & L^* \\
\| & \downarrow \alpha & \downarrow & \\
0 & \longrightarrow & K^* & \longrightarrow & \text{Cyl}(f) & \longrightarrow & C(f) & \longrightarrow & 0 \\
\downarrow \beta & & & & \downarrow & & & & \\
0 & \longrightarrow & L^* & \longrightarrow & C(f) & \longrightarrow & K^*[1] & \longrightarrow & 0
\end{array}
\]

where $\beta \alpha = \text{id}$ and $\alpha \beta \sim \text{id}$. And $K^* \to L^* \to C(f) \to K^*[1]$ is called a distinguished triangle. Any exact triple of complexes in $\text{Kom}(A)$ is quasi-isomorphic to a distinguished triangle. In fact, we can define the distinguished triangle in $K(A)$ as that induced by a split exact sequence, Cf.[Sta]014L.

Notice all this can imitate the similar parallel construction in the category of topological spaces.

Proof: Cf.[Gelfand P157] □

Cor. (3.3.3.14) [Long Exact Sequences]. A distinguished triangle will induce a long exact sequence of cohomology groups, for this, just need to verify that the $\delta$-homomorphism and the morphism $C(f) \to K^*[1]$ induce the same map of cohomology groups.

Cor. (3.3.3.15). A morphism of complexes $f : K^* \to L^*$ is quasi-iso iff $C(f)$ is acyclic. It is homotopic to 0 iff $f$ can be extended to a morphism $C(f) \to L$.

Prop. (3.3.3.16) [$K(A)$ is Triangulated]. If $A$ is an additive category, then $K(A)$ is a triangulated category, with shifting functors defined in (3.3.3.4) and distinguished triangles defined in (3.3.3.13).

Proof: Cf.[Sta]014S. □

Prop. (3.3.3.17). An additive functor $F : A \to B$ between additive categories induces an exact functor $K(A) \to K(B)$. Moreover, this functor maps quasi-isomorphisms to quasi-isomorphisms (3.3.4.1).

Proof: Cf.[Sta]014X. □

Def. (3.3.3.18) [Bounded Subcategories].

Prop. (3.3.3.19). Let $A$ be an Abelian category,

- If $A^* \subset K^+(A)$, then $\tau_{\leq n}(A^*) \to A^*$ is a quasi-isomorphism for $n$ sufficiently large.
- If $A^* \subset K^-(A)$, then $A^* \to \tau_{\geq n}A^*$ is a quasi-isomorphism for $n$ sufficiently small.

Unbounded Complexes

Lemma (3.3.3.20) [Left Resolutions of Unbounded Complexes]. Let $A$ be an Abelian category and $\mathcal{P}$ be a subset of objects of $A$. Assume that every object of $A$ is a quotient of an object of $\mathcal{P}$, then for any complex $K^*$, there exists a commutative diagram

\[
\begin{array}{ccc}
P_1^* & \longrightarrow & P_2^* \\
\downarrow & & \downarrow \\
\tau_{\leq 1}K^* & \longrightarrow & \tau_{\leq 2}K^* \\
& & \\
& & \ldots
\end{array}
\]
where the vertical arrows are quasi-isomorphisms, and each $P^n_\bullet$ is a bounded above complex with terms in $\mathcal{P}$, and each $P^n_\bullet \to P^{n+1}_\bullet$ are termwise-split injections and the cokernel is also a complex with terms in $\mathcal{P}$.

Proof: Cf. [Sta]06XX.

4 Cohomology of Complexes

Def. (3.3.4.1)[Quasi-irosmoepwhiss].

Prop. (3.3.4.2)[Five lemma]. In an Abelian category, if there is a diagram

\[
\begin{array}{c}
\ast & \longrightarrow & \ast & \longrightarrow & \ast & \longrightarrow & \ast & \longrightarrow & \ast \\
\downarrow{s} & & \downarrow{g} & & \downarrow{f} & & \downarrow{h} & & \downarrow{i} \\
\ast & \longrightarrow & \ast & \longrightarrow & \ast & \longrightarrow & \ast & \longrightarrow & \ast
\end{array}
\]

Where the rows are exact and $g, h$ are isomorphisms. If $i$ is injective, then $f$ is surjective; if $s$ is surjective, then $f$ is injective.

Proof: Rotate the diagram counterclockwise $90^\circ$. Then use the two different filtration both converge (3.4.7.8).

Prop. (3.3.4.3)[Snake lemma]. In an Abelian category, if there is a diagram

\[
\begin{array}{c}
\ast & \longrightarrow & \ast & \longrightarrow & \ast & \longrightarrow & \ast & \longrightarrow & 0 \\
\downarrow{f} & & \downarrow{g} & & \downarrow{h} & & & & \\
0 & \longrightarrow & \ast & \longrightarrow & \ast & \longrightarrow & \ast & \longrightarrow & \ast
\end{array}
\]

where the rows are exact, then there is a long exact sequence

$$\ker f \to \ker g \to \ker h \to \text{Coker } f \to \text{Coker } g \to \text{Coker } h$$

And if $i$ is injective, then the first one is injective; if $s$ is surjective, then the last one is surjective.

Proof: Rotate the diagram counterclockwise $90^\circ$. Then use the two different filtration both converge (3.4.7.8).

Cor. (3.3.4.4). In an Abelian category, if $f : A \to B, g : B \to C$, then there is a long exact sequence:

$$0 \to \ker f \to \ker gf \to \ker g \to \text{Coker } f \to \text{Coker } gf \to \text{Coker } g \to 0.$$

Proof: Use snake lemma (as modules), there is a diagrams:

\[
\begin{array}{c}
A & \longrightarrow & B & \longrightarrow & \text{Coker } f & \longrightarrow & 0 \\
\downarrow{gf} & & \downarrow{g} & & & & \\
0 & \longrightarrow & C & \longrightarrow & C & \longrightarrow & 0
\end{array}
\]

So by Snake lemma,

$$\ker gf \to \ker g \to \text{Coker } f \to \text{Coker } gf \to \text{Coker } g \to 0.$$

As Abelian category is dual, we can do this dually to get:

$$0 \to \ker f \to \ker gf \to \ker g \to \text{Coker } f \to \text{Coker } gf.$$

They splint together to get the desired long exact sequence.
Prop. (3.3.4.5). For a $3 \times 3$ diagram of complexes, the connection homomorphism satisfies an anti-commutative diagram:

\[
\begin{array}{ccc}
H^{q-1}(Z'') & \xrightarrow{\delta} & H^q(X'') \\
\downarrow{\delta} & & \downarrow{-\delta} \\
H^q(Z) & \xrightarrow{\delta} & H^{q+1}(X)
\end{array}
\]

by (3.4.1.15) as the category $K(A)$ is triangulated.

Prop. (3.3.4.6) [Universal Coefficient Theorem]. Should be somewhere in [Weibel].

Def. (3.3.4.7) [Herbrand Quotient]. For a complex of $R$-modules cyclic of order 2, we define the
additive Herbrand quotient as $\text{length}_R(H^0) - \text{length}_R(H^1)$, when both are definable and the
multiplicative Herbrand quotient as $|H^0|/|H^1|$ when they are both finite.

Prop. (3.3.4.8). For an exact sequence $0 \to M \to N \to K \to 0$ of complexes of cyclic order 2, we have
$h(N) = h(M) + h(K)$ and $h^*(N) = h^*(M)h^*(K)$ in the sense that if two of them are definable, then so is the third. This is an easy consequence of long exact sequence.

Prop. (3.3.4.9). If each term of this complex has finite length, then $h(M) = 0$. If each term is finite, then $h^*(M) = 0$. This is an consequence of isomorphism theorem. So we have, if a morphism of complexes has kernel and cokernel finite, then it induce an isomorphism on $h$ or $h^*$.

Proof: □

5 Injectives & Projectives

Def. (3.3.5.1). An injective object in a Abelian category is a $I$ s.t. $\text{Hom}(-, I)$ is an exact functor, equivalenty, maps to $I$ can be extended along injections.

A projective object in a Abelian category is a $I$ s.t. $\text{Hom}(I, -)$ is an exact functor, equivalently, maps to $I$ can be pulled back along surjections.

Prop. (3.3.5.2). Product of injective elements are injective, sums of projective elements are projective.

Prop. (3.3.5.3). In an Abelian category, the direct summand of a projective object is projective. (The summand has definition in an Abelian category).

Prop. (3.3.5.4). If a functor $f$ between Abelian categories is left adjoint to an exact functor, then it preserves injectives. Dually for projectives.

Prop. (3.3.5.5). If $A$ is an Abelian category, the chain complex category $Ch(A)$ is abelian by (3.3.2.8).

A chain complex $P$ is projective iff it is a split exact complex of projective objects. The same is true by dual argument for injectives.

Proof: If $K$ is projective, use the surjection $C(\text{id}_K) \to K[1]$, there is a homotopy between $\text{id}_K$ and 0. Thus we have $x = dx + hdw$. And if $dx = hy$, then $dhdy = 0$, thus $dy = 0$, so $K = dhK \oplus hdK$ and thus $K[n] = B_n \oplus B_{n+1}$. Thus $K$ is a direct product of $0 \to B \to B \to 0$. And this one is projective if $B$ is projective. □

Prop. (3.3.5.6) [Check Injectives]. In a Grothendieck Abelian category with generator $U$, an object is injective iff it is extendable over subobjects of $U$. (AB5 assures we can extend by Zorn’s lemma. Then use GEN, Cf.[Sta]079G?). If it is a family of objects, it suffice to extend over each one of them.
Injective Resolutions

Prop. (3.3.5.7) [Horseshoe Lemma]. For a exact sequence $0 \to X_1 \to X \to X_2 \to 0$ and a injective resolution of $X_1$ and $X_2$, there is a injective resolution of $X$ commuting with them. (Choose them one-by-one, in fact, $I_n = I_1 \oplus I_2$ using the injectivity of $I_1$. Snake lemma told us that the cokernel is an exact sequence, use that to define the next one.

Prop. (3.3.5.8). For two lifting of morhpisms $X_1 \to Y_1$ and $X_2 \to Y_2$, there is a lifting of the morphism $X \to Y$ compatible with that. Cf.[Weibel P2.4.6].

Prop. (3.3.5.9) [Cartan-Eilenberg Resolution]. For a complex $K \in \mathcal{K}_B^+$, a Cartan-Eilenberg resolution of $K$ consists of a 2-complex $I^{\bullet \bullet}$ and a map of complexes $K \to I^{\bullet,0}$ that the induced complexes:

\[
0 \to K^i \to I^{i,0} \to I^{i,2} \to \ldots
\]
\[
0 \to B^i(K) \to B^i_x(I^{\bullet,0}) \to B^i_x(I^{\bullet,1}) \to \ldots
\]
\[
0 \to Z^i(K) \to Z^i_x(I^{\bullet,0}) \to Z^i_x(I^{\bullet,1}) \to \ldots
\]
\[
0 \to H^i(K) \to B^i_x(I^{\bullet,0}) \to H^i_x(I^{\bullet,1}) \to \ldots
\]

are all injective resolutions, and the exact sequences

\[
0 \to B^i_x(I^{\bullet,j}) \to Z^i_x(I^{\bullet,j}) \to H^i_x(I^{\bullet,j}) \to 0
\]
\[
0 \to Z^i_x(I^{\bullet,j}) \to I^{\bullet,j} \to Z^i_x(I^{\bullet,j}) \to 0
\]

split.

Then if $I_B$ is sufficiently large, for any $K$ in $K(B)$ there is a Cartan-Eilenberg resolution.

Proof: Cf.[Gelfand P210],[Weibel P146].

Cor. (3.3.5.10). For a CE resolution of a complex $K \in K^+(\mathcal{B})$, the spectral sequence can be applied and shows $K \to \text{Tot}(L)$ is a quasi-isomorphism, i.e. $\text{Tot}(L)$ is an injective resolution of $K$.

Cor. (3.3.5.11) [Functoriality of Cartan-Eilenberg Resolution]. If $f : A \to B$ is a chain map and $A \to P, B \to Q$ are Cartan-Eilenberg resolutions, then there is a double complex map $\tilde{f} : P \to Q$ extending $f$. And if $f$ is homotopic to $g$, then $\tilde{f}$ is homotopic to $\tilde{g}$. In other words, we have a functor $K(A) \to K(I^{\bullet \bullet})$

In particular, for any two Cartan-Eilenberg resolutions $P, Q$ of $A$ and an additive functor $F$, the chain complex $\text{Tot}^{\Pi}(F(P))$ and $\text{Tot}^{\Pi}(F(Q))$ are chain homotopy equivalent.

Def. (3.3.5.12) [Injective Amplitude]. Let $\mathcal{A}$ be an Abelian category with sufficiently injectives, then $K \in D(A)$ is said to have finite injective dimension if $K \subset D^b(I_A)$. It is said to have injective amplitude in $[a, b]$ iff $K \subset D^{[a,b]}(I_{\mathcal{A}})$. 

6 Tensor Category Case

In this subsection we consider complexes over a tensor category \( \mathcal{A} \).

Lemma (3.3.6.1) [Koszul Sign Rule]. There is an isomorphism of complexes
\[
\sigma : C \otimes D \to D \times C : \sigma(x \otimes y) = (-1)^{mn}y \otimes x
\]
where \( x \in C^m \) and \( y \in D^n \).

Proof:
\[
\partial(\sigma(x \otimes y)) = \partial((-1)^{mn}y \otimes x) = (-1)^{mn}(\partial y \otimes x) + (-1)^{mn+n}(y \otimes \partial x) = (-1)^n\sigma(x \otimes \partial y) + \sigma(\partial y \otimes x) = \sigma(\partial(x \otimes y))
\]
\[\square\]

Prop. (3.3.6.2) [Monoidal Structure on \( \text{Comp}^*(\mathcal{A}) \)]. The functor
\[
\text{Comp}^*(\mathcal{A}) \times \text{Comp}^*(\mathcal{A}) \to \text{Comp}^*(\mathcal{A}) : (C, D) \mapsto \text{Tot}^\oplus(C \otimes D)
\]
deeds \( \text{Comp}(\mathcal{A}) \) with a (non-strict) commutative monoidal structure.

Proof: Commutativity follows from (3.3.6.1). Associality follows from the definition of totaliza-
tion (3.3.3.9).
\[\square\]

Prop. (3.3.6.3) [Commutative Monoidal Structure on \( K^*(\mathcal{A}) \)]. This monoidal functor descends
to a strict monoidal structure on \( K^*(\mathcal{A}) \).

Proof: 

Prop. (3.3.6.4) [Tensoring is Exact]. Let \( L^* \in K(\mathcal{A}) \), then tensoring functor \( \text{Tot}^\oplus(\cdot \oplus L^*) \) is an
exact functor between triangulated categories.

Proof: 

Prop. (3.3.6.5). An \( R \)-module \( I \) is injective iff for any injective homomorphism from \( I \) to any \( R\)-
module splits.

Proof: The critical point is that we can always embed \( I \) to an injective hull \( J \) by (3.3.2.24), then
\( J = I \oplus J' \), so \( I \) is clearly injective.
\[\square\]

Prop. (3.3.6.6) [K-Injective under Change of Rings]. If \( R \to S \) is a ring map, then
1. If \( R \to S \) is flat and \( I^* \) is a \( K \)-injective complex of \( S \)-modules, then \( I^* \) is \( K \)-injective as a
complex of \( R \)-modules.
2. If \( R \to S \) is surjective and \( I^* \) is a complex of \( S \)-modules that is \( K \)-injective as a complex of
\( R \)-modules, then it is \( K \)-injective as a complex of \( S \)-modules.
3. If \( I^* \) is a \( K \)-injective complex of \( R \)-modules, then \( \text{Hom}_R(S, I^*) \) is \( K \)-injective as a complex of
\( S \)-modules.

Proof: 1: This is because \( \text{Hom}_{K(R)}(M^*, I^*) = \text{Hom}_{K(S)}(M^* \otimes_R S, I^*) \) and (3.4.3.1), as tensoring
\( S \) is exact.
2: This is because \( \text{Hom}_{K(R)}(N^*, I^*) = \text{Hom}_{K(S)}(N^* \otimes_S I^*) \) for a complex of \( S \)-modules \( N^* \)
and (3.4.3.1).
3: This is because \( \text{Hom}_{K(S)}(N^*, \text{Hom}_R(S, I^*)) = \text{Hom}_{K(R)}(N^*, I^*) \), and (3.4.3.1).
\[\square\]
3.4 Derived Categories

Main references are [G-M03] and [Sta].

1 Triangulated Categories

Def. (3.4.1.1) [Triangulated Categories]. A triangulated category is an additive category \( \mathcal{D} \) with an additive automorphism \( T \) denoted by \( X \mapsto X[1] \) and a set of distinguished triangles \( \text{Tri}(\mathcal{D}) \) that is stable under isomorphism, and satisfying the following axioms:

(TR1): \( X \xrightarrow{\text{id}} \xrightarrow{\text{id}} X \xrightarrow{0} X[1] \in \text{Tri}(\mathcal{D}) \). Any morphism \( X \xrightarrow{u} Y \) can be completed to some \( X \xrightarrow{u} Y \xrightarrow{C(u)} C(1) \xrightarrow{C(1)} X[1] \in \text{Tri}(\mathcal{D}) \).

(TR2): \( X \xrightarrow{\text{id}} \xrightarrow{\text{id}} Y \xrightarrow{\text{id}} Z \xrightarrow{\text{id}} X \xrightarrow{\text{id}} X[1] \in \text{Tri}(\mathcal{D}) \) iff \( Y \xrightarrow{\text{id}} \xrightarrow{\text{id}} Z \xrightarrow{\text{id}} X \xrightarrow{\text{id}} Y[1] \in \text{Tri}(\mathcal{D}) \).

(TR3): Any two consecutive morphisms of two distinguished triangles can be extended to a morphism of distinguished triangles.

(TR4): If \( X \xrightarrow{f} Y \xrightarrow{g} Z \) are morphisms, then there are maps \( C(f) \rightarrow C(gf) \), \( C(gf) \rightarrow C(g) \) by TR3, Then \( C(f) \rightarrow C(gf) \rightarrow C(gf) \rightarrow C(g) \rightarrow C(f)[1] \) is distinguished.

A triangulated subcategory is an additive subcategory \( \mathcal{D}' \) stable under \([1] \) and \([-1]\) together with a subclass of triangles in \( \mathcal{D}' \) that forms a triangulated category.

Def. (3.4.1.2) [Notations]. We use the tuple \((X,Y,Z,f,g,h)\) to represent a distinguished triangle \( X \xrightarrow{f} Y \xrightarrow{g} Z \xrightarrow{h} X[1] \).

Prop. (3.4.1.3). Given \((X,Y,Z,f,g,h)\), \((X',Y',Z',f',g',h')\), they are both in \( \text{Tri}(\mathcal{D}) \) iff \((X \oplus X',Y \oplus Y',Z \oplus Z',f \oplus f',g \oplus g',h \oplus h')\) is in \( \text{Tri}(\mathcal{D}) \).

Proof: \([\text{Sta}]05QS.\]

Cor. (3.4.1.4). \((X,X \oplus Y,Y,(1,0),(0,1),0)\) is a distinguished triangle.

Prop. (3.4.1.5). There is a natural notation of a product of triangulated categories.

Def. (3.4.1.6) [Exact Functors]. A functor from a triangulated category to an Abelian category is called (co)homological iff it maps a distinguished triangle to a long exact sequence.

Conversely, a \( \delta \)-functor is a functor from an Abelian category to a triangulated category together with a map from the category of exact sequences to the category of distinguished triangles.

A functor \( F \) between two triangulated categories is called exact iff it maps distinguished triangles to distinguished triangles, and there is an isomorphism of functors \( \xi : F \circ [1] \rightarrow [1] \circ F \).

Prop. (3.4.1.7). An exact functor of triangulated categories is additive.

Proof: Cf.\([\text{Sta}]05QY.\]

Def. (3.4.1.8) [Bi-Exact Functors]. Let \( \mathcal{D}, \mathcal{D}', \mathcal{E} \) be triangulated categories, a bi-exact bifunctor \( F : \mathcal{D} \times \mathcal{D}' \rightarrow \mathcal{E} \) is a functor that for any \( X \in \mathcal{D}, F(X, -) : \mathcal{D} \rightarrow \mathcal{E} \) is an exact functor and for any \( Y \in \mathcal{D}', F(-, Y) : \mathcal{D} \rightarrow \mathcal{E} \) is an exact functor. By (3.4.1.7), any bi-exact functor is bi-additive.

Prop. (3.4.1.9). If \((F,G) : \mathcal{D} \Rightarrow \mathcal{D}' \) is an adjunction pair between triangulated categories and \( F \) is exact, then \( G \) is also an exact functor between triangulated categories.
**3.4. DERIVED CATEGORIES**

**Prop. (3.4.1.10).** If \((F, G) : \mathcal{D} \Rightarrow \mathcal{D}'\) is an adjunction pair between triangulated categories and \(F, G\) are exact, \(F\) is fully faithful and \(\ker(G) = 0\), then this is an equivalence of categories.

**Proof:** By (3.1.1.32), \(u : \text{id} \to gf\) is an isomorphism. Now for any \(X \in \mathcal{D}'\), choose a distinguished triangle \((F(G(X)), X \to Y) \in \text{Tri}(\mathcal{D}')\), which corresponds to \((G(F(G(X))), G(X), G(Y)) \in \text{Tri}(\mathcal{D})\), and by (3.1.1.30), \(G(X) \xrightarrow{h} GFG(X) \to G(X) = \text{id}_X\), so we get an isomorphism of triangles \((G(F(G(X))), G(X), G(Y)) \cong (G(X), G(X), 0)\), so \(G(Y) \cong 0\), and \(Y = 0\) by hypothesis. So \(v : FG \to \text{id}\) is also an isomorphism, so \((F, G)\) is an equivalence. \(\Box\)

**Lemma (3.4.1.11).** If \((X, Y, Z, f, g, h)\) is a distinguished triangle, then \(g \circ f = 0\).

**Proof:** By TR1 \((X, X, 0, \text{id}, 0, 0)\) is a distinguished triangle, and by TR3 there is a map of distinguished triangles

\[
\begin{array}{cccccc}
X & \to & X & \to & 0 & \to & X[1] \\
\| & & \| & & \| & & \\
X & \xrightarrow{f} & Y & \xrightarrow{g} & Z & \xrightarrow{h} & X[1]
\end{array}
\]

so \(g \circ f = 0\). \(\Box\)

**Prop. (3.4.1.12).** Let \(\mathcal{D}\) be a triangulated category and \(C \in \mathcal{D}\) be any object, \(\text{Hom}_\mathcal{D}(-, C)\) and \(\text{Hom}_\mathcal{D}(C, -)\) is (co)homological.

**Proof:** By (3.4.1.3), for any distinguished triangle \((X, Y, Z, f, g, h)\), \(\text{Hom}(C, X) \to \text{Hom}(C, Y) \to \text{Hom}(C, Z) = 0\), and if \(a \in \text{Hom}(C, Y)\) is mapped to \(0 \in \text{Hom}(C, Y)\), then the morphism \((a, 0) : (C, 0) \to (Y, Z)\) extends to a morphism of distinguished triangles \((b, a, 0) : (C, C, 0, \text{id}, 0, 0) \to (X, Y, Z, f, g, h)\), thus \(f \circ b = a\).

The converse case is dual. \(\Box\)

**Cor. (3.4.1.13).** If \((a, b, c) : (X, Y, Z, f, g, h) \to (X', Y', Z', f', g', h')\) is a morphism of distinguished triangles that two of \(a, b, c\) are isomorphisms, then this is an isomorphism of triangles.

In particular, the completion in TR1 is unique (may up to non-unique isomorphism) by TR3.

**Proof:** By 5-lemma, \(\text{Hom}(C, X) \to \text{Hom}(C, X')\) is an isomorphism, then \(X \to X'\) is an isomorphism by Yoneda lemma. \(\Box\)

**Prop. (3.4.1.14).** Let \(\mathcal{D}\) be a triangulated category, then \(f : X \to Y \in \mathcal{D}\) is an isomorphism iff \(C(f) = 0\).

**Proof:** There is a morphism \((\text{id}_X, f, 0) : (X, X, 0, \text{id}, 0, 0) \to (X, Y, C(f), f, g, h)\) by (TR1) and (TR3). By (3.4.1.13), \(f\) is an isomorphism iff \(0 \to C(f)\) is an isomorphism, which is equivalent to \(Z = 0\). \(\Box\)
Prop. (3.4.1.15). In a triangulated category $\mathcal{D}$, any commutative diagram
\[
\begin{array}{ccc}
X & \longrightarrow & Y \\
\downarrow & & \downarrow \\
X' & \longrightarrow & Y'
\end{array}
\]
can be extended to a diagram
\[
\begin{array}{cccccc}
X & \longrightarrow & Y & \longrightarrow & Z & \longrightarrow & X[1] \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
X' & \longrightarrow & Y' & \longrightarrow & Z' & \longrightarrow & X'[1] \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
X'' & \longrightarrow & Y'' & \longrightarrow & Z'' & \longrightarrow & X''[1] \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
\end{array}
\]
where the lower right is anti-commutative.

\textbf{Proof:} Let $(X, Y, Z), (X', Y', Z'), (X, X', X''), (Y, Y', Y''), (X, Y, A)$ be distinguished triangles, then we can find maps $a : Z \to A, b : A \to Y', a' : X'' \to A, b' : A \to Z$ by TR3(3.4.1.1). Then TR4 says $(Z \to A, Y''), (X'' \to Z \to Z')$ is distinguished.

Now let $(X'', Y'', Z'')$ be distinguished, then we use TR4 again to $(X'', A, Y'')$, then $(Z', Z'', Z[1])$ is distinguished, thus so does $(Z \to Z' \to Z'')$.

Now it is left to verify the anti-commutativity of the righthdown square, for this, Cf.[Sta]05R0.

\[\square\]

Prop. (3.4.1.16) [Kernels are Saturated Triangulated Subcategories]. Let $\mathcal{D}, \mathcal{D}'$ be triangulated categories and $\mathcal{A}$ an Abelian category.

- Let $F : \mathcal{D} \to \mathcal{D}'$ be an exact functor, then the full subcategory of $\mathcal{D}$ consisting of objects $X$ that $F(X) = 0$ is a strictly full saturated triangulated subcategory of $\mathcal{D}$, called the \textbf{kernel} of $F$.

- Let $H : \mathcal{D} \to \mathcal{A}$ be a (co)homological functor, then the full subcategory of $\mathcal{D}$ consisting of objects $X$ that $F(X[n]) = 0$ for all $n$ is a strictly full saturated triangulated subcategory of $\mathcal{D}$, called the \textbf{kernel} of $H$.

\textbf{Proof:} Cf.[Sta]05RC, 05RD. \[\square\]

Prop. (3.4.1.17) [$K^*(\mathcal{A})$ is Triangulated]. For Abelian category $\mathcal{A}$, the categories $K^*(\mathcal{A})$ with distinguished triangles (3.3.3.14) is triangulated, and they are all subcategories of $K(\mathcal{A})$. This is hard to verify, but it solves every problem. Cf[Gelfand P246][[Sta]014S]. And an additive functor will induce exact functor between $K^*$ because distinguished is split.

\textbf{Localizations of Triangulated Category}

Def. (3.4.1.18) [Compatible Localizing Systems]. Let $\mathcal{D}$ be a triangulated category, a localizing system (3.1.1.54) $S$ is said to be \textbf{compatible} with the triangulated structure if it satisfies the following axioms:
(LS4): For $s \in S, s[n] \in S$ for any $n \in \mathbb{Z}$.

(LS5): Any two consecutive morphisms of two distinguished triangle can be extended to a morphism of distinguished triangles by morphisms in $S$.

Cor. (3.4.1.19). Let $\mathcal{D}$ be a triangulated category. If a class of morphisms $S$ satisfy (LS1), (LS5) and (LS6), then (LS2) holds as well.

Proof: Let $f : X \to Y \in \mathcal{D}$ and $s : X \to X' \in S$, we can use (TR1) and (TR2) to extend these to a morphism of distinguished triangles

$$
\begin{align*}
X \xrightarrow{f} Y \xrightarrow{s} Z \xrightarrow{\cdot} X[1] \\
\downarrow^s \quad \downarrow^{s'} \quad \downarrow^{s[1]} \\
X' \xrightarrow{s'} Y' \xrightarrow{s} Z' \xrightarrow{\cdot} X'[1]
\end{align*}
$$

The right extension is dual. □

Prop. (3.4.1.20) [Exact Functors and Saturated Localizing Systems]. Let $\mathcal{D}, \mathcal{D}'$ be triangulated categories and $\mathcal{A}$ an Abelian category.

- If $F : \mathcal{D} \to \mathcal{D}'$ is an exact functor and

$$
S = \{ f \in \mathcal{D}|F(f) \text{ is an isomorphism}\},
$$

then $S$ is a saturated localizing system compatible with the triangulated structure (3.4.1.18).

- If $H : \mathcal{D} \to \mathcal{A}$ is a (co)homological functor and

$$
S = \{ f \in \mathcal{D}|H^i(f) \text{ is an isomorphism}\},
$$

then $S$ is a saturated localizing system compatible with the triangulated structure (3.4.1.18).

Proof: Cf. [Sta]05R4, 05R6. □

Prop. (3.4.1.21) [Localed Triangulated Categories]. Let $\mathcal{D}$ be a triangulated category and $S$ is a localizing system compatible with the triangulated structure, then there is a unique triangulated category structure on $S^{-1}\mathcal{D}$ that the localization functor $Q : \mathcal{D} \to S^{-1}\mathcal{D}$ (3.1.1.53) is exact.

Moreover, $S^{-1}\mathcal{D}$ satisfies the following universal properties:

- If $\mathcal{A}$ is an Abelian category and $H : \mathcal{D} \to \mathcal{A}$ is a cohomological functor that $H(s)$ are isomorphisms for all $s \in S$, then the unique factorization $H' : S^{-1}\mathcal{D} \to \mathcal{A}$ s.t. $H' \circ Q = H(3.1.1.57)$ is also a cohomological functor.

- If $\mathcal{D}'$ is a triangulated category and $F : \mathcal{D} \to \mathcal{D}'$ is an exact functor that $F(s)$ are isomorphisms for all $s \in S$, then the unique factorization $F' : S^{-1}\mathcal{D} \to \mathcal{A}$ s.t. $F' \circ Q = F(3.1.1.57)$ is also an exact functor.


Cor. (3.4.1.22) [Kernel of Localizing Functor]. An object $Z \in \mathcal{D}$ is in the kernel of the localizing functor $Q : \mathcal{D} \to S^{-1}\mathcal{D}$ iff it satisfies the following equivalent conditions:

- There exists $Z'$ s.t. $0 : Z \to Z' \in S$.

- There exists $Z'$ s.t. $0 : Z \to Z' \in S$. 

• There exists $Z'$ and a distinguished triangle $(X, Y, Z \oplus Z', f, g, h)$ that $f \in S$.

Proof: Cf. [Sta]05RH.

Prop. (3.4.1.23) [Triangulated Subcategories of Localized Triangulated Categories]. Let $\mathcal{D}$ be a triangulated category and $S$ is a localizing system compatible with the triangulated structure. Let $\mathcal{D}'$ be a full triangulated subcategory of $\mathcal{D}$ and $S'$ is a localizing system of $\mathcal{D}'$. If either of the following holds:

• For any $s : X \to Y \in S$ and $X \in \mathcal{D}'$, there is a morphism $t : Y \to Z$ that $Z \in \mathcal{D}'$ and $t \circ s \in S'$.

• The same as in item 1 but with arrows reversed.

Then the natural functor $(S')^{-1}\mathcal{D}' \to S^{-1}\mathcal{D}$ is fully faithful.

Proof: This is immediate from (3.1.1.60).

Quotients of Triangulated Categories

Def. (3.4.1.24) [Saturated Triangulated Subcategories]. Let $\mathcal{D}$ be a triangulated category, then a full triangulated subcategory $\mathcal{D}'$ is called a saturated triangulated subcategory if whenever $X \oplus Y$ is isomorphic to an object of $\mathcal{D}'$, $X, Y$ are all isomorphic to an object of $\mathcal{D}'$.

Prop. (3.4.1.25) [Full Triangulated Subcategories and Localizing Systems]. Let $\mathcal{D}$ be a triangulated category.

• If $\mathcal{D}'$ is a full triangulated subcategory, then

$$S = \{ f : X \to Y \in \mathcal{D}' | \text{there exists a distinguished triangle } (X, Y, Z, f, g, h), Z \in \mathcal{D}' \}$$

is a localizing system compatible with the triangulated structure of $\mathcal{D}$. And $S$ is saturated iff $\mathcal{D}'$ is saturated.

• If $S$ is a localizing system of $\mathcal{D}$, then $\mathcal{D}' = \ker(\mathcal{D} \to S^{-1}\mathcal{D})$ (3.4.1.21) (3.4.1.16) is a saturated full triangulated subcategory of $\mathcal{D}$.

Proof: 1: Cf. [Sta]05RH.

Def. (3.4.1.26) [Quotient Triangulated Categories]. Let $\mathcal{D}$ be a triangulated subcategory and $\mathcal{B}$ a full triangulated subcategory, define the quotient triangulated category $\mathcal{D}/\mathcal{B}$ as the localized triangulated category $S^{-1}\mathcal{D}$, where $S$ is the localizing system associated to $\mathcal{B}$ (3.4.1.25).

Moreover, $\mathcal{D}/\mathcal{B}$ satisfies the following universal properties:

• If $\mathcal{A}$ is an Abelian category and $H : \mathcal{D} \to \mathcal{A}$ is a cohomological functor that $\mathcal{B} \subset \ker(H)$, then $H$ factors uniquely through $\mathcal{D}/\mathcal{B}$ by a functor $H'$, and $H'$ is also a cohomological functor.

• If $\mathcal{D}'$ is a triangulated category and $F : \mathcal{D} \to \mathcal{D}'$ is a cohomological functor that $\mathcal{B} \subset \ker(F)$, then $F$ factors uniquely through $\mathcal{D}/\mathcal{B}$ by a functor $F'$, and $F'$ is also an exact functor.

Proof: The universal properties follow from the universal properties of localized triangulated categories (3.4.1.21) and the definition of $S$ (3.4.1.25), using the long exact sequence or (3.4.1.14).

Prop. (3.4.1.27) [Saturation]. Let $\mathcal{D}$ be a triangulated category and $\mathcal{D}'$ be a full triangulated subcategory, then the kernel of the quotient map $\mathcal{D} \to \mathcal{D}/\mathcal{D'}$ (3.4.1.26) is a strictly full saturated subcategory consisting of objects $Z \in \mathcal{D}$ that $Z \oplus Z'$ is an object of $\mathcal{D'}$ for some object $Z' \in \mathcal{D}$. In particular, it is the smallest saturated triangulated subcategory containing $\mathcal{D}'$, called the saturation of $\mathcal{D}'$. 
Proof: the kernel is a strictly full saturated subcategory by (3.4.1.16). The description of the objects of kernel follows from the definition (3.4.1.26)(3.4.1.25) and (3.4.1.22). □

Prop. (3.4.1.28) [Kernel of Cohomological Functor is Saturated]. Let $D$ be a triangulated category and $H : D \to A$ is a cohomological functor, then $\ker(H)$ is a saturated full triangulated subcategory (3.4.1.16) whose corresponding saturated localizing system (3.4.1.20) is the set

$$S = \{ f | H^i(f) \text{ is an isomorphism in } A \},$$

and $H$ factors through the quotient $D \to D/\ker(H)$.

Proof: The description of $S$ is clear from the definitions (3.4.1.16)(3.4.1.25) and a use of long exact sequences. The factorization follows from (3.4.1.26). □

K-Groups

Def. (3.4.1.29) [K-Groups of Triangulated Categories]. Let $D$ be a triangulated categories, then the K-group of $D$ is defined to be the quotient

$$\bigoplus_{X \to Y \to Z \text{ distinguished}} 1 \to \bigoplus_{X \in D} K_0(D) \to 0$$

where $e_{X \to Y \to Z}$ is mapped to $e_Y - e_X - e_Z$.

Prop. (3.4.1.30) [Naturality].

- An exact functor between triangulated categories induce a map of their corresponding K-groups,
- A bi-exact bifunctor $F : D \times D' \to E$ (3.4.1.8) induces a bilinear map $K_0(D) \times K_0(D') \to K_0(E)$ sending $([X], [X'])$ to $F(X, X')$.
- A $\delta$-functor from an Abelian category to a triangulated category induces a map of their corresponding K-groups (Notice these two K-groups are defined differently).
- A functor from an exact category to a triangulated category that sends exact sequences to distinguished triangles induces a map of their corresponding K-groups.

Brown Representability

Def. (3.4.1.31) [Generators]. Let $D$ be a triangulated category, a generator of $D$ is an object of $D$ s.t. for any object $K$ of $D$, there exists some integer $n$ and a non-zero map $E[n] \to K$.

Prop. (3.4.1.32). Let $D$ be a triangulated category, then the compact objects of $D$ form a Karoubian, saturated, strictly full triangulated category of $D$.

Proof: Cf. [Sta]09QH. □

Def. (3.4.1.33) [Compactly Generated]. Let $D$ be a triangulated category with arbitrary direct sums, then $D$ is said to be a compactly generated triangulated category if there exists a set of compact objects $\{ E_i \}$ that $\oplus E_i$ is a generator of $D$ (3.4.1.31).

Prop. (3.4.1.34) [Brown Representability]. Let $D$ be a triangulated category with direct sums that is compactly generated. Let $H$ be a contravariant cohomological functor that transforms direct sums into products, then $H$ is representable.
Proof: Cf.[Sta]018F.

Cor. (3.4.1.35) [Adjointness Lemma]. Let \( \mathcal{D} \) be a triangulated category with direct sums that is compactly generated and \( F : \mathcal{D} \to \mathcal{D}' \) an exact functor of triangulated categories that transforms direct limits to direct limits, then \( F \) has an exact right adjoint.

Proof: By Brown representability, for any \( Y \in \mathcal{D}' \), there is an object \( G(Y) \in \mathcal{D} \) that represents the contravariant cohomological functor \( \mathcal{D} \to \text{Ab} : X \mapsto \text{Hom}_{\mathcal{D}'}(F(X), Y) \). Then \( G \) is a functor by Yoneda lemma. It is exact by (3.4.1.9).

2 Derived Category

Def. (3.4.2.1) [Derived Category]. Let \( \mathcal{A} \) be an Abelian category. The full subcategory \( \text{Ac}(\mathcal{A}) \) of \( K(\mathcal{A}) \) consisting of acyclic complexes is a strictly full saturated triangulated subcategory, and its associated saturated localizing system is the class \( \text{QIso}(\mathcal{A}) \) of quasi-isomorphisms.

Thus the kernel of the localizing functor \( Q_{\mathcal{A}} : K(\mathcal{A}) \to \text{QIso}(\mathcal{A})^{-1}K(\mathcal{A}) \) is \( \text{Ac}(\mathcal{A}) \), and \( H^0 \) factors through \( Q_{\mathcal{A}} \). Then the quotient triangulated category (3.4.1.26)

\[
D(\mathcal{A}) = K(\mathcal{A})/\text{Ac}(\mathcal{A}) = \text{QIso}(\mathcal{A})^{-1}K(\mathcal{A})
\]

is called the derived category of \( \mathcal{A} \).

Proof: As \( H^0 \) is a cohomological functor (3.3.3.14), these follows from (3.4.1.28) and (3.4.1.27).

Cor. (3.4.2.2) [Universal Properties of Derived Categories]. Let \( \mathcal{A} \) be an Abelian category,

- By (3.4.1.21), the derived category \( D(\mathcal{A}) \) of an Abelian category \( \mathcal{A} \) has the universal property that any exact functor between Distinguished categories \( F : K(\mathcal{A}) \to \mathcal{D} \) s.t. quasi-isomorphisms is mapped to isomorphisms uniquely factors through \( D(\mathcal{A}) \).

- Let \( F : \mathcal{A} \to \mathcal{B} \) be an exact functor between Abelian categories, then \( F \) induces an exact functor \( F : K(\mathcal{A}) \to K(\mathcal{B}) \) of triangulated categories (3.3.3.17), and it maps quasi-isomorphisms to quasi-isomorphisms, so by item1 induces a morphism of categories \( D(\mathcal{A}) \to D(\mathcal{B}) \).

Prop. (3.4.2.3) [Universal \( \delta \)-Functors]. The functor \( \text{Comp}(\mathcal{A}) \to D(\mathcal{A}) \) is a \( \delta \)-functor.

Proof: Cf.[Sta]014Z.

Prop. (3.4.2.4) [Truncation Triangles]. Let \( \mathcal{A} \) be an Abelian category and \( K^\bullet \in K(\mathcal{A}) \), then for any \( a \in \mathbb{Z} \), the truncation is a distinguished triangle

\[
\tau_{\leq a}K^\bullet \to K^\bullet \to \tau_{\geq a+1}K^\bullet \to \tau_{\leq a}K^\bullet[1].
\]

Proof: This exact sequence comes from the exact sequence \( 0 \to \tau_{\leq a}K^\bullet \to K^\bullet \to K^\bullet/\tau_{\leq a}K^\bullet \) via the \( \delta \)-functor (3.4.2.3) and the fact \( K^\bullet/\tau_{\leq a} \to K^\bullet \to \tau_{\geq a+1}K^\bullet \) is a quasi-isomorphism thus an isomorphism in \( D(\mathcal{A}) \).

Triangulated Subcategories of \( D(\mathcal{A}) \)

Prop. (3.4.2.5). Let \( \mathcal{A} \) be an Abelian category and \( \mathcal{L} \) a full triangulated subcategory of \( K(\mathcal{A}) \), let \( S = \mathcal{L} \cap \text{QIso}(\mathcal{A}) \), then \( S \) is the saturated localizing system compatible with the triangulated structure associated to the cohomological functor \( H^0 \) restricted to \( L(3.4.1.20) \), the we can form the localizing triangulated category \( S^{-1}\mathcal{L}(3.4.1.21) \) and there is a natural exact functor of triangulated categories \( S^{-1}\mathcal{L} \to D(\mathcal{A}) \) by the universal property (3.4.1.21).
Prop. (3.4.2.6) [Full Subcategories of \( D(\mathcal{A}) \)]. Let \( \mathcal{L} \subset \tilde{\mathcal{L}} \) be full triangulated subcategories of \( K(\mathcal{A}) \), and \( S = \mathcal{L} \cap \text{QIs}(\mathcal{A}), \ S = \tilde{\mathcal{L}} \cap \text{QIs}(\mathcal{A}) \). If either of the following holds:

- For any \( s : L_1 \to \tilde{L}_1 \in \tilde{S} \) and \( L_1 \in \mathcal{L} \), there is a morphism \( t : \tilde{L}_1 \to L_2 \) that \( L_2 \in \mathcal{L} \) and \( t \circ s \in \tilde{S} \).
- The same as in item 1 but with arrows reversed.

then the natural functor \( S^{-1} \mathcal{L} \subset \tilde{S}^{-1} \tilde{\mathcal{L}} \) is fully faithful.

\[ \text{Proof: } \] This follows immediately from (3.4.2.5) and (3.4.1.23). \qed

Cor. (3.4.2.7) [Bounded Derived Categories]. For \( * = -, +, b \), the triangulated categories \( D^*(\mathcal{A}) \) are the localized category of \( K^*(\mathcal{A}) \) at the classes of isomorphism in \( K^*(\mathcal{A}) \) (3.4.2.5). Then they are naturally full subcategories of \( D(\mathcal{A}) \), by (3.4.2.6), as the condition is satisfied by (3.3.3.19).

Def. (3.4.2.8) [Derived Category of Serre Subcategories]. If \( \mathcal{B} \) is a Serre subcategory of an Abelian category \( \mathcal{A} \), let \( D_B^*(\mathcal{A}) \) be the full subcategory of \( D^*(\mathcal{A}) \) consisting of objects \( X \) that \( H^n(X) \in \mathcal{B} \) for all \( n \), then \( D_B^*(\mathcal{A}) \) is a strictly full saturated triangulated subcategory of \( D^*(\mathcal{A}) \), as it is just the kernel of the cohomological functor \( H^0 : D^*(\mathcal{A}) \to \mathcal{A} \to \mathcal{A}/\mathcal{B} \) (3.3.2.14)(3.4.1.16).

Also there are natural exact functors \( D^*(\mathcal{B}) \to D_B^*(\mathcal{A}) \), and \( D^*(\mathcal{A})/D_B^*(\mathcal{A}) \to D^*(\mathcal{A}/\mathcal{B}) \) (3.4.1.26).

Prop. (3.4.2.9). The map \( D^*(\mathcal{A}) \to D^*(\mathcal{A}/\mathcal{B}) \) is essentially surjective.

\[ \text{Proof: } \] Cf.[Sta]06XL. \qed

Prop. (3.4.2.10). Let \( \mathcal{B} \subset \mathcal{A} \) be a Serre subcategory and suppose that for any surjection \( X \to Y \in \mathcal{A} \) with \( Y \in \mathcal{B} \), there is a subobject \( X' \subset X \) that \( X' \to Y \) is surjective, then the exact functor \( D^*(\mathcal{B}) \to D_B^*(\mathcal{A}) \) is an equivalence for \( * = - \) or \( b \).

\[ \text{Proof: } \] Cf.[Sta]0FCL. \qed

Prop. (3.4.2.11). If \( (\mathcal{C}, \mathcal{O}) \) is a ringed site and \( \mathcal{A} \subset \text{Mod}_\mathcal{O} \) is the Serre subcategory of torsion modules, then the functor \( D(\mathcal{A}) \to D_A(\mathcal{O}) \) is an equivalence.

\[ \text{Proof: } \] Cf.[Sta]0DD7. \qed

Prop. (3.4.2.12) [Embedding of \( \mathcal{A} \) in \( D(\mathcal{A}) \)]. The natural inclusion \( i : \mathcal{A} \subset D(\mathcal{A}) \) induces an equivalence of \( \mathcal{A} \) with the subcategory of \( D(\mathcal{A}) \) consisting of complexes with cohomology concentrated at degree 0.

An object \( K \in D(\mathcal{A}) \) is called discrete if it is in the essential image of this inclusion.

\[ \text{Proof: } \] The natural map \( H^0 : D(\mathcal{A}) \to \mathcal{A} \) is inverse to \( i \), so \( i \) is faithful. To show it is full, let \((L, f, s^{-1})\) be a morphism from \( i(M) \) to \( i(N) \), then we get a morphism \((H^0(L), H^0(f), H^0(s)^{-1})\), and these two morphisms are both dominated by the morphisms \((\sigma_{\geq n}L, \sigma_{\leq n} \circ f, (\sigma_{\leq n} \circ s)^{-1})\), so they are equal morphisms in \( D(\mathcal{A}) \). But \((H^0(L), H^0(f), H^0(s)^{-1}) = i(s^{-1}f) \) is in the image of \( i \), so \( i \) is full.

The assertion that any complex with cohomology groups concentrated at degree 0 is true by using truncation functors (3.3.3.19).

\[ \text{Proof: } \] \qed

Prop. (3.4.2.13) [K-Groups]. Let \( \mathcal{A} \) be an Abelian category, then the embedding (3.4.2.12) induces an isomorphism of K-groups \( K_0(\mathcal{A}) \cong K_0(D^b(\mathcal{A})) \) (3.4.1.29).
Proof: The map $A \to D^b(A)$ is a $\delta$-functor by (3.4.2.3), thus by (3.4.1.30) induces a map $K_0(A) \cong K_0(D^b(A))$. There is a reverse map $K_0(D^b(A)) \to K_0(A) : X \mapsto \sum_i (-1)^i H^i(X)$, which is inverse the the map above: one direction is clear, for the other, use induction and the truncation triangles (3.4.2.4).

**Def. (3.4.2.14) [Perfect Complex].** Let $\mathcal{A}$ be an Abelian category, a perfect complex in $D(A)$ is a complex that is equivalent to a bounded complex.

**Operations on the Derived Category**

**Lemma (3.4.2.15) [Direct Sum].** If $\mathcal{A}$ is an Abelian category that has exact countable direct sums, then $D(\mathcal{A})$ has countable direct sums given by term-wise direct sums.

**Proof:** A system of morphisms $K_i^* \to L^*$ is a system of quasiisos $M_i^* \to K_i^*$ and $M_i \to L^*$. Then by hypothesis $\oplus M_i^* \to \oplus K_i^*$ is a quasi-iso, thus defines a morphism $\oplus K_i^* \to L^*$. It can be verified that this morphism is unique.

**Lemma (3.4.2.16) [Termwise Colimit as Hocolim].** Let $\mathcal{A}$ be an Abelian category, $L_n^*$ be a system of complexes of $\mathcal{A}$. Assume colimits over $\mathbb{N}$ exists and are exact over $\mathcal{A}$, then the termwise colimit $L^*$ is a derived colimit in $D(\mathcal{A})$.

**Proof:** We have an exact sequence

$$0 \to \oplus L_n^* \to \oplus L_n^* \to L^* \to 0$$

and the termwise direct sum is the direct sum in $D(\mathcal{A})$ by (3.4.2.15), and then $L^*$ is a derived colimit, by (3.3.3.13).

**Bounded (Co)Homological Dimensions**

**Def. (3.4.2.17) [Bounded Cohomological Dimensions].** An exact functor between two derived categories $F : D(\mathcal{A}) \to D(\mathcal{B})$ is called has cohomological dimension bounded by $N$ if $F(D^{\leq m}(\mathcal{A})) \subset D^{\leq m+N}(\mathcal{B})$. Dually, it has homological dimension bounded by $N$ if $F(D^{\geq m}(\mathcal{A})) \subset D^{\geq m-N}(\mathcal{B})$.

**Prop. (3.4.2.18).** If $(F,G) : D(\mathcal{A}) \to D(\mathcal{B})$ is an adjunction pair of exact functors, then $F$ has cohomological dimension bounded by $N$ iff $G$ has homological dimension bounded by $N$.

**Proof:** If $F$ has cohomological dimension bounded by $N$, let $K \in D^{\geq m}(\mathcal{B})$, then

$$\text{Hom}_{D(\mathcal{A})}(\tau_{\leq m-N-1}GK, GK) = \text{Hom}_{D(\mathcal{B})}(F\tau_{\leq m-N-1}GK, K) = 0.$$ 

The dual case is similar.

**3 K-injectives and K-Adapted Classes**

**Prop. (3.4.3.1) [K-injectives].** For an Abelian category $\mathcal{A}$, a complex $I^*$ in $K(\mathcal{A})$ is called a K-injective object iff it satisfies the following equivalent conditions:

- $\text{Hom}_{K(\mathcal{A})}(S^*, I^*) = 0$ for any acyclic $S^*$ in $K(\mathcal{A})$.
- $\text{Hom}_{K(\mathcal{A})}(N^*, I^*) \cong \text{Hom}_{K(\mathcal{A})}(M^*, I^*)$ for quasi-iso $M^* \to N^*$. 

The dual case is similar.
• $\text{Hom}_{K(A)}(X^\bullet, I^\bullet) \cong \text{Hom}_{D(A)}(X^\bullet, I^\bullet)$ for every $X^\bullet$. In particular, a quasi-iso between two $K$-injective objects is an isomorphism in $K(A)$.

Dually, we can define **$K$-projective** objects.

**Proof:** $1 \to 2$ is by (3.3.3.14); $2 \to 3$ use (3.4.2.7), for $3 \to 1$, notice any acyclic complex is quasi-iso to 0.

**Corollary (3.4.3.2).** $K$-Injectives form a full triangulated subcategory of $K(A)$.

**Corollary (3.4.3.3).** If $I^\bullet$ is $K$-injective and quasi-isomorphic to an object in $K^+(A)$, then $I^\bullet \in K^+(A)$.

**Corollary (3.4.3.4) [K-Injective Resolutions are Unique].** by item 3 of the definition (3.4.3.1), $K$-injective resolutions are unique in $K(A)$.

**Proposition (3.4.3.5) [Injectives and $K$-Injective].** Objects $K^+(I_A)$ are all $K$-injectives. Thus the injective resolution is unique in $K^+$. Dually $K^-(P)$ are all $K$-projectives.

**Proof:** Use the first definition of $K$-injectives (3.4.3.1), we prove any morphism $f : S^\bullet \to I^\bullet$ from an acyclic complex to a $K$-injective $I^\bullet$ is homotopic to $0$ by a homotopy $h$. Let $I_k = 0$ for $k < n$, choose $h_k = 0$ for $k \leq n$, then $f_k = dh_k + h_{k+1}d$ for $k < n$. We use induction on $n$ to find $h_k$, $k \leq n$ that $f_k = dh_k + h_{k+1}d$ for $k < n$. Suppose $h_k$ are constructed for $k \leq n$, for $n + 1$, $(f_n - dh_n)d = f_n d - df_{n-1} = 0$, thus $f_n - dh_n = h_{n+1}d$ for some $h_{n+1}$ as $I_n$ is injective. Then we are done.

**Proposition (3.4.3.6).** If a functor $f$ between Abelian categories is left adjoint to an exact functor, then it preserves $K$-injectives (use definition 1).

**Proposition (3.4.3.7) [Products of $K$-Injectives].** Let $A$ be an Abelian category, $I_t$ be $K$-injective complexes. If the termwise product of $I_t$ exists, then it is also $K$-injective, and is the products of $I_t$ in $D(A)$.

**Proof:** It is clearly $K$-injective by (3.4.3.1) item 1 as it is the product in the category $K(A)$. Thus we can easily use the (3.4.3.1) item 3 to see that $I^\bullet$ is also the product in the category $D(A)$.

**Lemma (3.4.3.8).** [Sta] 070M

**Proposition (3.4.3.9) [Functorial $K$-Injective Resolution].** If $A$ is an Abelian category having enough injectives and exact countable products, then every complex is quasi-isomorphic to a $K$-injective complex that each term is injective.

Moreover, if $A$ is a Grothendieck category, then the $K$-injective resolution can be chosen to be functorial.

**Remark (3.4.3.10).** Maybe this can be extended to any large enough class of elements, at least for $K^+(A)$.

**Proof:** By (3.4.3.8), it suffices to show that $K \to R\lim_{\geq -n}K$ is a quasi-isomorphism for all complex $K$. But this is clear from the distinguished triangle

$$R\lim_{\geq -n}K \to \prod_{\geq -n}K \to \prod_{\geq -n}K \to R\lim_{\geq -n}K[1]$$

and the fact $H^p(\prod_{\geq -n}K) = \prod_{p\geq -n}H^p(K)$.

For the second assertion, Cf. [Sta] 079P.
K-Adapted Classes

**Def. (3.4.3.11) [K-Adapted Classes].** Let \( \mathcal{A} \) be an Abelian category, \( \mathcal{D} \) a triangulated category and \( F : K(\mathcal{A}) \to \mathcal{D} \) a triangulated functor, a **K-adapted class** for \( F \) is a full triangulated subcategory \( \mathcal{R} \subset K(\mathcal{A}) \) that

- If \( I \to I' \) is a quasi-isomorphism in \( \mathcal{R} \), then \( F(I) \to F(I') \) is an isomorphism in \( \mathcal{D} \).
- Every \( A^\bullet \in K(\mathcal{A}) \) admits some quasi-isomorphism \( A^\bullet \to I^\bullet \) where \( I^\bullet \in \mathcal{R} \).

**Cor. (3.4.3.12) [K-Injective is K-Adapted].** If \( \mathcal{A} \) has sufficiently many K-injectives, then the class of K-injectives is K-adapted to any left exact functor \( F \), by (3.4.3.2) and (3.4.3.1).

4 Derived Functors

**Def. (3.4.4.1) [Right Derived Functors].** Let \( \mathcal{A} \) be an Abelian category, \( E \) a triangulated category and \( F : K(\mathcal{A}) \to E \) an exact functor between triangulated categories. Then a **right derived functor** of \( F \) is an exact functor \( RF : D(\mathcal{A}) \to \mathcal{D} \) together with a natural transformation \( \eta : F \to RF \circ Q_A \) that satisfies the following universal property: For any exact functor \( G : D(\mathcal{A}) \to \mathcal{D} \) and a natural transformation \( \eta' : F \to G \circ Q_A \), there is a natural transformation \( \theta : RF \to G \) that

\[
\eta' = (\theta \circ Q_A) \circ \eta.
\]

In particular, if \( RF \) exists, then it is unique up to unique isomorphism of exact functors.

**Prop. (3.4.4.2) [Derived Functors via K-Adapted Classes].** Let \( \mathcal{A} \) be an Abelian category, \( \mathcal{D} \) a triangulated category and \( F : K(\mathcal{A}) \to E \) an exact functor, if there exists a K-adapted class \( \mathcal{R} \) for \( F \), then \( RF \) exists. Moreover, for \( I \in \mathcal{R} \), the morphism \( \eta_I : F(I) \to RF \circ Q_A(I) \) is an isomorphism in \( \mathcal{D} \).

**Proof:** Let \( S = \mathcal{R} \cap \text{QIso}(\mathcal{A}) \), then \( \mathcal{R}, K(\mathcal{A}) \) and the localizing systems \( S, \text{QIso}(\mathcal{A}) \) satisfy the conditions in (3.4.2.6), so \( \iota : S^{-1} \mathcal{R} \subset D(\mathcal{A}) \) is a full triangulated subcategory, and it is also essentially surjective, thus it is an equivalence of categories. Let \( I \) be a right adjoint of the inclusion, then \( I \) is also an exact functor (3.4.1.9), and there is a natural isomorphism \( \zeta : \text{id}_{D(\mathcal{A})} \cong \iota \circ I \).

By the universal property, there is an exact functor \( F_{\mathcal{R}} : S^{-1} \mathcal{R} \to \mathcal{D} \) extending \( F|_{\mathcal{R}} \). Define

\[
RF = F_{\mathcal{R}} \circ I : D(\mathcal{A}) \to \mathcal{D}.
\]

To construct \( \eta : F \to RF \circ Q_A \), for any \( X \in \text{Ob}(K(\mathcal{A})) = \text{Ob}(D(\mathcal{A})) \), the isomorphism \( \zeta \) gives an isomorphism \( X \cong \iota(I(X)) \), which is represented by a roof \( (R, f, s^{-1}, f, s) \in \text{QIso}(\mathcal{A}) \), and we can assume \( R \in \text{Ob}(\iota(S^{-1} \mathcal{R})) = \text{Ob}(\mathcal{R}) \) by hypothesis, thus \( s \in S \), and \( F(s) \) is an isomorphism in \( E \) by hypothesis. Thus we get a morphism \( \eta_X : F(s)^{-1} \circ F(f) : F(X) \to F(\iota(I(X))) = RF(Q_A(X)) \).

This \( \eta_X \) is independent of the representation given, because if there is another dominant roof \( (R', t \circ f, (t \circ s)^{-1}) \), where \( t : R \to R' \in S \), then \( F(t \circ s)^{-1} \circ F(t \circ f) = F(s)^{-1} \circ F(f) \in E \).

And for a morphism \( f : X \to Y \in K(\mathcal{A}) \), \( \zeta \) gives a commutative diagram

\[
\begin{array}{ccc}
X & \xrightarrow{\xi_X} & \iota(I(X)) \\
\downarrow f & & \downarrow \iota(I(f)) \\
Y & \xrightarrow{\xi_Y} & \iota(I(Y))
\end{array}
\]

in \( D(\mathcal{A}) \) where \( \xi_X, \xi_Y \) are represented by \( (R_X, f_X, s_X^{-1}), (R_Y, f_Y, s_Y^{-1}) \), and \( I(f) \) is represented \( (R_0, f_0, s_0^{-1}) \), then we can construct roof to realize this commutative diagram in \( K(\mathcal{A}) \) and show
there is a commutative diagram

\[
\begin{array}{ccc}
F(X) & \xrightarrow{F(s_X)\circ F(f_X)} & RF(Q_A(X)) \\
\downarrow{F(f)} & & \downarrow{F(s_0)\circ F(f_0)=RF\circ Q_A(f)} \\
F(Y) & \xrightarrow{F(s_Y)\circ F(f_Y)} & RF(Q_A(Y))
\end{array}
\]

in \( E \), which means \( \eta : F \rightarrow RF \circ Q_A \) is a natural isomorphism.

Notice that \( \eta_I \) is an isomorphism for \( I \in \mathcal{R} \), because in this case \( F(f_I), F(s_I) \) are both isomorphisms.

It remains to show the universal properties of \( \eta \): Given any exact functor \( G : D(A) \rightarrow E \) and a natural transformation \( \eta' : F \rightarrow G \circ Q_A \), for any \( X \in \text{Ob}(K(A)) = \text{Ob}(D(A)) \), we get a morphism \( \eta'_X : F(X) \rightarrow G(X) \) in \( E \). Notation as before, because \( \eta' \) is a natural transformation, we get a commutative diagram in \( K(A) \)

\[
\begin{array}{ccc}
F(X) & \xrightarrow{\eta'_X} & G(X) \\
\downarrow{F(f)} & & \downarrow{G(Q_A(f))} \\
F(R_X) & \xrightarrow{\eta'_R_X} & G(R_X) \\
\downarrow{F(s)} & & \downarrow{G(Q_A(s))} \\
F(\iota(I(X))) & \xrightarrow{\eta'_\iota(I(X))} & G(\iota(I(X)))
\end{array}
\]

In \( E \). As \( \zeta_X = (R_X, f, s^{-1}) \) is an isomorphism between \( X \) and \( \iota(I(X)) \), \( f, s \) are both quasi-isomorphisms, thus the vertical arrows are both isomorphisms, and we get a commutative diagram

\[
\begin{array}{ccc}
F(X) & \xrightarrow{\eta_X} & G(X) \\
\downarrow{\eta'_X} & & \downarrow{G(\zeta_X)} \\
RF(Q_A(X)) & \xrightarrow{\eta'_\iota(I(X))} & G(\iota(I(X)))
\end{array}
\]

So we can define

\[
\theta_X = (G(\zeta_X))^{-1} \circ \eta'_\iota(I(X)) : RF(Q_A(X)) \rightarrow G(X),
\]

then it is is functorial in \( X \) as both \( \eta'_\iota(I(X)) \) and \( G(\zeta_X) \) are functorial in \( X \), so defines a natural transformation \( RF \circ Q_A \rightarrow G \) that \( (\theta \star Q_A) \circ \eta = \eta' \).

For the uniqueness of \( \eta \): For any \( X \in \text{Ob}(S^{-1}\mathcal{R}) = \text{Ob}(\mathcal{R}) \), \( \eta_X \) is an isomorphism, thus \( \eta_X \) is determined, but \( \iota : S^{-1}\mathcal{R} \rightarrow D(A) \) is essentially surjective, so \( \eta_X \) is determined for any \( X \in D(A) \).

\[
\square
\]

\textbf{Cor. (3.4.4.3) [Derived Functors via K-Injective Classes].} Let \( A \) be an Abelian category, \( E \) a triangularized category and \( F : K^+(A) \rightarrow E \) an exact functor, if \( K^+(A) \) has enough K-injectives, then the class of K-injectives is K-adapted to \( F(3.4.3.12) \), so \( RF : D^+(A) \rightarrow E \) exists. Moreover, for any K-injective \( I^* \), the morphism \( \eta_{I^*} : F(I^*) \rightarrow RF \circ Q_A(I^*) \) is an isomorphism in \( E \).
Cor. (3.4.4.4) [Derived Functors via Injectives]. Let \( \mathcal{A}, \mathcal{B} \) be Abelian categories s.t. \( \mathcal{A} \) has enough injective and countable products, and \( F : \mathcal{A} \to \mathcal{B} \) an additive functor, then \( K^*(F) : K^*(\mathcal{A}) \to D^*(\mathcal{A}) \) is an exact functor by (3.4.1.17), and \( K^*(\mathcal{A}) \) has enough K-injectives by (3.4.3.9).

However, this is useless unless \( F \) is left exact in which case we see \( R^0 F(A) = F(A) \) for any \( A \in \mathcal{A} \) by (3.4.4.3).

Cor. (3.4.4.5) [Naturality]. If \( \eta : F \to F' \) is a natural transformation of left-exact functors, then by universal property (3.4.4.1), there is a natural transformation \( R\eta : RF \to RF' \) inducing a long exact sequence about cohomology groups extending \( \eta \).

Prop. (3.4.4.6) [Composition of Derived Functors]. \( \mathcal{A}, \mathcal{B} \) be Abelian categories and \( \mathcal{D} \) a triangulated category. If \( F : K^*(\mathcal{A}) \to K^*(\mathcal{B}), G : K^*(\mathcal{B}) \to \mathcal{D} \) are exact functors between triangulated categories, and \( R_{\mathcal{A}} \) is K-adapted to \( F \) and \( G \circ F \), \( R_{\mathcal{B}} \) is K-adapted to \( G \), then the natural transformation \( R(G \circ F) \to RG \circ RF \) is an isomorphism.

**Proof:** \( RF \) is isomorphic to \( F \) on \( R_{\mathcal{A}}, \) so for any \( A^* \in K^*(\mathcal{A}) \), choose some quasi-isomorphism \( A^* \to R \), where \( R \in R_{\mathcal{A}}, \) then there is a commutative diagram
\[
\begin{array}{ccc}
R(G \circ F)(A^*) & \xrightarrow{\cong} & R(G \circ F)(R) \\
\downarrow & & \downarrow \\
RG \circ RF(A^*) & \xrightarrow{\cong} & RG \circ RF(R)
\end{array}
\]
\[
R(G \circ F)(R) \xrightarrow{\cong} G \circ F(R),
\]
and we are done. \( \square \)

Def. (3.4.4.7) [Universal \( \delta \)-Functor]. A universal \( \delta \)-functor between Abelian categories is one that any natural transformation from \( T^0 \) to another \( \delta \)-functor will generate a \( \delta \)-map. A effaceable \( \delta \)-functor is one that for any \( n > 0 \) and any object \( A \), there is an injection \( A \to B \) that \( T^n(A) \to T^n(B) = 0 \).

Prop. (3.4.4.8) [Grothendieck]. A \( \delta \)-functor is universal if it is effaceable.

**Proof:** We construct by induction on \( n \). choose a \( 0 \to A \to B \to C \to 0 \) such that \( T^{n+1}(A) \to T^{n+1}(B) = 0 \) then there is an isomorphism \( T^{n+1}(A) \cong \text{Coker}(T^n(B) \to T^n(C)), \) and so we can construct the map on \( T^{n+1} \) induces by
\[
\text{Coker}(T^n(B) \to T^n(C)) \to \text{Coker}(G^n(B) \to G^n(C)) \to G^{n+1}(A).
\]
This can be verified to be a \( \delta \) map. \( \square \)

Prop. (3.4.4.9). The derived functors form a universal \( \delta \)-functor (when it exists).

**Proof:** It is a \( \delta \) functor by (3.4.2.1), it is universal by (3.4.4.8). \( \square \)

Prop. (3.4.4.10). Derived functor commutes with filtered colimits on a Grothendieck Abelian category, this is by AB5.
Prop. (3.4.4.11) [Hypercohomology]. Given an Abelian category $\mathcal{A}$ with enough injectives, $\mathcal{B}$ a complete Abelian category, $F : \mathcal{A} \rightarrow \mathcal{B}$ a left exact functor, and $K \in K(\mathcal{A})$, we can define the right hyper-derived functor of $F$ at $K$ as $RF(K) = \text{Tot}^n F(P) \in K(\mathcal{B})$ where $K \rightarrow P$ is a Cartan-Eilenberg resolution of $K$. and the hypercohomologies of $F$ at $K$ as $R^n F(K) = H^n(\text{Tot}^n F(P))$. Dually we can define the left hyper-derived functor and hyperhomologies.

For complexes in $K^+(\mathcal{A})$, there is no restriction and the right derived-hyper functor descends to a functor from $D^+(\mathcal{A}) \rightarrow D^+(\mathcal{B})$.

When the Abelian category $\mathcal{A}$ satisfies AB3* and AB4*, i.e. the direct product is exact, then $\text{Tot}^n$ of the Cartan-Eilenberg resolution of any complex is a quasi-isomorphism to it by the dual of??. (Take horizontal filtration, AB4* assures it collapse).

Derived Bifunctors

Def. (3.4.4.12) [Right Derived Functors of Bi-Exact Bi-Functors]. Let $\mathcal{A}, \mathcal{B}$ be Abelian categories and $F : K(\mathcal{A}) \times K(\mathcal{B}) \rightarrow \mathcal{D}$ be bi-exact bifunctor between triangulated categories, a right derived functor of $F$ is a bi-exact bifunctor $RF : D(\mathcal{A}) \times D(\mathcal{B}) \rightarrow \mathcal{D}$ together with a natural transformation $\eta : F \rightarrow RF \circ (Q_\mathcal{A} \times Q_\mathcal{B})$ that satisfies the following universal property: For any bi-exact bifunctor $G : D(\mathcal{A}) \times D(\mathcal{B}) \rightarrow \mathcal{D}$ and a natural transformation $\eta' : F \rightarrow G \circ (Q_\mathcal{A} \times Q_\mathcal{B})$, there is a natural transformation $\theta : RF \rightarrow G$ that $\eta' = (\theta \circ (Q_\mathcal{A} \times Q_\mathcal{B})) \circ \eta$.

In particular, if $RF$ exists, then it is unique up to unique isomorphisms of bi-exact bi-functors.

Prop. (3.4.4.13) [Deriving Bi-Exact Functors]. Let $\mathcal{A}_1, \mathcal{A}_2$ be Abelian categories and $F : K(\mathcal{A}_1) \times K(\mathcal{A}_2) \rightarrow \mathcal{D}$ be bi-exact bifunctor between triangulated categories, if $\mathcal{R}_i$ are full subcategories of $\mathcal{A}_i$ s.t.

- If $R_i \rightarrow R_i'$ are quasi-isomorphisms in $\mathcal{R}_i$, the induced map $F(R_1, R_2) \rightarrow F(R_1', R_2')$ is an isomorphism in $\mathcal{D}$.
- Any $A_i^\bullet \in K(\mathcal{A}_i)$ admits some quasi-isomorphism $A_i^\bullet \rightarrow I_i^\bullet$ where $I_i^\bullet \in \mathcal{R}_i$.

Then the right derived functor (3.4.4.12) $RF$ exists. Moreover, for any $R_i \in \mathcal{R}_i$, $\eta_{R_1, R_2} : F(R_1, R_2) \rightarrow RF \circ (Q_{A_1} \times Q_{A_2})(R_1, R_2)$ is an isomorphism.

Proof: Let $S_i = \mathcal{R}_i \cap \text{QIso}(\mathcal{A}_i)$, then $\mathcal{R}_i, K(\mathcal{A}_i)$ and the localizing systems $\mathcal{S}_i, \text{QIso}(\mathcal{A}_i)$ satisfy the conditions in (3.4.2.6), so $\iota : S_i^{-1} \mathcal{R}_i \subset D(\mathcal{A}_i)$ is a full triangulated subcategory, and it is also essentially surjective, thus it is an equivalence of categories. Let $I_i$ be a right adjoint of the inclusion, then $I_i$ is also an exact functor (3.4.1.9), and there is a natural isomorphism $\zeta_i : \text{id}_{D(\mathcal{A}_i)} \cong \iota_i \circ I_i$.

By hypothesis of universal properties, the functor $F$ extends to an exact functor $F_\mathcal{R} : \prod_i S_i^{-1} \mathcal{R}_i \rightarrow \mathcal{D}$. Define

$$RF = F_\mathcal{R} \circ \prod_i I_i : \prod_i D(\mathcal{A}_i) \rightarrow \mathcal{D}.$$  

The rest of the proof is verbatim as that of (3.4.4.2).

Remark (3.4.4.14). This proposition can be naturally extended to any multi-exact multi-functors. In fact, I suppose this can be deduced from the usual derived functors by considering the tensor product category $\mathcal{A} \otimes \mathcal{B}$, Cf. [Basic Concepts of Enriched Category Theory, Kelly].

Prop. (3.4.4.15) [Derived Functors of Adjunctions]. Let $\mathcal{A}_1, \mathcal{A}_2$ be Abelian categories and $(F, G)$ be an adjunction between $K(\mathcal{A}_1)$ and $K(\mathcal{A}_2)$, and $\mathcal{R}_i$ are full subcategories of $\mathcal{A}_i$ s.t.

- If $R_i \rightarrow R_i'$ are quasi-isomorphisms in $\mathcal{R}_i$, the induced map $F(R_1', R_2) \rightarrow \text{Hom}_B(R_1, R_2')$ is an isomorphism in $D(\mathcal{A}_B)$.  


Any $A_1^\bullet \in K(A_1)$ admits some quasi-isomorphism $A_1^\bullet \to I_1^\bullet$ where $I_1^\bullet \in \mathcal{R}_1$.

Any $A_2^\bullet \in K(A_2)$ admits some quasi-isomorphism $I_2^\bullet \to A_2^\bullet$ where $I_2^\bullet \in \mathcal{R}_2$.

then there is a functorial isomorphism

$$R\text{Hom}(LF(A^\bullet), B^\bullet) \cong R\text{Hom}(A^\bullet, RG(B^\bullet)) \in D(\text{Ab})$$

for $A^\bullet \in K(A), B^\bullet \in K(B)$. In particular,

$$\text{Hom}(LF(A^\bullet), B^\bullet) \cong \text{Hom}(A^\bullet, RG(B^\bullet)) \in \text{Ab}$$

Proof: Regard both side as a right derived functor of the isomorphic bi-exact bi-functors

$$K(A)^{op} \times K(B) \to D(\text{Ab}) : (A^\bullet, B^\bullet) \mapsto \text{Hom}_B^\ast(F(A^\bullet), B^\bullet) \cong \text{Hom}_A^\ast(A^\bullet, G(B^\bullet)) \in D(\text{Ab}).$$

Then the functorial isomorphism follows from universal properties. □

Prop. (3.4.4.16). Situation as in (3.4.4.15), for any $K^\bullet \in K(A_2)$, there is a commutative diagram of adjunction maps

$$\begin{array}{ccc}
LF \circ G(K^\bullet) & \longrightarrow & F \circ G(K^\bullet) \\
\downarrow & & \downarrow \\
LF \circ RG(K^\bullet) & \longrightarrow & K^\bullet
\end{array}$$

Proof: Cf. [Sta] 0FPI. □

Internal Hom

Def. (3.4.4.17) [Internal Hom]. If $\mathcal{A}$ is an Abelian category and $K(\mathcal{A})$ has enough K-injectives or enough K-projectives, thus by (3.4.4.13), we can define the internal Hom

$$R\text{Hom} : D(\mathcal{A})^{op} \times D(\mathcal{A}) \to D(\mathcal{A})$$

as the right derived functor of the bi-exact bifunctor $\text{Hom}^\ast : K(\mathcal{A})^{op} \times K(\mathcal{A}) \to D(\text{Ab})$.

Prop. (3.4.4.18) [Ext Groups]. For $X, Y \in D(\mathcal{A})$, define the ext groups

$$\text{Ext}^i_{\mathcal{A}}(X, Y) = H^i(R\text{Hom}(X, Y)) = \text{Hom}_{D(\mathcal{A})}(X[0], Y[i]).$$

Proof: To show $H^i(R\text{Hom}(X, Y)) = \text{Hom}_{D(\mathcal{A})}(X[0], Y[i])$, choose a K-injective resolution $Y \to I^\bullet$ of $Y$, then

$$H^i(R\text{Hom}(X, Y)) = H^i(\text{Hom}_{\mathcal{A}}(X, I^\bullet)) = \text{Hom}_{K(\mathcal{A})}(X, I^\bullet[n]) = \text{Hom}_{D(\mathcal{A})}(X, I^\bullet[n]) = \text{Hom}_{D(\mathcal{A})}(X, Y[n]),$$

by (3.3.3.10) and the definition (3.4.3.1). □

Prop. (3.4.4.19). If $P^\bullet \to X^\bullet$ is a projective resolution, then $\text{Ext}^i(X^\bullet, Y^\bullet) = \text{Hom}_{K(\mathcal{A})}(P^\bullet[-i], Y^\bullet)$. If $Y^\bullet \to I^\bullet$ is an injective resolution, then $\text{Ext}^i(X^\bullet, Y^\bullet) = \text{Hom}_{K(\mathcal{A})}(X^\bullet, I^\bullet)$.

Prop. (3.4.4.20). If $X \in D^{\leq a}(\mathcal{A})$ and $Y \in D^{\geq b}(\mathcal{A})$, then for $i < b - a$, $\text{Ext}^i(X, Y) = 0$, and $\text{Ext}^{b-a}(X, Y) = \text{Hom}(H^a(X), H^b(Y))$.

In particular, for $A, B \in \mathcal{A}$, $\text{Ext}^i(A, B) = 0$ for $i < 0$ and $\text{Ext}^0(A, B) = \text{Hom}(A, B)$. 
Proof: This is because $X$ can be represented by $K\leq a(P)$ or $Y$ can be represented by $K\geq b(I)$. □

**Prop. (3.4.4.21) [Long Exact Sequences]**. Let $0 \to A_1 \to A_2 \to A_3 \to 0$ be an exact sequence in $\mathcal{A}$, then it is distinguished in $D(\mathcal{A})$, so by (3.4.1.12), for any $B \in \mathcal{A}$, there is a long exact sequence

$$0 \to \text{Hom}(B, A_1) \to \text{Hom}(B, A_2) \to \text{Hom}(B, A_3) \to \text{Ext}^1(B, A_1) \to \text{Ext}^1(B, A_2) \to \ldots,$$

and similarly a long exact sequence

$$0 \to \text{Hom}(A_3, B) \to \text{Hom}(A_2, B) \to \text{Hom}(A_1, B) \to \text{Ext}^1(A_3, B) \to \text{Ext}^1(A_2, B) \to \ldots.$$

**Def. (3.4.4.22) [Yoneda Extensions]**. Let $\mathcal{A}$ be an Abelian category and $A, B \in \mathcal{A}$, a **Yoneda extension** of $B$ by $A$ of degree $d$ is an exact sequence

$$0 \to A \to Z_{d-1} \to \ldots \to Z_0 \to B \to 0.$$

One Yoneda extension is said to **dominate** another if there is a map of extensions s.t. restricts to $\text{id}_A$ and $\text{id}_B$. Two Yoneda extensions of degree $d$ is called **equivalent** if they are dominated by a common Yoneda extension. (Notice this is an equivalence relation by (3.4.4.23).

**Prop. (3.4.4.23) [Ext and Yoneda Extensions]**. There is a map from the equivalence classes of Yoneda extensions of degree $d$ of $B$ over $A$ to $\text{Ext}^d(B, A)$, which maps the exact sequence $0 \to A \to Z_{d-1} \to \ldots \to Z_0 \to B \to 0$ to $fs^{-1} \in \text{Hom}_{D(\mathcal{A})}(B[0], A[d])$, where $f : (A \to Z_{d-1} \to \ldots \to Z_0) \to A[d]$, and $s : (A \to Z_{d-1} \to \ldots \to Z_0) \to B[0]$.

and corresponds to the set of $i$-term extensions of $Y$ by $X$. There is a natural map

$$\text{Ext}^i_A(X, Y) \times \text{Ext}^j_A(Y, Z) \to \text{Ext}^{i+j}_A(X, Z)$$

by composition or equivalently the conjunction of extensions.

Proof: Cf.[Sta]06XU. □

**Prop. (3.4.4.24) [Explicit Addition as Extensions]**. In an Abelian category with enough injectives, the extension $\text{Ext}^1(N, M)$ is equivalent with the Abelian group of extensions with Baer sum as addition.

Proof: We choose a projective resolution $0 \to K \to P \to N \to 0$, so $\text{Hom}(K, M) \to \text{Ext}^1(N, M)$ is surjective, so choose a lifting and the pushout $0 \to M \to L \to N \to 0$ with be the corresponding extension, Now the Baer sum is easy to define and verify. □

**Prop. (3.4.4.25)**. If $\mathcal{A}$ is an Abelian category and $p \geq 0$ s.t. $\text{Ext}^p(A, B) = 0$ for any $A, B \in \mathcal{A}$, then $\text{Ext}^i(A, B) = 0$ for any $i \geq p$ and $A, B \in \mathcal{A}$.

Proof: Any Yoneda extension of degree $i$ is a conjunction of extensions of degree $p$ and degree $i-p$. □

**Cor. (3.4.4.26)**. If $\mathcal{A}$ is an Abelian category s.t. $\text{Ext}^2(A, B) = 0$ for any $A, B \in \mathcal{A}$, then each object of $D^b(\mathcal{A})$ is isomorphic to a direct sum of cohomologies.

Proof: Let $K$ be represented by $K^\bullet \in D^{[a,b]}(\mathcal{A})$. We use induction on $b-a$. If $b-a > 0$, then there is a distinguished triangle $\tau_{b-1}K \to K^\bullet \to H^b(K)[-b] \to \tau_{b-1}K^\bullet[1]$. (3.4.2.4). If we can prove $H^b(K)[-b] \to \tau_{b-1}K^\bullet[1]$ is 0, then we finish by (3.4.1.4). But by induction and the hypothesis,

$$\text{Hom}_{D(\mathcal{A})}(H^b(K)[-b], \tau_{b-1}(K^\bullet)[1]) = \bigoplus_{b \leq i \leq b} \text{Ext}^{b-i+1}_A(H^b(K), H^i(K)),$$

which vanishes by hypothesis. □
Acyclic Objects

Prop. (3.4.4.27) [F-Acyclic Objects]. For a left exact functor $F$, an object $X$ is (right)$F$-acyclic if $RF$ is defined for $X$, and the natural map $F(X) \to RF(X)$ is an isomorphism, or equivalently $R^iF(X) = 0$ for all $i > 0$.

Then there is an adapted class of $F$ iff the class of $F$-acyclic objects $Acy(F)$ is sufficiently large, and in this case adapted classes of $F$ are exactly sufficiently large subclasses of $Acy(F)$, and $Acy(F)$ contains all injectives. (But the class of injectives may not be sufficiently large!)

Proof: Cf.[Gelfand P195]. □

Prop. (3.4.4.28) [Leray’s Acyclicity Lemma]. Let $F : A \to B$ be an additive functor and $RF$ is everywhere defined, then for a complex $A^\bullet$ in $K^+(A)$ consisting of $F$-acyclic objects, the natural map $F(A^\bullet) \to RF(A^\bullet)$ is an isomorphism.

Proof: Cf.[Sta]015E. This may be equivalent to (3.4.4.27). □

Prop. (3.4.4.29) [Acyclic Criterion]. Let $F$ be a left exact functor from an Abelian category $C$ of enough injectives to another Abelian category, $T$ is a class of objects of $C$ that satisfies:

- $T$ is sufficiently large.
- Cokernel of maps between elements of $T$ is in $T$ and $0 \to F(A) \to F(A') \to F(\text{Coker}) \to 0$ is exact. (To use induction).

Then every object of $T$ is $F$-acyclic.

Proof: Cf.[Sta]05T8. □

Prop. (3.4.4.30) [Injectives are adapted]. By (3.4.3.5), if $A$ contains sufficiently many injectives, then injective objects are adapted to any left exact functor $F$. (Because id on acyclic injective complexes is homotopic to 0 by the lemma).

5 (Co)Homological Dimension

Prop. (3.4.5.1). If $A$ has enough projectives, then the projective dimension of an object $X$ is the length of projective resolutions. (Use resolution and long sequence).

Prop. (3.4.5.2) [Hilbert Theorem]. For an Abelian category $A$, the category $A[T]$ is an Abelian category. If $A$ has enough projectives and have infinite direct sum, then $\text{dhp}_{A[T]}(X, t) \leq \text{dhp}_A(X) + 1$ and equality with $t = 0$.

Cor. (3.4.5.3). The Categories $\text{Ab}$ and $K[X]$-mod have homological dimension 1. $K[X_1, \ldots, X_k]$ has homological dimension $k$.

Def. (3.4.5.4) [Injective Amplitude]. Let $A$ be an Abelian category with enough injectives, $K \in D(A)$ is said to have finite injective dimension if $K \in D^b(I)$. It is said to have injective amplitude in $[a, b]$ if $K \in D[a, b](I)$.

Prop. (3.4.5.5). Let $A$ be an Abelian category and $K \in D(A)$,

- If $K \in D^b(A)$ and $H^i(K)$ all have finite injective dimensions, then $K$ also has finite injective dimension.
- If $K$ is represented by $K^\bullet \in K^b(A)$, and $K^i$ all have finite injective dimensions, then $K$ also has finite injective dimension.
3.4. DERIVED CATEGORIES

Proof: 1 follows from the Grothendieck spectral sequence applied to the functor $\text{Hom}(N, -)$ for any $N \in \mathcal{A}$ and the CE resolution of $K$ (3.3.5.9).

2 follows from 1 as we can use induction to show all $H^i(K)$ has finite injective dimensions. □

6 Derived Limits and Colimits

Def. (3.4.6.1) [Derived (Co)Limits]. Let $\mathcal{D}$ be a triangulated category, and $(K_n, f_n)$ is an inverse system of objects in $\mathcal{D}$, then an object $K$ is called the derived colimit of it iff there exists and there is a distinguished triangle

$$\oplus K_n \rightarrow K \rightarrow \oplus K_n[1]$$

where the first map is given by $(1 - f_n)$. By TR1, the derived colimit exists as long as $\oplus K_n$ exists, and by TR3 (3.4.1.12), the colimit is unique if it exists. And by TR3 again a morphism of systems induces a morphism of colimits.

The definition of derived limit is dual.

Prop. (3.4.6.2) [Cofinality of Hocolim]. Let $\mathcal{D}$ be a triangulated category and $(K_n, f_n)$ be a system, if $0 \leq n_{i_0} < n_{i_1} < \ldots$ be a sequence of integers, then there is an isomorphism $\text{hocolim} K_{n_i} \rightarrow hocolim K_n$.

Proof: Cf. [Sta]0CRJ. □

Lemma (3.4.6.3). Let $\mathcal{A}$ be an Abelian category with countable products and enough injectives, then the derived limit $R\lim$ for any inverse system in $D^+(\mathcal{A})$ exists.

Proof: It suffices to show $\prod K^\bullet_n$ exists in $D(\mathcal{A})$. But every $K^\bullet_n$ has a $K$-injective resolution $I^\bullet_n$, by (3.3.5.9)(3.4.3.5). And then $\prod K^\bullet_n$ is represented by $\prod I^\bullet_n$, by (3.4.3.7). □

Def. (3.4.6.4) [Rlim]. $R\lim$ on an Abelian category $\mathcal{A}$ with countable products and enough injectives is defined to be the right derived functor of $\lim : \mathcal{A}^\mathbb{N} \rightarrow \mathcal{A}$. Equivalently, it is just the derived limit (3.4.6.1)(3.4.6.3) in $D(\mathcal{A})$ restricted to the case where each $K_n$ is discrete.

Prop. (3.4.6.5). Let $R\lim A$ exists on $\mathcal{A}$, if $K_n, f_n$ is a system of objects in $D^+(\mathcal{A})$, then there are exact sequences

$$0 \rightarrow R^1 \lim (H^m(K_n), f_n) \rightarrow R^{m+1} \lim (K_n, f_n) \rightarrow \lim (H^m(K_n), f_n) \rightarrow 0.$$

Immediately from the definition (3.4.6.1).

7 Spectral Sequence

Reference for this section is [Weibel Ch5]. All the definition below is dual for homology and cohomology, just rotate the diagram 180 degree.

We work in an Abelian category.

Def. (3.4.7.1). A convergent Spectral Sequence is a three-dimensional arrange of entries $E^{p,q}_r$ that:

1. $d_r : E^{p,q}_r \rightarrow E^{p+r,q-r+1}_r$ that $d_r d_r = 0$.

2. $H^p,q(E^{p,q}_r) \cong E^{p,q}_{r+1}$. And $E^{p,q}_r$ has a direct limit $E^{p,q}_\infty$.  

3. There is a complex $E^\bullet$ and a decreasing bounded filtration $F^pE^n$ on each $E^n$ and $E^{p,q}_\infty \cong F^pE^{p+q}/F^{p+1}E^{p+q}$.

**Def. (3.4.7.2)** [Notations For Cohomological Spectral Sequence].
- The cohomology filtration is called **bounded below** $F^{n_s}E^n = 0$ for some $n_s$, it is called **bounded above** $F^{n_s}E_n = E^n$ for some $n^s$.
- The cohomology filtration is called **exhaustive** if $\cup F^iE^n = E^n$.
- The spectral sequence is called **regular** if $d_{pq}^r = 0$ for sufficiently large $r$.
- A spectral sequence is said to **weakly converges** to $E^\bullet$ if there is a filtration $$\ldots \subset F^dH^n \subset F^{d-1}H^n \subset \ldots \subset F^sH^n \subset \ldots \subset H^n$$ that $E^{pq}_\infty \cong F^pH^{p+q}/F^{p+1}H^{p+q}$.
- A spectral sequence **approaches** $E^\bullet$ if it weakly converges to $E^\bullet$.
- A spectral sequence **converges** to $E^\bullet$ if it approaches $E^\bullet$, it is regular, and $E^n = \lim(E^n/F^pE^n)$.
- If a first quadrant spectral sequence converges to $E^\bullet$, then the morphisms $E^{n,0}_0 \to E^{n,0}_\infty \subset E^n$ and $E^n \to E^{0,n}_\infty \to E^{0,n}_0$ are called the **edge morphisms**.

**Prop. (3.4.7.3)** [Notation for Filtrations on Homological Complexes]. Let $C_\bullet$ be a complex and $\ldots \subset F_{p-1}C \subset F_pC \subset \ldots \subset C$ be filtrations of complexes. Then it is called **exhaustive** if $C = \lim F_pC$. It is called **Hausdorff** if $\cap F_pC = 0$. It is called **complete** if $C = \lim C/F_pC$.

**Def. (3.4.7.4)** [Spectral Sequence of a Filtered Complex]. For a complex $K^\bullet$ and a filtration $F^pK^n$ on $K^n$, we have a natural spectral sequence $$E^{pq}_1 = H^{p+q}(F^pE^{p+q}/F^{p+1}E^{p+q}), \quad E^n = H^n(K^\bullet), \quad F^pE^n = H^n(F^pK^\bullet).$$

For a morphism of filtered complexes that are isomorphism for some $r$, induction on the exact sequence $0 \to F^pE^n \to F^{p+1}E^n \to E^{p,n-p}_\infty$ and use five-lemma shows it induces isomorphism on $H^SE$.

**Prop. (3.4.7.5)** [Comparison Theorem]. For a morphism $F$ between two convergent spectral sequences, if it is an isomorphism for some $r$, then it induce isomorphism on the infinite homologies.

**Proof:** Clearly $F$ induces isomorphisms on $E^{p,q}_\infty$. Because there are exact sequence $$0 \to F^{p+1}H^n \to F^pH^n \to E^{p,n-p}_\infty \to 0$$ we can use five lemma and induction to show that $F$ induces isomorphisms on $F^pH^n/F^sH^n$. Then because $H^n = \cup F^pH^n$, we can take colimit to show $F$ induces isomorphisms on $H^n/F^sH^n$, then take inverse limits, we are done.

**Prop. (3.4.7.6)** [Classical Convergence]. If the filtration on a complex $C_\bullet$ is bounded below and exhaustive for all $C_n$, then there is a spectral sequence that is also bounded below and converges to $H_\bullet(C_\bullet)$.

**Proof:** Cf[Gelfand P203] for cohomological case and [Weibel P135] for homological case.
Prop. (3.4.7.7) [Complete convergence]. If the filtration is complete, exhaustive and the spectral sequence is regular, then the spectral sequence weakly converges to $H_\bullet(C_\bullet)$. And if it is also bounded above, then it converges to $H_\bullet(C_\bullet)$.

Proof: Cf. [Weibel, P139].

There are two examples, the stupid filtration and the canonical filtration, the canonical filtration is natural and factors through $D(A)$.

Prop. (3.4.7.8) [Spectral Sequence of a Double Complex]. A double complex has two natural filtrations of the total complex, they define two spectral sequences, one has

$$E^{p,q}_{2,x} = H^p_x(H^q_y(L_\bullet))$$

and the other has

$$E^{p,q}_{2,y} = H^p_y(H^q_x(L_\bullet)).$$

Cf. [Gelfand P209]. In fact under reflection, there is only one spectral sequence. For the horizontal filtration, the differential goes vertical first, for the vertical filtration, the differential goes horizontal first. The differential goes one way, the convergence goes reversely.

If both the filtration is finite and bounded, in particular if $E$ is in the first quadrant, then they both converge to $H^n(E)$, this will generate important consequences.

Cor. (3.4.7.9). If a double complex in the first quadrant has its all column acyclic (3rd-quadrant pointing), then the total complex is acyclic. Thus a morphism of double complex inducing quasi-isomorphism on each column induces a quasi-isomorphism on the total complex.

If a double complex has $H_p(C_{\bullet,q}) = 0, \forall p > 0, q$, then

$$H_n(\text{Tot}C_{\bullet,*}) = H_n(\text{Coker}(C_{1,*} \to C_{0,*})$$

Prop. (3.4.7.10) [Horizontal Filtration]. For a second-quadrant-free homology double complex, the filtration is bounded below and exhaustive for $\text{Tot}^\oplus$, so the classical convergence (3.4.7.6) applies and there is a convergence

$$E^{p,q}_{2} = H^p_x(H^q_y(C)) \Rightarrow H_{p+q}(\text{Tot}^\oplus C).$$

For a fourth-quadrant free homology double complex, the filtration is complete and exhaustive for $\text{Tot}^\Pi$, so the complete convergence (3.4.7.7) applies and there is a weak convergence

$$E^{p,q}_{2} = H^p_x(H^q_y(C)) \Rightarrow H_{p+q}(\text{Tot}^\Pi C).$$

Cor. (3.4.7.11) [Grothendieck Spectral Sequence]. If $\mathcal{A}, \mathcal{B}, \mathcal{C}$ be Abelian categories, $\mathcal{B}$ have enough injectives and $F: K^+(\mathcal{A}) \to K^+(\mathcal{B}), G: K^+(\mathcal{B}) \to K^+(\mathcal{C})$ are exact functors between triangulated categories. If $R_\mathcal{A}$ is adapted to $F, G \circ F$, then for any $X^\bullet \in K^+(\mathcal{A})$, there is a spectral sequence convergence (to upper left)

$$E^{p,q}_{2} = R^pG(R^qF(X)) \Rightarrow E^n = R^n(G \circ F)(X).$$

And if $R_\mathcal{A} = I_\mathcal{A}$, this spectral sequence is functorial in $X^\bullet$.

In particular, this applies to the case that $F$ is right adjoint to an exact functor and both $\mathcal{A}, \mathcal{B}$ have enough injectives.
Proof: Choose a functorial injective resolution \( X \mapsto \mathcal{I}_X^\bullet(3.4.3.9) \), let \( K^\bullet = F(I_X^\bullet) = RF(X) \), and choose a functorial CE resolution of \( K^\bullet(3.3.5.9) \), because the resolutions for \( B^i \to Z^i \to H^i \) and \( Z^i \to K^i \to B^{i+1} \) split and \( G \) is additive, we have

\[
H^q_x(G(L^{**})) = G(H^q_x(L^{**})) = RG(H^q(K))
\]

So

\[
E^{p,q}_{2,y} = H^p_y(H^q_x(L^{**})) = R^pG(H^q(K)) = R^pG(R^qF(X))
\]

and

\[
E^\bullet = RG(Tot(L)) = G(Tot(L)) = RG(K) = RG \circ RF(X) \cong R(G \circ F)(X)(3.4.4.6).
\]

\( \square \)

**Cor. (3.4.7.12).** The low degree parts read:

\[
0 \to R^1G(F(A)) \to R^1(G \circ F)(A) \to G(R^1F(A)) \to R^2(G \circ F)(A).
\]

(Check definition). More generally, if \( R^pG(R^qF(A)) = 0, 0 < q < n \), then

\[
R^mG(F(A)) \cong R^m(G \circ F)(A) \quad m < n
\]

And

\[
0 \to R^nG(F(A)) \to R^n(G \circ F)(A) \to G(R^nF(A)) \to R^{n+1}(G \circ F)(A).
\]

**Remark (3.4.7.13).** The Grothendieck spectral sequence is tremendously important.

**Cor. (3.4.7.14) [Spectral Sequence for Hypercohomologies].** For chain complex \( K \) in \( K^+(A) \) and a left exact functor \( F \), the CE resolution will generate two spectral sequences by(3.4.7.10):

\[
E^{p,q}_{2,x} = H^p_x(R^qF(A)) \Rightarrow R^{p+q}(A), \text{when } A \text{ is bounded below}
\]

\[
E^{p,q}_{2,y} = (R^pF)(H^q(A)) \Rightarrow R^{p+q}(A) \text{, weakly convergent}
\]

where the RHS is the hypercohomologies(3.4.4.11).

8 T-Structures

**Examples**
3.5 Differential Graded Algebras

Main references are [Ker] and [Sta].

Def. (3.5.0.1) [Differential Graded Algebras]. A differential graded algebra or DGA is a chain complex $A^\bullet$ of $R$-modules with $R$-linear maps $A^m \times A^n \to A^{m+n}$ that

$$d(ab) = d(a)b + (-1)^n ad(b),$$

that makes $\oplus A^n$ into an associative and unital $R$-algebra.

Notice the first condition is equivalent to giving a map $\text{Tor}(A^\bullet \times_R A^\bullet) \to A$.

For a differential algebra $A^\bullet$, a right differential module is defined naturally. The tensor operation gives a closed symmetric monoidal structure $M_A$.

Notice a usual $R$-algebra $A$ can be seen as a differential graded algebra as $A^0 = A$ and $A^n = 0$ for $n > 0$.

And as in the case of chain complexes, the category of differential modules over $A$ can be given a derived category.

Def. (3.5.0.2). A differential graded algebra $A^\bullet$ is called commutative if $ab = (-1)^{\deg(a)\deg(b)}ba$. It is called strictly commutative if moreover $a^2 = 0$ for $\deg(a)$ odd.

Def. (3.5.0.3). For two differential graded algebras $A, B$, the tensor graded algebra $A^\bullet \otimes B^\bullet$ is given by the $\text{Tor}(A^\bullet \otimes_R B^\bullet)$.

1 dg-Categories

Def. (3.5.1.1) [dg-Categories]. Given a DGA $A$, a dg-category over $A$ is a category enriched over the monoidal category $M_A(3.5.0.1)$. Let $\text{dgCat}_A$ denote the category of small dg-categories over $A$ where morphisms are given by monoidal functors.

Def. (3.5.1.2) [Homotopy Categories]. Because $H^0$ and $Z^0$ are right-lax monoidal functors from $\text{Ch}(R)$ to $\text{Mod}(R)$, given a dg-category $C$, by transferring, we can get categories $H^0(C)$ and $Z^0(C)$ enriched over $\text{Mod}_{A^0}$.

Def. (3.5.1.3) [Equivalences]. A morphism between dg-categories are called an equivalence if induces quasi-isomorphisms on all hom-complexes.

Prop. (3.5.1.4) [Model Category of dg-Categories]. There is a cofibrantly generated model category on $\text{dgCat}_A$, where weak equivalences are quasi-equivalences and the fibrations are morphisms $F : A \to B$ that:

- induces component-wise surjections on hom-complexes.

- given an isomorphism $g : F(X) \to Y \in H^0(B)$, there is an isomorphism in $H^0(A)$ lifting $g$.

This monoidal structure is induced from that of the case $A = R$ and the right-lax monoidal functor $\text{Ch}(R) \to M(A)$ given by $M^\bullet \mapsto A \otimes M$.


2 Sheaves of DGAs
3.6 Topology I

Main references are [Mun00], [Mor19], [H-J99].

1 Basics

Def. (3.6.1.1) [Topologies].

Def. (3.6.1.2) [Continuous Functions].

Def. (3.6.1.3) [Semicontinuous Functions]. A function from $X \to [-\infty, \infty]$ is called upper semi-continuous iff $f^{-1}((-\infty, a))$ are all open. It is called lower semicontinuous iff $f^{-1}((a, \infty])$ are all open.

Def. (3.6.1.4). A topological space is called separable if it has a countable dense subset.

Def. (3.6.1.5) [Product Topology]. Arbitrary product exists in the category of topological spaces. It is constructed as follows: for a family of topology spaces $X_i$ indexed over an index set $I$, the product $\prod_I X_i$ is the set-theoretic product endowed with the topology generated by the basis $\pi_i^{-1}(U)$ for $U_i$ open in $X_i$.

Prop. (3.6.1.6) [Limits and Colimits]. Arbitrary limits and colimits exist in the category of topological spaces. The limits is given as a subspace of the product topology, and the colimits $X = \text{colim} X_i$ is given a topology that $U \subset X$ is open iff $U \cap X_i$ is open for each $i$.

Prop. (3.6.1.7) [Pullback Space]. Let $E \to X$ and $f : X' \to X$ be maps of spaces, then there is a pullback map $f^*E = E \times_X X' \to X'$, called the pullback space.

Def. (3.6.1.8) [Quotient Topology]. Let $f : X \to Y$ be a surjective map of spaces, and $X$ has a topology, then we can define a quotient topology on $Y$ that $U \subset Y$ is open iff $f^{-1}(U)$ is open in $X$. It has the universal property that any continuous map $X \to Z$ that factors through $f$ set-theoretically factors through $f$ as a continuous map.

Such a map is called a quotient map.

Prop. (3.6.1.9). A surjective open map $\pi$ is a quotient map.

Proof: It is clearly that a subset $U$ is open iff $\pi^{-1}(U)$ is open. \qed

Def. (3.6.1.10) [Glueing Space]. Let $A \subset X$ and $f : A \to Y$, then we have the glueing space $Y \coprod_f X$.

Def. (3.6.1.11) [Mapping Cylinder]. Let $f : X \to Y$ be a map, then we define the mapping cylinder $M(f) = Y \coprod_f X \times I$, where $X \times \{0\} \subset X \times I$ mapsto $Y$ by $f$.

Def. (3.6.1.12) [Cone]. For $X \in \text{Top}$, define the cone over $X$ to be the space $C(X) = (X \times \mathbb{I})/(X \times \{1\})$. Notice that $C(\emptyset) = \text{pt}$.

Def. (3.6.1.13) [Mapping Cone]. Let $f : X \to Y$ be a map, then we define the mapping cone $C(f) = M(f)/X \times \{1\}$.

Lemma (3.6.1.14). If $f : X \to Y$ is a surjective continuous map that $f(E) \neq Y$ for any proper closed subspace of $X$, then for any $U \subset X$ open, $f(U) \subset Y \setminus f(X \setminus U)$. 

3.6. TOPOLOGY I

Proof: Take $y \in f(U)$ and a nbhd $V$ of $y$ in $Y$, we show that $V$ intersect $Y \setminus f(X \setminus U)$: $W = U \cap f^{-1}(V)$ is nonempty, thus $f(X \setminus W) \neq Y$, take $y' \in Y \setminus f(X \setminus W)$, then it is clear $y' \in Y \setminus f(X \setminus U)$, and $y' \in V$. □

Def. (3.6.1.15) [Locally Closed Subset]. A subset $Z$ of $X$ is called locally closed if for any $z \in Z$, there is a nbhd $U$ of $z$ in $X$ that $U \cap Z$ is closed in $Z$. Equivalently, a locally closed subset is the intersection of an open subset with a closed subset.

Proof: An intersection of an open subset and a closed subset is clearly locally closed. Conversely, if $Z$ is locally closed, we choose for each $z \in Z$ a nbhd $U_z$ that $U_z \cap Z$ is closed in $U$, then we can show $Z = \overline{Z} \cap \bigcup_z U_z$. This is because if $x \in \overline{Z} \cap \bigcup_z U_z$, then $x \in U_z$ for some $z$, and also $x \in Z$, thus $x$ is in $Z$. □

Filter Langrange

Def. (3.6.1.16) [Convergence and Filter]. For a filter $F$ on a topological space, $F$ converges to a point $y$ iff any open set containing $y$ is in $F$.

If $X$ is a set and $Y$ is a topological space and $X \to Y$ is a function, then $y \in Y$ is a $F$-limit of $f$ if $f_* F$ converges to $y$.

Prop. (3.6.1.17) [Ultrafilter Convergence Theorem]. Let $X, Y$ be a topological space, then:

1. $Y$ is compact iff any ultrafilter on $Y$ has a limit point.

2. $Y$ is Hausdorff iff any ultrafilter on $Y$ has at most one limit point.

3. A function $f : X \to Y$ is continuous iff for any filter on $X$ converging to $x$, the filter $f_* F$ converges to $y$.

Proof:

1. If $Y$ is compact but every point is not a limit point, then for any $x$, there is an open set $U_x$ that $U_x \notin F$, but then $F$ of them covers $Y$, which is in $F$, so one of them must be in $F$ by (1.1.8.7), contradiction.

Conversely, if $\cup_i U_i = X$ but no finite union of them cover $X$, then $X - U_i$ satisfies the finite intersection property, so there is an ultrafilter containing $X - U_i$ by (1.1.8.4) and (1.1.8.5). Then clearly any point $x$ is not a limit point of $F$.

2. If $Y$ is Hausdorff and $x, y$ are both limit point of a filter $F$, then there are two non-intersecting nbhd of them in $F$, so its intersection $\emptyset \notin F$, contradiction.

Conversely, if $x, y$ are two point that their nbhds both intersect, then their nbhds together satisfies the finite intersection property, so there is an ultrafilter containing all of them, by (1.1.8.4) and (1.1.8.5), thus converging to both $x$ and $y$.

3. This is an easy consequence considering the filter of all the nbhd containing $x$. □

Connected Components

Def. (3.6.1.18) [Connectedness]. A space $X$ is called connected if it satisfies: for any open subset $U, V$ of $X$ that $U \cup V = X$ and $U \cap V = \emptyset$, either $U = \emptyset$ or $V = \emptyset$.

$X$ is called locally connected if there is a basis of $X$ consisting of connected open subsets of $X$.
Def. (3.6.1.19) [Path-Connectedness]. A space $X$ is called path-connected if any two points of $X$ can be connected by an arc.

$X$ is called locally path-connected if there is a basis of $X$ consisting of path-connected open subsets of $X$.

Prop. (3.6.1.20). If $X$ is an ordered set with the least upper bound property and satisfies: for any $x < y \in X$, there exists $z \in X$ s.t. $x < z < y$. Then $X$ is connected, so are intervals and rays in $X$.

Proof: Let $Y$ be an interval or ray in $X$. Suppose for contradiction $Y = A \mathbin{\cup} B$, where $A, B$ are open and non-empty in $Y$. Choose $a \in A, b \in B$, then $[a, b] \subseteq Y$. Let $A_0 = A \cap [a, b]$ and $B_0 = B \cap [a, b]$, and $c = \sup A_0 \in [a, b]$.

Then $c \notin B_0$: If $c \in B_0$, then $c \neq a$, and because $B_0$ is open, there exists some $a \leq d < c$ s.t. $(d, c] \subseteq B_0$. So $d$ is a smaller upper bound for $A_0$, contradiction.

And also $c \notin A_0$: If $c \in A_0$, then $c \neq b$, and because $A_0$ is open, there exists some $c < e \leq b$ s.t. $[c, e) \subseteq A_0$. Then by hypothesis, there exists $z \in (c, e) \subseteq A_0$, contradicting the fact $c$ is an upper bound for $A_0$.

Then we derived a contradiction that $c \notin Y$, which proves $Y$ is connected. \hfill \Box

Def. (3.6.1.21) [Connected Components]. In a topological space $X$, if $x \in X$, the connected component of $x$ is the maximal connected subspace of $X$ containing $x$. The path-connected component of $x$ is the maximal path-connected subspace of $X$ containing $x$.

Prop. (3.6.1.22).

- Any connected component of $X$ is closed.
- If $X$ is locally connected, then any connected component of $X$ is clopen.
- If $X$ is locally path-connected, then any path-connected component of $X$ is open, and any connected component is also open.

Prop. (3.6.1.23) [Clopen Subsets and Connected Components]. Let $X$ be a normal topological space and $x \in X$, then the connected component of $X$ containing $x$ is the intersection of clopen subsets containing $x$, denoted by $A$.

Proof: Assume $A$ splits into two components $B, D$. Since $A$ is closed, $B$ and $D$ are both closed, because $X$ is normal there are disjoint open neighborhoods $U$ and $V$ around $B$ and $D$, respectively. The open sets $U$ and $V$ cover the intersection of all clopen neighborhoods of $A$, so cause $X$ is compact, there must exist a finite number of clopen sets around $A$, say $A_1, \ldots, A_n$ such that $U \cup V$ covers $K = \bigcap_{i=1}^n A_i$.

Note that $K$ is clopen. We can assume that $x \in U$. It is not difficult to see that $K \cap U$ is clopen and does not contain all of $A$, contradicting the definition of $A$. \hfill \Box

Cor. (3.6.1.24). For a compact Hausdorff topological space $X$ and a point $x \in X$, the connected component of $X$ containing $x$ is the intersection of all compact open neighborhoods of $x$, because $X$ is normal (3.6.7.6).

Def. (3.6.1.25) [Totally Disconnected Space]. A space is called totally disconnected iff any connected subset of $X$ contains only one point.

Prop. (3.6.1.26). A subspace of a totally disconnected space is totally disconnected, because totally disconnected is equivalent to the only connected subsets are pt sets.
Extremally Disconnected Space

**Def. (3.6.1.27) [Extremally Disconnected Space].** A topological space $S$ is called **extremally disconnected** if the closure of any open subset of $X$ is open.

**Prop. (3.6.1.28).** Let $X$ be an extremally disconnected space, if $U, V$ are disjoint open subsets of $X$, then $U, V$

*Proof:* Because $V \cap U = \emptyset$, thus similarly $V \cap U = \emptyset$. □

**Lemma (3.6.1.29).** Let $f : X \to Y$ be a continuous surjective map of compact Hausdorff spaces that $Y$ is extremally disconnected and $f(Z) \neq Y$ for any proper closed subspace of $X$, then $f$ is a homeomorphism.

*Proof:* By (3.6.2.11) it suffices to show that $f$ is injective. Suppose $f(x) = f(x') = y$, then choose disjoint nbhd $U, U'$ of $x, x'$, and $T = f(X \setminus U), T' = f(X \setminus U')$ closed in $Y$, then $Y = T \cup T'$ and $y$ is contained in the closure of $Y \setminus T$ and $Y \setminus T'$ by (3.6.1.14), but this contradicts (3.6.1.28). □

**Prop. (3.6.1.30) [Projective Spaces].** Compact Hausdorff extremally disconnected spaces are exactly the projective objects in the category of compact Hausdorff spaces.

*Proof:* Assume $X$ is projective, let $U \subseteq X$ be open, and the complement by $Z$, then consider the surjection $U \coprod Z \to X$, and let $\sigma$ be the projection, then $\sigma(U) \subseteq \mathcal{U}$, thus $\sigma^{-1}(U) = \mathcal{U}$, and it is open.

Conversely, if $X$ is extremally disconnected, then by (3.6.2.13), there is a compact subset $E \subseteq Y$ that $f(E) = X$ and $f(E') \neq X$ for all closed subspace $E' \subseteq E$. Then (3.6.1.29) says $f|_E$ is a homeomorphism, and the inverse of it gives a desired section. □

**Prop. (3.6.1.31) [Gleason].** In an extremally disconnected space $X$, a convergent sequence is eventually constant. In particular, $\mathbb{Z}_p$ is a profinite group that is not extremally disconnected.

*Proof:* Cf.[Projective Topological Spaces] □

## 2 Compactness

**Def. (3.6.2.1) [Quasi-Compact Space].** A topological space is called **compact** or **quasi-compact** iff any open covering of it has a finite sub-covering. A subspace of a topological space is called **precompact** if its closure is compact.

**Def. (3.6.2.2) [Quasi-Compact Morphism].** A map of topological spaces is called a **quasi-compact morphism** if the inverse image of any quasi-compact open subset is quasi-compact open.

**Prop. (3.6.2.3) [Alexander Subbase Theorem].** A topological space is compact iff the closed subsets has the finite intersection property(1.1.8.3). In fact, it suffices to show that the family of complements of a subbasis of open sets has the finite intersection property.

*Proof:* Cf.[Sta]08ZP. □

**Prop. (3.6.2.4).** Let $X$ be a totally ordered set with the least upper bound property, then each closed interval of $X$ is compact in the order topology. In particular, this applies to a complete totally ordered set $X(1.1.3.19)$. 
Proof: Let \( a < b \) and \( \mathcal{U} \) a covering of \([a, b]\). We first show that for any \( x \in [a, b] \), there exists some \( x < y \leq b \) that \([x, y]\) can be covered by at most two elements of \( \mathcal{U} \): If \( x \) has an immediate successor, then take \( y \) to be it. If \( x \) has no immediate successor, choose an element \( U \) of \( \mathcal{U} \) containing \( x \), then \( U \) contains some \([x, c]\). Choose \( y \in [x, c] \), then \([x, y]\) is covered by a single element of \( \mathcal{U} \).

Now let \( C \) be the set of points \( y \in [a, b] \) that \([a, y]\) can be covered by f.m. elements of \( \mathcal{U} \). We showed before this set is non-empty. Let \( c \) be the least upper bound of \( C \), then \( a < c \leq b \).

Next, we show \( c \in C \): take an element \( U \) of \( \mathcal{U} \) containing \( c \), then \( U \) contains some \((d, c]\). There must be some element of \( C \) lying in the interval \((d, c]\), otherwise \( d \) is an upper bound of \( C \). Then \([a, y]\) is covered by f.m. elements of \( \mathcal{U} \), so \( c \in C \).

Finally, we show \( c = b \), but this is because otherwise we can find \( c < y \leq b \) that \([c, y]\) is covered by 2 elements, thus \( y \in C \), so \( y \leq c \), contradiction. \( \square \)

Prop. (3.6.2.5) [Tychonoff]. An arbitrary direct product of compact topological groups is compact.

Proof: We prove the finite intersection property. If \( A \) is a family of subsets that any finite intersection of closure of them is nonempty, then consider a maximal family \( \mathcal{D} \) of subsets containing \( A \) that any finite intersection of closures of them is nonempty, it exists by Zorn’s lemma. Consider the projection of \( \mathcal{D} \) onto a coordinate, then by Hypothesis, it has an intersection \( x_\alpha \). Now we want to show \( x = (x_\alpha) \) belongs to each \( D \in \mathcal{D} \).

If \( U_\beta \) is any subbasis element containing \( x \), then \( U_\beta \) intersect each \( \mathcal{D} \) because \( x_\beta \in \pi_\beta(D) \), so it is in \( \mathcal{D} \), by maximality of \( \mathcal{D} \). So the finite intersections are also in \( \mathcal{D} \), so all local basis of \( x \) are in \( \mathcal{D} \). This means that local basis intersect each element of \( \mathcal{D} \), that is, all closure of elements in \( \mathcal{D} \) contains \( x \).

Def. (3.6.2.6) [Sequentially Compact]. A subset \( A \) in a space \( X \) is called sequentially compact iff any sequence of points in \( A \) has a convergent subsequence in \( X \). It is called self sequentially compact if it is sequentially compact in itself.

Prop. (3.6.2.7). \( f : X \to Y \), \( X \) is compact and \( Y \) is Hausdorff, then for a descending chain \( Y_i \) of closed subsets of \( X \),

\[ f(\bigcap_n Y_n) = \bigcap_n f(Y_n). \]

Proof: The left side is compact, so if \( x \notin f(\bigcap_n Y_n) \), there is a closed subsets \( x \in T \) that \( T \cap f(\bigcap_n Y_n) = 0 \), so \( f^{-1}(T) \bigcap_n Y_n = 0 \), so \( f^{-1}(T) \bigcap_n Y_n = 0 \) for some \( n \), hence \( x \notin f(Y_n) \). \( \square \)

Prop. (3.6.2.8) [Fixed Point Theorem]. If \( X \) is a compact metric space \( M \), \( T \) is a continuous map \( X \to X \) that \( d(x, y) < d(Tx, Ty) \), then \( T \) has a unique fixed point in \( X \).

Proof: The uniqueness is obvious, for the existence, first notice \( T \) is obviously continuous, so consider \( d(x, Tx) \), this is a continuous function on \( M \), so it contains a minimum value, if it not 0, then \( d(Tx, Tx^2) < d(x, Tx) \), which is a contradiction. \( \square \)

Def. (3.6.2.9) [Proper Map]. A proper map is a continuous map s.t. the inverse image of compact subsets are compact.

Prop. (3.6.2.10). If \( X \) is compact and \( Y \) is Hausdorff, then a continuous map \( f : X \to Y \) is proper.

Cor. (3.6.2.11). A continuous bijective map from a compact space to a Hausdorff space is a homeomorphism.
Prop. (3.6.2.12) [Proper Continuous Maps Closed]. Let $f : X \to Y$ be a proper continuous map with $Y$ locally compact Hausdorff, then $f$ is a closed map.

Proof: Let $K \subset X$ closed, and $y \in \overline{f(K)}$. Choose precompact open nbhd $U$ of $y$, then $f^{-1}(U)$ is compact in $X$, so $f(K \cap f^{-1}(U)) = f(K) \cap U$ is compact and thus closed in $Y$. Then $y \in f(K)$, and $f(K)$ is closed.

Lemma (3.6.2.13). Let $f : X \to Y$ be a continuous map of compact Hausdorff spaces, then there exists a smallest closed subset $E$ of $X$ that $f(E) = Y$.

Proof: Use Zorn’s lemma, noticing that the intersection of a chain of possible $E_i$s also maps to $Y$, by the intersection property (3.6.2.3).

Stone-Čech Compactification

Def. (3.6.2.14) [Stone-Čech Compactification]. The Stone-Čech Compactification $\beta$ is defined to be a functor from the category of sets to the category of compact Hausdorff space that is left adjoint to the forgetful functor.

The construction of $\beta(X)$ is as follows: $\beta X =$the set of all ultrafilters on $X$, and the topology is generate by $U_A = \{ F | A \in F \}$ as a basis of clopen subsets. For a map $f : X \to Y$, the map $\beta X \to \beta Y$ is given by $f_*$.

Proof: First $\beta X$ is a compact Hausdorff space: it is compact because if there are sets $A_i$ that any ultrafilter contains at least one of them, then f.m. of them must cover $X$, otherwise $X - A_i$ satisfies the finite intersection property thus is contained in some ultrafilter, by (1.1.8.4) and (1.1.8.5), contradiction. Then by (1.1.8.7) shows that any ultrafilter contains one of them. It is Hausdorff because for any two different ultrafilter, there must be an $A$ that $A \in F_1$ and $X - A \in F_2$. $f_*$ is continuous because $f^{-1}(U_A) = U_{f^{-1}(A)}$.

Now for any map $f : X \to Y$ where $Y$ is a topological space, map an ultrafilter $F$ to the unique limit point of $f_*F$ in $Y$ (existence and uniqueness by (3.6.1.17)). This map is continuous from $\beta X$ to $Y$ because for any open set $V \subset Y$, $U_{f^{-1}(V)}$ is mapped into $V$. And for any $\beta X \to Y$ continuous, consider $X \to Y$ which maps $x$ to the image of the principle ultrafilter $F_x$ in $Y$.

This two map are mutually converses to each other, first for a $f : X \to Y$, $X \to \beta X \to Y$ is $f$ itself, because the pushout of the principle ultrafilter clearly converges to $f(x)$. And for a $\beta X \to Y$, if $F$ doesn’t map to $\lim f_*F$ but mapped to some $t$, then by definition, there is a nbhd $U$ of $t$ that $f^{-1}(U) \not\in F$, but by continuity, there is a $F \in U_B$ mapped into $U$. But then $B \in f^{-1}(U)$, otherwise if $x \in B - f^{-1}(U)$, then $F_x$ is mapped to $U$, contradiction, so $f^{-1}(U)$ containing $B$ is also in $F$, contradiction.

Lemma (3.6.2.15). In fact, the spaces in the image of the Stone-Čech compactification are all profinite spaces.

Proof: As shown before, for any two different ultrafilter, there must be an $A$ that $A \in F_1$ and $X - A \in F_2$, $U_A$ is open and closed.

Prop. (3.6.2.16) [Stone Representation Theorem]. The Stone-Čech compactification $\beta$ gives an equivalent of categories from the category of Boolean algebras to the category of profinite spaces.

Proof: $\beta B$ is a profinite space by lemma (3.6.2.15), and $B$ can be recovered from $\beta B$ as the Boolean algebra of all clopen subsets of $\beta B$, because $\beta B$ is compact. This is an inverse isomorphism because ?.
Prop. (3.6.2.17). The Stone-Čech compactification of a set \( \beta S_0 \) is extremally disconnected.

Proof: We check condition (3.6.1.30): For any surjection \( S' \to \beta S_0 \), we may take a lift \( S_0 \to S \) arbitrarily, then by definition there is a morphism \( \beta S_0 \to S' \) extending this morphism. It is a section by the universal property. \( \square \)

Locally Compact Space

Def. (3.6.2.18) [Locally Compact Space]. A Hausdorff space is called **locally compact** if for any point \( x \), there is a compact subset containing a nbhd of \( x \).

Prop. (3.6.2.19). If \( X \) is Hausdorff, then \( X \) is locally compact iff for any \( x \in X \) and \( x \in U \) open, there exists a precompact nbhd \( V \) that \( x \in V \subset \overline{V} \subset U \).

Proof: One direction is trivial. For the other, for any \( x \in X \) and a nbhd \( U \) of \( x \), let \( U_0 \) be a precompact nbhd of \( x \), then \( U_0 \setminus U \) is closed thus compact and disjoint from \( x \). Because \( X \) is Hausdorff, we can find a nbhd \( V' \) of \( x \) that \( \overline{V'} \) is disjoint from \( U_0 \setminus U \). Now let \( V = V' \cap U_0 \), then \( \overline{V} \subset U_0 \) is closed thus compact, and \( \overline{V} \subset \overline{V'} \cap U_0 \subset U \). \( \square \)

Cor. (3.6.2.20). Open subsets and closed subsets of a locally compact Hausdorff space \( X \) is locally compact Hausdorff.

Proof: If \( A \subset X \) is closed and \( x \in A \), then there exists a precompact nbhd \( U \) of \( x \), then \( A \cap \overline{U} \) is closed in \( U \) thus compact, and contains the nbhd \( U \cap A \) of \( x \), so \( A \) is locally compact.

If \( A \subset X \) is open, \( x \in A \), let \( x \in U \subset A \), and \( U \) open in \( X \), then we can apply (3.6.2.19) to find a precompact nbhd \( V \) that \( x \in V \subset \overline{V} \subset U \), so \( A \) is locally compact. \( \square \)

Prop. (3.6.2.21) [One-Point Compactification]. Let \( X \) be a space, then \( X \) is locally compact Hausdorff iff there exists a compact Hausdorff space \( Y \) containing \( X \) s.t. \( Y \setminus X \) is a single point. Moreover, in this case, \( Y \) is unique up to homeomorphisms, called the **one-point compactification** of \( X \).

Proof: Cf. [Mun00]P183. \( \square \)

Cor. (3.6.2.22). A space \( X \) is homeomorphic to an open subset of a compact open subspace iff it is locally compact Hausdorff, by (3.6.2.21) and (3.6.2.20).

Prop. (3.6.2.23). A locally compact second countable Hausdorff space \( X \) has a countable basis consisting of precompact open subsets. In particular, \( X \) is \( \sigma \)-compact.

Proof: Choose a countable basis \( \{ U_n \} \) of \( X \). For any \( x \in X \) and any nbhd \( U \) of \( x \), there exists a precompact \( U_x \subset U \) containing \( x \) by (3.6.2.19). Then for some \( n(x) \), \( U_{n(x)} \subset U_x \) containing \( x \), so \( U_{n(x)} \) is precompact. Thus the set of \( U_n \) that is precompact forms a countable basis of \( X \). \( \square \)

Prop. (3.6.2.24). If \( f : X \to Y \) is a quotient map and \( Z \) is locally compact, then \( X \times Z \to Y \times Z \) is also a quotient map.

Proof: Consider \( W \) as \( Y \times Z \) in the quotient map topology, then \( X \times Z \to W \) is continuous, which means \( X \to \text{Map}(Z,W) \) is continuous. But then \( Y \to \text{Map}(Z,W) \) is continuous because \( Y \) is a quotient map. Applying (3.6.3.7), we see \( Y \times Z \to W \) is continuous. \( W \to Y \times Z \) is continuous by quotient map hypothesis, so \( Y \times Z \cong W \). \( \square \)
Compactly Generated Spaces

**Def. (3.6.2.25)** [Compactly Generated Spaces]. A **compactly generated space** is a space that is the colimit of its compact Hausdorff subspaces. The category of compactly generated spaces is denoted by \( \mathcal{CG} \).

**Prop. (3.6.2.26).** For \( X \in \mathcal{CG} \) and \( Y \in \text{Top} \), a set-theoretical map \( f : X \to Y \) is continuous iff for any \( K \in \text{Top} \) compact Hausdorff and a map \( i : K \to X \), the composite map \( K \to Y \) is continuous.

**Prop. (3.6.2.27)** [Compact Generating Functor]. There is a compact generating functor \( (-)_c : \text{Top} \to \mathcal{CG} \) right adjoint to the inclusion functor.

**Proof:** \( k \) is constructed by \( X \mapsto \lim_{\longrightarrow K \subset X, K \text{ compact}} K \). Notice \( X_c = X \) set-theoretically. It is easy to verify that if \( Y \in \mathcal{CG} \) and \( Y \to X \) is continuous, then the set-theoretical map \( Y \to X_c \) is also continuous. So \( (-)_c \) is right adjoint to the inclusion functor. \( \square \)

**Cor. (3.6.2.28).** \( \mathcal{CG} \) is both complete and cocomplete, and the colimits coincide with colimits in \( \text{Top} \).

**Cor. (3.6.2.29).** \( \mathcal{CG} \) is Cartesian closed (3.1.4.7).

**Cor. (3.6.2.30).** The right adjoint to the Cartesian product is the compactification of the mapping space functor (3.6.3.1), by (3.6.3.6) and (3.6.2.27).

**Prop. (3.6.2.31).** Locally compact Hausdorff topological spaces are compactly generated.

**Proof:** For \( X \in \text{Top} \), if \( Z \subset X \) satisfies \( Z \cap K \) is closed for any compact Hausdorff subset \( K \subset X \), for any \( x \in X \), there exists a precompact nbhd \( U \) of \( x \) in \( X \), so \( Z \cap U \) is closed, and \( Z \cap U \) is closed in \( U \). Thus \( Z \) is closed in \( X \). \( \square \)

**Prop. (3.6.2.32).** Quotients and closed subspaces of a compactly generated space are compactly generated. Colimits of compactly generated spaces are compactly generated.

**Proof:** These follow from (3.6.2.25). \( \square \)

**Prop. (3.6.2.33).** If \( X \in \mathcal{CG} \) and \( Y \) is locally compact Hausdorff, then \( X \times Y \in \mathcal{CG} \).

**Proof:** Notice by (3.6.3.7), a map \( X \times Y \to Z \) is continuous iff \( C \times Y \to Z \) is continuous for any compact Hausdorff subset \( C \subset X \). The assertion is equivalent to \( X \times Y \to (X \times Y)_c \) is continuous, which is then equivalent to \( C \times Y \to (X \times Y)_c \) continuous for any compact subset \( C \subset X \). But \( Y \) is compactly generated, and \( C \) is locally compact, thus it suffices to show \( C \times C' \to (X \times Y)_c \) is continuous for any compact subset \( C' \subset Y \). Then this is true because \( C \times C' \) is compact. \( \square \)

### 3 Mapping Spaces

**Compact-Open Topology on Mapping Spaces**

**Def. (3.6.3.1)** [Compact-Open Topology]. The **compact-open topology** on a function space \( \text{Map}(X,Y) \) is a topology generated by the sets \( (K,U) = \{ f : f(K) \subset U \} \), where \( K \) is compact in \( X \) and \( U \) is open in \( Y \).

**Prop. (3.6.3.2).** For \( X' \to X, Y \to Y' \in \text{Top} \), the induced map \( \text{Map}(X,Y) \to \text{Map}(X',Y') \) is continuous. In particular, if \( X \cong X' \) and \( Y \cong Y' \), then \( \text{Map}(X,Y) \cong \text{Map}(X',Y') \).
Prop. (3.6.3.3). If \( Y \) is compact and \( X \) a metric space, this the compact open topology on \( \text{Map}(Y, X) \) coincides with the uniform topology on functions.

Proof: If \( f \in (K, U) \), then \( f(K) \subset U \), then there is a \( \varepsilon > 0 \) that \( B(K, \varepsilon) \subset U \), thus \( B(f, \varepsilon) \subset (K, U) \).

For any \( f \in \text{Map}(Y, X) \), \( f(Y) \) is compact thus there are f.m. open balls \( B(f(y_i), \frac{\varepsilon}{2}) \) that covers \( f(Y) \). Now if \( K_i = f^{-1}(B(f(y_i), \frac{\varepsilon}{2})) \), then \( \bigcup K_i = Y \), and \( f \in \cap_i(K_i, B(f(y_i), \frac{\varepsilon}{2})) \). Also \( \cap_i(K_i, B(f(y_i), \frac{\varepsilon}{2})) \subset B(f, \varepsilon) \), because for any \( g \in \cap_i(K_i, B(f(y_i), \frac{\varepsilon}{2})) \) and \( y \in K_i \), \( |f(y) - g(y)| \leq |f(y) - f(y_i)| + |f(y_i) - g(y_i)| < \frac{\varepsilon}{2} + \frac{\varepsilon}{2} = \varepsilon \). \( \square \)

Def. (3.6.3.4) [Relative Maps]. Let \( A \subset X \) and \( B \subset Y \), we denote by \( \text{Map}((X, A), (Y, B)) \) the subspace of \( \text{Map}(X, Y) \) consisting of continuous functions \( f : X \to Y \) that map \( A \) into \( B \).

Prop. (3.6.3.5) [Composition is Continuous]. If \( Y \) is locally compact Hausdorff, then the composition map

\[
\text{Map}(Y, Z) \times \text{Map}(X, Y) \to \text{Map}(X, Z)
\]

is continuous.

Proof: For any compact \( K \subset X \), open \( U \subset Y \) and \( g \circ f \in (K, U) \), \( f(K) \subset g^{-1}(U) \subset Y \). Because \( Y \) is locally compact, there is an precompact open subset \( V \) that \( f(K) \subset V \subset \overline{V} \subset g^{-1}(U) \), then \( (\overline{V}, U) \times (K, V) \) maps into \( (K, U) \). \( \square \)

Lemma (3.6.3.6) [Subbasis]. Let \( X \) be Hausdorff, \( W_\alpha \) be a subbasis of \( Y \), then \( (K, W_\alpha) \) where \( K \subset X \) compact is a subbasis of \( \text{Map}(X, Y) \).

Proof: If \( f \in (K, U) \subset \text{Map}(X, Y) \), let \( U = \bigcup_\beta U_\beta \), where \( U_\beta = \bigcap_{j=1}^{k(\beta)} W_{\beta,j} \). Now \( K \subset \bigcup_\beta f^{-1}(U_\beta) \), because \( K \) is compact Hausdorff thus the partition of unity(3.6.7.9) gives us f.m. compact subsets \( K_1, \ldots, K_n \) of \( K \) that \( K_i \subset f^{-1}(\overline{U_\beta}) \) for some \( \beta \). Then

\[
f \in \bigcap_{i=1}^n \bigcap_{j=1}^{k(\beta)} (K_i, W_{\beta,i,j}) = \bigcap_{i=1}^n (K_i, U_{\beta,i}) \subset (K, \bigcup_{i=1}^n U_{\beta,i}) \subset (K, U).
\]

\( \square \)

Prop. (3.6.3.7) [Adjoints of Mapping Space]. Let \( Y \) be a locally compact Hausdorff space, then

\[
\text{Map}(X \times Y, Z) \cong \text{Map}(X, \text{Map}(Y, Z))
\]

as sets. And if moreover \( X \) is Hausdorff, then it is a homeomorphism.

Proof: Let \( \varphi \in \text{Map}(X \times Y, Z) \), for any \( x \in X \), take \( \varphi(x) : Y \to Z : \varphi(x)(y) = \varphi(x, y) \), then \( \varphi(x) \) is continuous, and \( \varphi : X \mapsto \text{Map}(Y, Z) : x \mapsto \varphi(x) \) is continuous: for any compact \( K \subset Y \) and open \( U \subset Z \), \( \varphi^{-1}(K, U) = \{ x \in X | \varphi(x, K) \subset U \} \), which is open.

Conversely, for any \( \psi : X \to \text{Map}(Y, Z) \), let \( \tilde{\psi} : X \times Y \to Z \) be given by \( \tilde{\psi}(x, y) = \psi(x)(y) \). Then \( \tilde{\psi} \) is continuous: For any open \( U \subset Z \), if \( (x, y) \in \tilde{\psi}^{-1}(U) \), then \( \psi(x)y \subset U \). Because \( \psi(x) \) is continuous, there is a nbhd \( W \) of \( y \in Y \) that \( \varphi(x)(W) \subset U \). Then because \( Y \) is locally compact Hausdorff, there is a precompact nbhd \( V \) of \( y \in Y \) that \( y \in V \subset \overline{V} \subset W \). Then \( \psi^{-1}((\overline{V}, U)) \) is a nbhd of \( x \in X \), and \( (x, y) \in (\psi^{-1}((\overline{V}, U)), V) \subset \tilde{\psi}^{-1}(U) \), thus \( \tilde{\psi}^{-1}(U) \) is open, and \( \tilde{\psi} \) is continuous.
Now let $F : \varphi \mapsto \bar{\varphi}$ and $G : \psi \mapsto \bar{\psi}$, then we show $F,G$ are both continuous: By (3.6.3.6), $(K,(L,U))$ is a subbasis of $\text{Map}(X,\text{Map}(Y,Z))$. $F$ is continuous because $F((K \times L,U)) = (K,(L,U))$. $G$ is continuous because $X \times Y$ is Hausdorff and for any $J$ compact in $X \times Y$, $J \times J \xrightarrow{(pr_1,pr_2)} X \times Y$ is continuous, so for any $U \subset Z$ open, there exists $J_1 \subset X, J_2 \subset Y$ compact s.t. $G((J_1,(J_2,U))) \subset (J,U)$. \hfill $\square$

**Cor. (3.6.3.8).** If $Y$ is locally compact and Hausdorff, $A \subset X, B \subset Y, C \subset Z$, then

$$\text{Map}((X \times Y, X \times B \cup A \times Y),(Z,C)) \equiv \text{Map}((X,A),\text{Map}((Y,B),(Z,C)))$$

as sets, and if moreover $X$ is Hausdorff, then it is a homeomorphism.

**Def. (3.6.3.9)[Admissible Topology].** For $X,Y \in \text{Top}$, an admissible topology on $\text{Map}(X,Y)$ is a topology that makes the evaluation map $e : \text{Map}(X,Y) \times X \to Y$ continuous.

**Prop. (3.6.3.10).** The compact-open topology on $\text{Map}(X,Y)$ is coarser than admissible topology on it (3.6.3.9). And if $X$ is locally compact Hausdorff, then it is admissible.

**Proof:** It suffices to show any $(K,U)$ is open in $\text{Map}(X,Y)$. Let $f \in (K,U)$, then for any $x \in K$, $e(f,x) \in U$, thus there is a nbhd $U_x$ of $f$ and a nbhd $W_x$ of $x$ that $e(U_x \times W_x) \subset U$. Now because $K$ is compact, we can choose a nbhd $V$ of $f$ that $e(V \times K) \subset U$. Thus $f \in V \subset (K,U)$, and $(K,U)$ is open in $\text{Map}(X,Y)$. If $Y$ is locally compact Hausdorff, then $\text{Map}(Y,Z) \times X \to Z$ continuous by applying (3.6.3.5) with $X = \text{pt}$. \hfill $\square$

**Mapping Spaces in $\mathcal{C}^G$**

**Def. (3.6.3.11)[Mapping Spaces].** For $X,Y \in \mathcal{C}^G$, the mapping space $\text{Map}_c(X,Y)$ is the compact generation (3.6.2.27) of the space of continuous functions from $X$ to $Y$ with the topology generated by the sets $(K,U) = \{ f : f(i(K)) \subset U \}$, where $K$ is a compact Hausdorff space, $i : K \to X$ and $U$ is open in $Y$.

**Prop. (3.6.3.12).** For $X' \to X, Y \to Y' \in \mathcal{C}^G$, the induced map $\text{Map}_c(X,Y) \to \text{Map}_c(X',Y')$ is continuous. In particular, if $X \cong X'$ and $Y \cong Y'$, then $\text{Map}_c(X,Y) \cong \text{Map}_c(X',Y')$.

**Lemma (3.6.3.13)[Evaluations are Continuous].** For $X,Y \in \mathcal{C}^G$, the composition map

$$\text{Map}_c(Y,X) \times_c Y \to X$$

is continuous.

**Proof:** It suffices to prove that for any compact Hausdorff space $K, F$ mapping into $\text{Map}(Y,X), Y, K \times F \to X$ is continuous: For $(f_0,y) \in \text{Map}_c(Y,X) \times_c Y$ and $f_0(y) \in U$, as $f_0$ is continuous, there exists a nbhd $N$ of $y \in Y$ s.t. $f_0(N \cap F) \subset U$, and then $(f_0,y) \in (K \cap (N \cap F), N \cap F)$ is mapped into $U$. \hfill $\square$

**Prop. (3.6.3.14)[Adjointness of Mapping Space].** For $X,Y,Z \in \mathcal{C}^G$, there is a natural homeomorphism

$$\text{Map}_c(X \times_c Y,Z) \cong \text{Map}_c(X,\text{Map}_c(Y,Z))$$
Proof: Let \( \varphi \in \text{Map}_c(X \times_c Y, Z) \), for any \( x \in X \), take \( \varphi(x) : Y \to Z : \varphi(x)(y) = \varphi(x, y) \), then \( \varphi(x) \) is continuous, and \( \tilde{\varphi} : X \to \text{Map}(Y, Z) : x \mapsto \varphi(x) \) is continuous: if \( \varphi(x) \in (K, U) \), \( \tilde{\varphi}^{-1}(K, U) = \{ x \in X | \varphi(x \times i(K)) \subset U \} \), which is open.

To prove this construction is continuous, notice we have already seen that if \( f : X \times_c Y \to Z \) is continuous then \( f : Y \to \text{Map}_c(Y, Z) \) is continuous. Apply this to

\[
\text{Map}_c(Y \times_c X, Z) \times_c Y \times_c X \to Z
\]

we see that

\[
X \times_c \text{Map}_c(Y \times_c X, Z) \to \text{Map}_c(Y, Z)
\]

is continuous, and

\[
\text{Map}_c(Y \times_c X, Z) \to \text{Map}_c(X, \text{Map}_c(Y, Z))
\]

is continuous. Similarly, as

\[
\text{Map}_c(X, \text{Map}_c(X, Z)) \times_c Y \times_c X \to Z
\]

is continuous, we get

\[
\text{Map}_c(X, \text{Map}_c(Y, Z)) \to \text{Map}_c(X \times_c Y, Z)
\]

is continuous, and it is clearly the inverse to the construction above. \( \square \)

Cor. (3.6.3.15). For \( X, Y, Z \in \mathcal{C} \), \( A \subset X, B \subset Y, C \subset Z \), then there is a natural homeomorphism

\[
\text{Map}((X \times Y, X \times B \cup A \times Y), (Z, C)) \cong \text{Map}((X, A), \text{Map}((Y, B), (Z, C)))
\]

Cor. (3.6.3.16). Products in \( \mathcal{C} \) commute with colimits.

Cor. (3.6.3.17)[Compositions are Continuous]. For \( X, Y, Z \in \mathcal{C} \), the composition map

\[
\text{Map}_c(Y, Z) \times_c \text{Map}_c(X, Y) \to \text{Map}_c(X, Z)
\]

is continuous.

Proof: It suffices to show that

\[
\text{Map}_c(Y, Z) \times_c \text{Map}_c(X, Y) \times_c X \to Z
\]

is continuous, and this follows from (3.6.3.13). \( \square \)

Construction of Spaces

Def. (3.6.3.18)[Path Spaces]. For \( f : A \to B \in \text{Top} \), let \( E_f \) be the subspace of \( A \times \text{Map}(I, B) \) consisting of pairs \( (a, \gamma) \) that \( \gamma(0) = a \).

The fibers of \( E_f \to B \) are called homotopy fibers of \( f \).

Def. (3.6.3.19)[n-Loop Space]. The \( n \)-loop space of \( X \) is defined to be \( \Omega^n(X, x_0) = M(I^n, \partial I^n; X, x_0) \). Then by (3.6.3.8) we have

\[
\Omega(\Omega^n(X, x_0), \bar{x}_0) \cong \Omega^{n+1}(X, x_0).
\]

Prop. (3.6.3.20)[Loop spaces are Homotopy Fibers]. Let \( f : x_0 \to B \) be a point, then \( E_f \) is the path space \( PB \) of all paths starting from \( x_0 \), and the homotopy fiber over \( x_0 \) is just the loop space \( \Omega(X, x_0) \). \( PB \) is contractible, with the contraction given by \( H : PB \times I \to PB : \gamma_t(x) = \gamma(tx) \).
4 Profinite Space

Def. (3.6.4.1) [Profinite Space]. A space is called a **profinite space** if it is a cofiltered limit of discrete topological spaces. The category of profinite spaces is denoted by $\mathcal{P}rof$.

A profinite space is the same thing as a totally disconnected, compact Hausdorff topological space. Thus a closed subspace of a profinite space is profinite.

Proof: The profinite spaces are clearly totally disconnected, compact Hausdorff (by Tychonoff).

Conversely, if it is totally disconnected and compact Hausdorff, let $I$ be the set of clopen decompositions $X = \bigsqcup_i U_i$ of $X$, then for each $I \subset I$, there is a map $X \to I$, and there is a partial order on the decompositions of $X$. We show that the map $X \to \varinjlim_{I \subset I} I$ is a homeomorphism. It is injective by (3.6.1.25)(3.6.1.23)(3.6.7.6). It is surjective by compactness of $X$, and it is clearly open, thus homeomorphism by (3.6.2.11).

Cor. (3.6.4.2). A cofiltered limit of profinite spaces is profinite.

Prop. (3.6.4.3). Any open covering of a profinite space has a clopen disjoint subcover.

Proof: By (3.6.4.1), we may assume that $X = \varinjlim_{i \in I} X_i$, where $X_i$ is finite. Let $f_i$ be the projection, as the limit is filtered, a fundamental family of nbhds of a point $(x_i) f_i^{-1}(x_i)$, Then for each covering, we may assume it is finite $X = \bigcup_i f_i^{-1}(x_i)$, choose a $j > i$ for each $i$, as $I$ is cofiltered, then $X = \bigsqcup_{x \in X_j} f_j^{-1}(x)$ satisfies the desired property.

Prop. (3.6.4.4). If $X$ is quasi-compact and any connected component of $X$ is the intersection of clopen sets containing it (e.g. $X$ is normal (3.6.1.23)), then $\pi_0(X)$ is a profinite space.

Proof: $\pi_0(X)$ is an image of $X$, so it is quasi-compact, also it is clearly totally disconnected. To show it is Hausdorff, let $C, D$ be disjoint connected components of $X$, then $C = \cap U_\alpha$, where $U_\alpha$ are clopen. Since $C \cap D = \emptyset$, $U_\alpha \cap D = \emptyset$ for some $\alpha$. and then the image of $U_\alpha$ separates $C$ and $D$ in $\pi_0(X)$.

Locally Profinite Space

Def. (3.6.4.5) [Locally Profinite Space]. A space is called **locally profinite** iff it is a totally disconnected, locally compact Hausdorff topological space.

Prop. (3.6.4.6). A locally closed subsets of a locally profinite space is locally profinite. And compact subsets are profinite.

Proof: Closed subsets are clearly locally profinite, for the open subsets, it is also locally compact.

Cor. (3.6.4.7). Any open covering of a compact subsets of a locally profinite space has an clopen disjoint subcover, by (3.6.4.3).

Prop. (3.6.4.8). The set of all compact open subsets form a basis of the topology of $G$.

Prop. (3.6.4.9). If $X$ is locally profinite and $K$ is a compact subspace of $X$. Let $K \subset \cup U_\alpha$ be an open covering, then there exist f.m. disjoint open compact subsets $V_i \subset X$ that each $V_i \cap K \subset U_\alpha$ for some $\alpha$, and $K \subset \cup V_i$.

Proof: Because $K$ is profinite (3.6.4.6), (3.6.4.3) shows there is a finite disjoint compact open subcover $W_i$ of $U_\alpha$, then $W_i = V_i \cap K$ for $V_i$ compact, and using compactness of $W_i$, we can assume $V_i$ is compact. Finally to make $V_i$ disjoint, we can let $V_i = V_i \setminus (\cup_{k=1}^{i-1} V_k)$.  \(\square\)
5 Real Numbers

References are [H-J99]Chap10 and [Mun00].

Topology

Prop. (3.6.5.1) [\( \mathbb{R} \) is Connected]. \( \mathbb{R} \) is connected, and so are intervals and rays in \( \mathbb{R} \).

Proof: This follows from (3.6.1.20), as the hypothesis is satisfied by \( \forall \)nd the fact for any \( a < b \in \mathbb{R}, a < \frac{a+b}{2} < b \).

Prop. (3.6.5.2). \( \mathbb{R}^n \) satisfies the Heine-Borel property (10.6.1.7), i.e. bounded closed sets are compact.

Proof: It suffices to consider the square metric. If \( A \) is bounded, then \( A \) is in \( [-N, N]^n \) for some number \( N \). \([-N, N]^n \) is compact by (3.6.2.4) and (3.6.2.5).

Borel Set

Def. (3.6.5.3). Let \( U \) be an ultrafilter on a set \( I \) and \( \{a_I\} \) be a bounded sequence of real numbers. Then a number \( a \) is called the \( U \)-limit of \( \{a_I\} \) is for every \( \varepsilon > 0, \{i \in I| |a_i - a| < \varepsilon \} \in U \).

There is at most one limit, because \( \{i \in I| |a_i - a| < \varepsilon \}, \{i \in I| |a_i - b| < \varepsilon \} \) will be disjoint hence cannot both be in \( U \).

Prop. (3.6.5.4) [Generalized Limit]. Let \( U \) be an ultrafilter on \( \mathbb{N} \), then for any bounded sequence of real numbers \( \{a_n\} \), \( \lim_U a_n \) exists. i.e. There is a functional from \( l^\infty \) to \( \mathbb{R} \).

And if \( \{a_n\} \) has a limit pt \( a \) in the usual sense, then \( \lim_U a_n = a \) for any non-principal ultrafilter \( U \), because any \( \{i \in I| |a_i - a| < \varepsilon \} \) is cofinite hence in \( U \) (1.1.8.9).

Proof: Let \( A_x = \{n|a_n < x\} \). Then \( A_x \) is monotone, then we can choose \( c = \sup\{x|A_x \notin U\}\) (1.1.3.19). And it is easily verified that \( c = \lim_U a_n \). □

Cor. (3.6.5.5) [Density Measure]. There exists a measure \( m \) on \( \mathbb{N} \) that \( m(A) = d(A) \) for each set \( A \subset \mathbb{N} \) that has a density \( d(A) \).

Proof: Let \( U \) be a non-principal ultrafilter on \( \mathbb{N} \), let \( m(A) = \lim_U \frac{A(n)}{n} \). It is clearly additive and monotone. And it equals the density by (3.6.5.4) □

6 Separation Axioms

Prop. (3.6.6.1). Any Quasi-compact \( T_0 \) space \( X \) contains a closed point.

Proof: Consider the family of non-empty closed subsets of \( X \), there is a minimal element by quasi-compactness. Choose a minimal element \( T \), and let \( x \in T \), then \( \{x\} = T \). Then \( x \) is closed, otherwise there is some \( x' \neq x \in \{x\} \), and \( \{x'\} \neq \{x\} \) because \( X \) is \( T_0 \). □

Hausdorff

Hausdorffization

Cf. [the Hausdorff Quotient].
Regular

Completely Regular

Normal (T4)

Prop. (3.6.6.2) [Urysohn lemma]. Let $X$ be normal, $A$ and $B$ two closed subset of $X$, then there exists a continuous map from $X$ to $[0, 1]$ that maps $A$ to 0 and $B$ to 1.

Proof: Use the countability of rational numbers to construct a family of $U_q$ s.t. $p < q \Rightarrow \overline{U}_p \subset U_q$. Then choose $f(x) = \inf\{p \in \mathbb{Q} | x \in U_p\}$, then this $f$ meets the requirement. \hfill \Box

Cor. (3.6.6.3) [Tietze extension]. If $X$ is normal and $Y$ is a closed subspace, then any continuous function $f$ on $Y$ can be extended to a continuous function on $X$.

Proof: \hfill \Box

7 Paracompactness

Def. (3.6.7.1) [Paracompactness]. A space $X$ is called paracompact if any open covering $U$ has a locally finite open refinement covering.

Prop. (3.6.7.2) [Characterization of Paracompactness]. If $X$ is regular, then TFAE:

1. Each open cover of $X$ has an open locally finite refinement.
2. Each open cover of $X$ has a locally finite refinement.
3. Each open cover of $X$ has a closed locally finite refinement.
4. Each open cover of $X$ is even. i.e. for any cover, there is an open nbhd $V$ of diagonal of $X \times X$ such that $\forall x, V[x] = \{y | (x, y) \in V\}$ refines the cover.
5. Each open cover of $X$ has an open $\sigma$-discrete refinement.

If this is satisfied, then $X$ is called paracompact.

Proof: $6 \rightarrow 2$: Just minus every open set the part of open sets that appeared in families that ordered before it. $2 + 4 \rightarrow 1$: Use the lemma below, we can transform the cover $A$ into $V[A] \cap U_A$ which is an open locally finite cover. Cf. [General Topology Kelley] and [Mun00]P254. \hfill \Box

Lemma (3.6.7.3). If $X$ satisfies 4, let $U$ be a nbhd of diagonal of $X \times X$, then their exists a symmetric nbhd of diagonal s.t. $V \circ V \subset U$, where $U \circ V = \{(x, z) | (x, y) \in U, (y, z) \in V, \exists y\}$.

Proof: $\forall x$ in $X$, there is a nbhd s.t. $W[x] \times W[x] \subset U$, this is an open cover, so there is a nbhd $R$ of diagonal s.t. $R[x]$ refines it. Hense $R[x] \times R[x] \subset U$. Let $V = R \cap R^{-1}$, $V \circ V$ is the union of sets $V[x] \times V[x]$, so $V \circ V \subset U$. \hfill \Box

Lemma (3.6.7.4). In the preceding proposition, if $X$ satisfies 4, Let $A$ be a locally finite(resp. discrete i.e. intersect only one) family of subsets of $X$, then use the last lemma, there is a nbhd $V$ of diagonal of $X \times X$ such that $V[A] = \{y | (x, y) \in V, \exists x \in A\}$ is locally finite(resp. discrete).
Prop. (3.6.7.5). A locally compact second countable Hausdorff space $X$ is paracompact.

Proof: Let $U$ be a covering of $X$, because $X$ is second countable and locally compact, by (3.6.2.23), we may assume $U$ is a countable covering and consisting of precompact subsets. Moreover, we can change $U_n$ to $U'_n = \bigcup_{i=1}^n U_i$, because if \{$B_\alpha$\} is a locally finite refinement of \{${\cup}_{i=1}^n U_i$\}, then \{$B_\alpha \cap U_n$\} is a locally finite refinement of \{${U}_i$\}. So $U_n \subset U_{n+1}$, and because $U_n$ is compact, we may assume $U_n \subset U_{n+1}$.

Now let $K_n = U_{n+1} \setminus U_n$ (where $U_0 = \emptyset$), then $K_n$ are all compact, and $W_n = U_{n+1} \setminus U_{n-2}$ is an open subset containing $K_n$. So there are f.m. open subsets of $W_n$ that cover $K_n$. There open subsets is then a refinement covering of $U$, and they are locally finite, because any $x \in X$ is contained in $U_n$ for some $n$.

Prop. (3.6.7.6) [Paracompact Spaces are Normal]. A Hausdorff paracompact space $X$ is normal. In particular, a compact Hausdorff space is normal.

Proof: Firstly $X$ is regular: Let $x \in X$ and $B$ a closed subset disjoint from $x$, then because $X$ is Hausdorff, there is a covering of $B$ by open subsets $V_\alpha$ that $x \not\in V_\alpha$. Now consider the open covering \{$X \setminus B, V_\alpha$\} of $X$, then there is a locally finite refinement \{\{$B_\beta$\}\}. Those $B_\beta$ that intersect $B$ is then a locally finite cover of $B$. Let $U$ be the union of these open subsets, then $B \subset U$ and $x \not\in U$, because of the locally finiteness.

To prove $X$ is normal, we do the same but $x$ replaced by a closed subset disjoint from $B$ and use regularity.

Prop. (3.6.7.7) [Paracompactness for Manifolds]. For a connected Hausdorff locally Euclidian space, the condition of paracompact, second countable and a compact exhaustion is equivalent.

Proof: Cf. [Paracompactness and second countable].

Lemma (3.6.7.8) [Shrinking Lemma]. Let $X$ be a paracompact Hausdorff space and \{$U_\alpha$\}$_{\alpha \in I}$ an open covering of $X$, then there is an open covering \{$V_\alpha$\} of $X$ that $V_\alpha \subset U_\alpha$ for any $\alpha$.

Proof: Let $A$ be the family of open subsets $A$ of $X$ that $\overline{A} \subset U_\alpha$ for some $\alpha$, then because $X$ is normal (3.6.7.6), $A$ is a covering of $X$. Then we find a locally finite open covering $\mathcal{B}$ of $A$, and let the covering map be $B_\beta \subset U_{f(\beta)}$, then we can get a covering $V$ of $X$ indexed by $I$ that $V_\alpha = \bigcup_{f(\beta) = \alpha} B_\beta$. This is also locally finite, and $V_\alpha \subset U_\alpha$ by the locally finiteness of $B$.

Prop. (3.6.7.9) [Partition of unity]. In a paracompact Hausdorff space, given any open cover \{$U_\alpha$\}, there exists a partition of unity \{$\rho_\alpha$\} that $\text{supp} \rho_\alpha \subset U_\alpha$, and \{$\text{Supp}(\rho_\alpha)$\} is locally finite. Moreover, if $X$ is locally compact, we can assume

Proof: Using shrinking lemma (3.6.7.8) twice, we can find locally finite open coverings \{$W_\alpha$\}, \{$V_\alpha$\} that $W_\alpha \subset V_\alpha$, $V_\alpha \subset U_\alpha$. Because $X$ is normal, we can find functions $\psi_\alpha$ on $X$ that $\psi(W_\alpha) = 1$, $\psi_\alpha(x) \leq 0$. Then $\text{Supp}(\psi) \subset V_\alpha \subset U_\alpha$, so \{$\text{Supp}(\psi_\alpha)$\} is locally finite. So we can define $\Phi(x) = \sum_\alpha \psi_\alpha(x)$. $\Phi(x) > 0$ for any $x$ because \{$W_\alpha$\} is a covering of $X$. Finally, we define $\rho_\alpha = \psi_\alpha / \Phi$, then this is a partition of unity dominated by \{$U_\alpha$\}. 

$\Box$
8 Metric Space

Def.(3.6.8.1)[Metric Balls]. Let $X$ be a metric space and $x \in X, \delta \in \mathbb{R}_+$, define the metric balls

$$U(x, \delta) = \{y \in X : d(x, y) < \delta\}, \quad D(x, \delta) = \{y \in X : d(x, y) \leq \delta\}.$$

Prop.(3.6.8.2)[Metric Spaces are Paracompact]. Any metric space is paracompact.

Proof: Cf.[Mun00]P257.

Complete Metric Space

Def.(3.6.8.3). A set $E$ in a metric space is called **totally bounded** iff for every $\varepsilon > 0$, there exists a finite set $F$ that $E \subset B(F, \varepsilon)$. This definition is compatible with that in the case of a topological vector space when it is metrizable.

Prop.(3.6.8.4). The closure of a totally bounded set in a metric space is totally bounded.

Proof: For each $\varepsilon > 0$, choose a finite set $F$ that $E \subset B(F, \varepsilon/2)$, then $\overline{E} \subset B(F, \varepsilon)$.

Prop.(3.6.8.5). A totally bounded metric space $X$ is separable.

Proof: $\bigcup N_n$ is dense and countable in $X$, where $N_n$ is a finite $1/n$-net of $X$.

Prop.(3.6.8.6)[Hausdorff]. Let $X$ be a metric space, then:

1. A sequentially compact subset $M$ is totally bounded and the converse is true if $X$ is complete.
2. A subset $M$ is compact iff it is self-sequentially compact iff it is closed and sequentially compact.
3. $M$ is precompact iff it is sequentially compact.

Proof:

1. If $M$ is not totally bounded, then for some $\varepsilon > 0$, we can choose consecutively a sequence of points $x_i$ that $d(x_i, x_j) \geq \varepsilon$, this cannot has a convergent subsequence in $X$.

Conversely, if $M$ is totally bounded, choose a $1/k$-net for each $k$, then for any sequence in $M$, there is a $y_i$ that some infinite subsequence $\{x^{(1)}_n\} \subset B(y_1, 1)$, and consecutively find infinite subsequences $\{x^{(m)}_n\} \subset B(y_k, 1/k)$, then finally choose the diagonal, then it is a Cauchy sequence.

2. If it is compact, given a sequence, if no point is a convergent point, then each point has a nbhd that contains at most one point of the sequence. Then by compactness, there are at most f.m. points, contradiction. A compact set must has the convergent point in itself because it is closed as $M$ is Hausdorff.

Conversely, if it is self-sequentially compact, then it is totally bounded by 1. so if $M$ is not compact, then for each $n$ it has $1/n$-net $N_n$, then there is at least one $x_n$ that $B(x_n, 1/n)$ cannot by covered by f.m. of the covering, The sequence $\{x_n\}$ has a subsequence $\{x_{n_k}\}$ that is convergent to $x$. But $x \in M$ is in some open cover, so $B(x_{n_k}, 1/n_k)$ is contained in some open cover, contradiction.

That closed and sequentially compact is equivalent to self sequentially compact is obvious.
3. If it is precompact, then it is sequentially compact by 2, conversely, if \( x_i \) is a sequence in \( M \), then choose \( |y_n - x_n| \leq 1/n \), so some sequence \( y_{n_k} \) is convergent to \( y_0 \in M \), so \( x_{n_k} \) also converges to \( y_0 \). So \( M \) is self-sequentially compact, so it is compact by 2.

\[ \square \]

**Cor. (3.6.8.7) [Arzela-Ascoli].** For \( M \) compact Hausdorff, \( F \subset C(M) \) is a sequentially compact (precompact, by (3.6.8.6)) subset iff it is uniformly bounded and equicontinuous.

**Proof:** As \( C(M) \) is complete metric space, sequentially compact is equivalent to totally bounded. If it is totally bounded, then it is clearly uniformly bounded, and for every \( \varepsilon > 0 \), find a \( \varepsilon/3 \)-net for \( F \), which means f.m. functions in \( F \) that any other function is \( \varepsilon/3 \)-close to one of them. So they are equicontinuous.

Conversely, if it is uniformly bounded and equicontinuous, for every \( \varepsilon > 0 \), find a finite covering of \( M \) that for any two points \( x, y \) in one cover of them, \( |f(x) - f(y)| < \varepsilon/3 \) for all \( f \in F \). Then choose for each covering a point \( x_i \), consider \( f : F \to \mathbb{C}^n : \varphi \mapsto (\varphi(x_1), \ldots, \varphi(x_n)) \), then the image is bounded, hence precompact by (3.6.5.2), so it is totally bounded by (3.6.8.6). So we can choose an \( \varepsilon/3 \)-net \( \varphi_k \) for \( x_i \) simultaneously, and it is by \( \varepsilon/3 \) argument that these \( \varphi_k \) is a \( \varepsilon \)-net for \( F \). \( \square \)

**Prop. (3.6.8.8) [Fixed point theorem].** If \( X \) is a complete metric space and \( f : X \to X \) satisfies \( d(f(x), f(y)) \leq \lambda d(x, y) \) for some \( 0 \leq \lambda < 1 \), then \( f \) has a unique fixed point in \( X \). If \( X \) is moreover compact, then and \( f \) that \( d(f(x), f(y)) < d(x, y) \) will have a unique fixed point.

**Proof:** \( x + f(x) + f^2(x) + \cdots \) is the fixed point. And uniqueness is easy. For compact case, notice the image \( \text{Im } f^n \) is a descending chain, it must stable to some \( T \). If \( x, y \in Y \) attains the diameter of \( Y \), and let \( x = f(X), y = f(Y) \), where \( X, Y \in T \), then \( d(x, y) < d(X, Y) \leq d(x, y) \), contradiction. \( \square \)

**Prop. (3.6.8.9) [Dilation Closed].** If \( X, Y \) are metric spaces that \( X \) is complete metric space, then if \( f : X \to Y \) is continuous function that is a dilation, i.e. \( d(f(x_1), f(x_2)) \geq d(x_1, x_2) \), then \( f(X) \) is closed.

So a continuous dilation map on a complete metric space is a closed map.

**Proof:** If \( y \in f(X) \), then because \( Y \) is metric, there are \( x_n \) that \( y = \lim f(x_n) \). Thus \( \{f(x_n)\} \) is Cauchy in \( Y \), and \( \{x_n\} \) is Cauchy too. So there is a \( x = \lim x_n \), and clearly \( f(x) = y \). \( \square \)

**Compact Metric Space**

**Lemma (3.6.8.10) [Lebesgue Number Lemma].** For any open covering \( U_i \) of a compact metric space \( X \), there exists a \( \delta > 0 \) that any subset \( X \) of diameter smaller than \( \delta \) is contained in some \( U_i \).

**Proof:** If \( X \) is in the covering \( U_i \), then there is nothing to prove, otherwise, it suffices to assume the covering is a finite covering, let \( C_i = X - U_i \), and let \( f(x) = \frac{1}{n} \sum d(x, C_i) \). Notice \( f(x) > 0 \), because \( x \notin C_i \) for some \( C_i \). Now it is also continuous, so it has a minimal value \( > \delta > 0 \).

Now if \( B \) has diameter smaller than \( \delta \), then if \( x_0 \in B, \delta < f(x_0) < d(x, C_{i_0}) \), where \( d(x, C_{i_0}) \) is the maximal among \( d(x, C_k) \), and \( B \in B(x, \delta) \), thus \( B \in U_{i_0} \). \( \square \)

**Prop. (3.6.8.11) [Uniform Continuity Theorem].** If \( f : X \to Y \) is a continuous map between two metric spaces that \( X \) is compact, then \( f \) is uniformly continuous.
3.6. TOPOLOGY I

Proof: Take an open covering of \( Y \) with balls \( B(y_i, \varepsilon/2) \) of diameter \( \varepsilon/2 \), and consider their inverse image, then choose the lebesgue number \( \delta \) for this covering.(3.6.8.10), we see that for any \( d(x, y) < \delta \), \( d(f(x), f(y)) < \varepsilon \).

Prop.(3.6.8.12). If \( f \) is an isometry of a compact metric space \( X \), then it is a bijection thus an homeomorphism.

Proof: It is clearly injective. If it is not surjective, then choose a \( x \notin \text{Im}(f) \), because \( \text{Im}(f) \) is compact hence closed in \( X \), \( d(x, \text{Im}(f)) = \varepsilon > 0 \). Now consider the minimal \( N \) that we can cover \( X \) with open subsets of diameter smaller than \( \varepsilon \), this \( N \) exists because \( X \) is compact. Now if \( U_i \) covers \( X \), then the one that contains \( x \) cannot intersect with \( \text{Im}(f) \). But \( f^{-1}(U_i) \) is an open cover of \( X \) with smaller numbers of open subsets, contradiction.

9 Baire Space

Def.(3.6.9.1)[Baire Spaces]. A subset of a topological space \( X \) is called of first category if it is contained in some countable union of closed subsets of \( X \) having no interior point. It is called of second category if it is not of first category.

A Baire space is a topological space that any nonempty open subsets of \( X \) is of second category.

Prop.(3.6.9.2)[Baire Category Theorem]. Every complete metric space & locally compact Hausdorff space is a Baire space.

Proof: Choose consecutively (precompact)open subsets that doesn’t intersect \( \overline{E_n} \) to find a limit point.

10 Uniform Space

Def.(3.6.10.1)[Uniform Spaces].

Def.(3.6.10.2)[Cauchy Filter in the Topological Group Case]. A Cauchy filter is a topological Abelian group is a filter \( \mathcal{F} \) that for any nbhd \( U \) of 0, there exists \( E \in \mathcal{F} \) that \( x - y \in U \) if \( x, y \in E \).

Def.(3.6.10.3)[Complete Uniform Spaces]. A topological Abelian group is called complete uniform space iff it is Hausdorff, and any Cauchy filter has a limit.

11 Manifolds

Def.(3.6.11.1)[Manifolds]. A (topological) manifold of dimension \( n \) is a topological space that is Hausdorff, second countable and locally Euclidean. By(3.6.7.7), the last condition is equivalent to say it is paracompact.

The category of topological manifolds is denoted by \( \text{Mani} \).

Thm.(3.6.11.2) [Annulus Theorem, Rado-Moise-Quinn-Kirby]. For any map \( h : \mathbb{R}^n \to \mathbb{R}^n \) that maps \( D^n \) into its interior, there is a homeomorphism \( D^n \setminus h(D^n) \cong S^{n-1} \times I \) that identifies \( \partial D^n \) and \( h(\partial D^n) \) with \( S^{n-1} \times \{0\}, S^{n-1} \times \{1\} \) resp.

Proof:
Triangularizations

Def. (3.6.11.3) [Triangularizations]. A triangularizable space is a space that is homeomorphic to the geometrization of a simplicial set (3.12.3.7).

Thm. (3.6.11.4) [Triangularization of Surfaces]. All compact connected surface is triangularizable.

Proof: □

Surfaces

Def. (3.6.11.5) [Topological Surfaces]. A topological surface (with boundaries) is a topological manifold of dimension 2 (with boundaries).

Def. (3.6.11.6) [Planer Glueing Diagram]. A planer glueing diagram is a polygon with some glueing of its edges with orientations clockwise such that no three edges are glued together. We can label the edges by symbols and their inverses. Different symbols are considered not glued together. For example, $aba^{-1}b^{-1}, abab$.

A compact planer glueing diagram is a planer glueing diagram that every symbol appear exactly twice in the edges of the polygon.

Prop. (3.6.11.7). The space correspond to a planer glueing diagram is a compact topological surface with boundaries.

The space correspond to a compact planer glueing diagram is a compact topological surface.

Proof: It is compact as a quotient of a compact space. It can verified that it is locally Euclidean at each space. And it is clearly Hausdorff. □

Lemma (3.6.11.8). $T^2 \# \mathbb{RP}^2 \cong \mathbb{RP}^2 \# \mathbb{RP}^2 \# \mathbb{RP}^2$.

Proof: By ??, it suffices to show that $aabcb^{-1}c^{-1}$ is homeomorphic to $eefgg$. For this, use cut-and-paste.? □

Thm. (3.6.11.9) [Classification of Surfaces]. Any compact topological surface is homeomorphic to exactly one of the following: $S^2, \#^n T^2$ or $\#^n \mathbb{RP}^2$, $n \in \mathbb{Z}_+$. The corresponding planer diagram is $aa^{-1}, a_1b_1a_1^{-1}b_1^{-1} \ldots a_nb_n a_n^{-1}b_n^{-1}, e_1e_1e_2e_2 \ldots e_ne_n$.

Proof: By triangularization theorem (3.6.11.4), it is easy to see that any compact surface is the space corresponding to a compact planer diagram. Then it suffices to show any compact planer diagram is isomorphic to either $aa^{-1}, a_1b_1a_1^{-1}b_1^{-1} \ldots a_nb_n a_n^{-1}b_n^{-1}, e_1e_1e_2e_2 \ldots e_ne_n$.

Firstly we can reduce to the case where all vertices are glued together: Take a vertex $P$, then we can spot all the vertices that are glued to $P$. If these are not all the vertices, we can find an edge $e = PQ$, and let $RPQ$ be a triangle, then we can cut this triangle out to paste along the edge pairing $e$. Then we can reduce the number of vertices glued to $P$. Eventually, we can eliminate $P$.

Secondly we can collect all edges with the same orientation (i.e. $\ldots a \ldots a \ldots$) to be adjacent: (i.e. $\ldots aa \ldots$). To do this, suppose $a = P_1Q_1 = P_2Q_2$, we simply cut along the line $P_1P_2$ and glue $a$ together.

Now if all edges glued together are of the same orientations, then it is clearly isomorphic to $\#^n \mathbb{RP}^2$. Otherwise there are edges $a, a^{-1}$ glued together with the opposite orientation. Then
there must be another pair $b, b^{-1}$ s.t. these four pairs are ordered by $a, b, a^{-1}, b^{-1}$. This is because otherwise there will be two vertices. Then by some cut-and-paste, we can move these edges together as $\ldots aba^{-1}b^{-1}\ldots$. By induction, we can make all edges with the opposite orientations together and in pairs.

Thus our diagram is a connected sum of $T^2$ and $\mathbb{RP}^2$. Then we can reduce the diagram to one of the three kinds by (3.6.11.8).

Finally, it suffices to show these three kinds are different: Their Euler characteristics are

$$
\chi(S^2) = 2, \quad \chi(\#^n T^2) = 2 - 2n, \quad \chi(\#^n \mathbb{RP}^2) = 2 - n.
$$

So the only case their Euler characters equal are $\chi(\#^n T^2) = \chi(\#^2 \mathbb{RP}^2)$. But in this case, they are still not homeomorphic, as $H_2(\#^n T^2) = \mathbb{Z}$ and $H_2(\#^2 \mathbb{RP}^2) = 0$. □

12 Common Spaces

Def. (3.6.12.1) [Torus]. The $(n$-dimensional) torus $T^n$ is defined to be $T^n = (S^1)^n$.

Def. (3.6.12.2) [RP $^n$]. The real projective space $\mathbb{RP}^n$ is the $\mathbb{R}$-points of $\mathbb{RP}_\mathbb{R}$ with the canonical topology.

Def. (3.6.12.3) [Möbius Band]. The Möbius band is the space defined to be the planer glueing diagram $abac$.

Def. (3.6.12.4) [Klein Bottle]. The Klein bottle $K^2$ is the space defined by the planer glueing diagram $aba^{-1}b$. 
3.7 Model Categories

Main references are [Model Category and Simplicial Methods, Goerss], [Model Categories, Kan-
tor], [Homotopy Theories and Model Categories, Dwyer/Spalinski], [Higher Topos Theory, Lurie].

Prop.(3.7.0.1). If \(C\) is a class of morphisms in a category, we denote \(l(C)\) the set of morphisms that
has left lifting property w.r.t. all morphisms in \(C\), and \(r(C)\) the set of morphisms that have right
lifting property w.r.t. all morphisms in \(C\). Then \(l(C)\) is stable under pushout and \(r(C)\) is stable
under base change.

Def.(3.7.0.2) [Model Structure]. A model structure on a category \(C\) is three classes of mor-
phisms: fibrations, cofibrations and weak equivalences that satisfy the following axioms: (Den-
ote a A trivial (co)fibration is a (co)fibration that is also a weak equivalence.)
M1 \(C\) has finite limits and colimits.
M2 (two out of three)If two of \(f, g, fg\) is weak equivalence, then so is the third.
M3 (retracts) Fibrations, cofibrations and weak equivalences are closed under retract.
M4 (lifting property) We have a lifting property with a cofibration \(i\) and fibration \(p\) when either
of them is a weak equivalence.
M5 (factorization) Any map \(f\) can be factored as \(pi\) where \(i\) is trivial cofibration and \(p\) is a fibration,
and also as \(pi\) where \(i\) is a cofibration and \(p\) is a trivial fibration.

Remark(3.7.0.3). Notice the axioms are symmetric in fibrations and cofibrations, thus the opposite
category \(\mathcal{C}^{op}\) has a natural model structure. So whenever we write a theorem, we should always
remember its dual counterpart.

Lemma(3.7.0.4)[Closedness]. A model category satisfies retraction axiom iff:
- fibration= \(r(\text{trivial cofibrations})\),
- cofibration= \(l(\text{trivial fibrations})\),
- weak equivalence= \(uv\), where \(v\) is in \(l(\text{fibrations})\) and \(u\) in \(r(\text{cofibrations})\).

Proof: If these are satisfied, retraction axiom is easy: A retract satisfies the same lifting properties.
Hence retraction of a (co)fibration is a (co)fibration. For retracts weak equivalences, Cf.[Quillen,
Homotopical Algebra, Chap5.2].

Conversely, using(3.1.6.7), we first factorize a \(p = f \circ i\), where \(i\) is a trivial cofibration, then
because \(p\) is in \(r(i)\), \(p\) is a retraction of \(f\) hence a fibration. And similarly for cofibrations and weak
equivalences. \(\square\)

Cor.(3.7.0.5). In a model category,
- trivial fibrations= \(r(\text{cofibrations})\),
- trivial cofibrations= \(l(\text{fibrations})\).

Proof: The proof is the same as that of(3.7.0.4). \(\square\)

Cor.(3.7.0.6). In a model category, the class of (trivial)fibrations is stable under base change and
the class of (trivial)cofibrations is stable under cobase change.

Prop.(3.7.0.7). Let \(p\) be a fibration in \(C_{\text{cf}}\), then \(p \in r(\text{Cof})\) iff \(\gamma(p)\) is an isomorphism, Cf.[Quillen
5.2]. So if conditions of(3.7.0.4) are satisfied (i.e. \(C\) is a closed model category), \(\gamma(f)\) is an isomor-
phism iff \(f\) is a weak equivalence by the characterization of weak-equivalence of(3.7.0.4).
**Def. (3.7.0.8) [Proper].** A model category is called **left proper** if weak equivalences are stable under cobase change by cofibrations. Dually it is called **right proper** if weak equivalences are stable under base change by fibrations.

**Lemma (3.7.0.9) [Cofibration is Left Proper].** For a pushout diagram

\[
\begin{array}{ccc}
  A & \xrightarrow{i} & B \\
   \downarrow{j} & & \downarrow{j'} \\
  A' & \xrightarrow{i'} & B'
\end{array}
\]

in a model category \( \mathcal{C} \), if \( i \) is cofibration and \( A, A' \) are cofibrant, and \( j \) is weak equivalence, then \( j' \) is also weak equivalence.

**Proof:** It suffices to show \( j' \) is an isomorphism in \( \text{Ho}(\mathcal{C})(3.7.1.15) \). For this, by Yoneda lemma, it suffices to show \( \text{Hom}_{\text{Ho}(\mathcal{C})}(B', Z) \cong \text{Hom}_{\text{Ho}(\mathcal{C})}(B, Z) \) for any fibrant object \( Z \).

For surjectivity, by (3.7.1.18), it suffices to show \( \pi(B', Z) \cong \pi(B, Z) \). Given a map \( f : B \to Z \), because \( j \) is weak equivalence, there is a map \( g : A' \to Z \) that \( g \circ j \sim f \circ i \). Then by (3.7.1.10), there is a \( f' \sim f \) that \( f' \circ i = g \circ j \), which determines a morphism \( B' \to Z \).

For injectivity, If \( P \) is a path object that \( H : B \to P \) induces a homotopy between maps \( s \circ j', s' \circ j' \), then we need to extend this homotopy to \( \tilde{H} : B' \to P \), and the method is the argument is the same as above. \( \square \)

### 1 Homotopies

**Def. (3.7.1.1) [Cylinder Objects].** A **cylinder object** for an object \( X \) is an object \( X \wedge I \) which gives a factorization of the natural map \( X \coprod X \to X \) as \( X \coprod X \xrightarrow{j} X \wedge I \xrightarrow{i} X \), where \( j \in W \). It is called a **good cylinder object** if \( i \) is a cofibration, and **very good cylinder object** if \( j \) is trivial fibration. By factorization axiom, every object has a very good cylinder object.

There are two natural morphisms \( X \Rightarrow X \wedge I \), denoted by \( \partial_0 \) and \( \partial_1 \).

Dually we can define **path object** \( Y^I \) for \( Y \), and every object has a very good path object.

**Prop. (3.7.1.2).** If \( A \) is cofibrant and \( A \wedge I \) is a cylinder object for \( A \), then \( \partial_i : A \to A \times I \) are trivial cofibrations.

**Proof:** Because it’s pushout of \( \emptyset \to A \) and \( \sigma \circ \partial_i = \text{id}_A \). \( \square \)

**Cor. (3.7.1.3).** if \( f \sim^l g \), then \( f \) is a weak equivalence iff \( g \) is a weak equivalence.

**Proof:** This is because \( f = H \circ \partial_0, g = H \circ \partial_1 \), and we can use (3.7.1.2). \( \square \)

**Def. (3.7.1.4) [Homotopies].** Two morphisms \( f, g : X \to Y \) are called **(good/very good) left homotopic**, denoted by \( f \sim^l g \) iff there is a (good/very good) cylinder object \( X \coprod X \to X \wedge I \) with \( X \wedge I \to Y \) that induce \( (f, g) : X \coprod X \to Y \). Dually for right homotopies. And we denote by \( \pi^l(A, B)/\pi^r(A, B) \) the equivalence classes of \( \text{Hom}(A, B) \) under the equivalence relation generated by left/right homotopies.

If \( f, g \in \text{Hom}(X, Y) \) and \( \varphi \in \text{Hom}(Y, Z) \) that \( \varphi \circ f = \varphi \circ g \), then \( f, g \) is called **left homotopic over** \( Z \) if there is a homotopy \( H \) of \( f \sim^l g \) that \( \varphi H \) is the trivial homotopy. Dually for **right homotopic under** \( X \).
Lemma (3.7.1.5) [Very Good Homotopies]. For \( f, g \in \text{Hom}(X, Y) \), if \( f \sim_l g \), then \( f, g \) are good left homotopic. And if \( Y \) if fibrant, then \( f, g \) are moreover very good left homotopic.

Proof: The first assertion is each, just choose a factorization of the cylinder object \( X \coprod X \xrightarrow{j} X \times I \) that \( i \) is cofibrant. If \( Y \) is fibrant, then we further factorize \( X \times I \xrightarrow{i} X \times I'' \xrightarrow{j} X \), where \( i \) is cofibrant and \( j \) is trivial fibration, then by two out of three, \( i \) is also trivial cofibration, and it suffices to extend the homotopy \( X \times I' \to Y \) to \( X \times I'' \to Y \), and this is because \( Y \) is fibrant. \( \square \)

Prop. (3.7.1.6) [Homotopy is Equivalence Relation]. If \( A \) is cofibrant, then the left homotopy is an equivalence relation on \( \text{Hom}(A, B) \).

Proof: Reflexivity and symmetry is trivial, the only problem is transitivity, so we construct a glueing \( A \times I'' \) as the pushout of \( \partial_1 : A \to A \times I \) and \( \partial_0 : A \to A \times I' \). \( A \times I'' \to A \) is a weak equivalence by the universal property and (3.7.0.4), so this is a cylinder object. The rest is easy. \( \square \)

Prop. (3.7.1.7) [Properties of Left Homotopies]. If \( A \) is cofibrant and \( f, g \in \text{Hom}(A, B) \), then
1. If \( f, g \) are right homotopic, then \( s \to B^I \) can be chosen to be trivial Cof.
2. If \( f, g \) are right homotopic, then so does \( uf \sim ug \) or \( fv \sim gv \). Thus if \( A \) is cofibrant, there is a composition map: \( \pi^r(A, B) \times \pi^r(B, C) \to \pi^r(A, C) \).
3. For any trivial fibration \( X \to Y \), \( \pi_l(A, X) \to \pi^l(A, Y) \) is a bijection.
And dual arguments hold for fibrant objects.

Proof:
1. factorize \( B \to B^I \) to \( B \to B'' \to B^I \) where \( B \to B'' \in \text{TCof} \) and \( B'' \to B^I \in \text{W} \), so \( B'' \) is also a cylinder object and the homotopy \( A \to B^I \) can be lifted to \( A \to B'' \).

\[
\begin{array}{ccc}
B & \xrightarrow{su} & C^I \\
\downarrow s & & \downarrow (d_0, d_1) \\
B^I & \xrightarrow{(d_0 u, d_1 u)} & C \times C
\end{array}
\]

will give the desired homotopy.

3. the map is well-defined, it is surjective because of lifting property, and it is injective because \( A \coprod A \to A \times I \in \text{Cof} \) so the homotopy can be lifted to \( X \).
Cf. [Homotopy Theories and Model Categories, P20, 21]. \( \square \)

Lemma (3.7.1.8) [Left and Right Homotopies]. If \( X \) is cofibrant, then for \( f, g \in \text{Hom}(X, Y) \), if \( f \sim_l g \), then \( f \sim_r g \). And the dual conclusion holds for \( Y \) fibrant.

In particular, for morphisms between bifibrant objects, left and right homotopic are equivalent.

Proof: Consider a cylinder object \( j : X \times I \to X \) for \( X \) and a path object for \( Y \). Suppose \( f, g \) are left homotopic via a map \( H : X \times I \to Y \), then we consider the diagram

\[
\begin{array}{ccc}
X & \xrightarrow{f} & Y & \xrightarrow{Y^I} \\
\downarrow \partial_1 & & \downarrow & \\
X \times I & \xrightarrow{(j \times H \times)} & Y \times Y
\end{array}
\]
Then it can be solved by some \( \tilde{H} \) because \( \partial_1 \) is trivial cofibration (3.7.1.2), and then it can be checked \( H \circ \partial_1 \) gives the desired right homotopy.

\[ \square \]

**Prop.** (3.7.1.9) **[Whitehead’s Theorem].** Let \( X, Y \in \mathcal{C} \) be bifibrant, then a map \( f : X \to Y \) is an equivalence iff there is a \( g : X \to Y \) that \( fg \) and \( gf \) are homotopic to id.

**Proof:** Cf. [Homotopy Theories and Model Categories, P23].

\[ \square \]

**Prop.** (3.7.1.10) **[Lifting Criterion].** Let \( \mathcal{C} \) be a model category and \( i : A \to B \) be a cofibration between cofibrant objects, and \( X \) is fibrant, \( g : B \to X \), \( f : A \to X \) satisfies \( g \circ i \sim f \), then there is a \( g' \sim g \) that \( g' \circ i = f \).

**Proof:** Choose a good cylinder object \( C(A) \) for \( A \) and factorize
\[
C(A) \coprod_{A \coprod A} (B \coprod B) \to C(B) \to B
\]
where the first map is cofibration and the second is trivial fibration, then \( C(B) \) is a good cylinder object for \( B \).

The homotopy is given by a map \( C(A) \coprod_A B \to X \), and we check \( (A) \coprod_A B \to C(B) \) is a trivial cofibration (check \( C(A) \coprod_A B \to C(B) \) is a weak equivalence using (3.7.0.6) and check \( C(A) \coprod_A B \to C(A) \coprod_B (B \coprod B) \) is a cofibration as a cobase change of \( A \to B \) and \( C(A) \coprod_A (B \coprod B) \to C(B) \) is a cofibration by definition), so the homotopy extends to a homotopy \( C(B) \to X \), which is a homotopy between \( g \) and some \( g' \) and \( g' \circ i = f \).

\[ \square \]

**Def.** (3.7.1.11). Let \( C_c, C_f, C_{cf} \) denote the full subcategory of cofibrant, fibrant and cofibrant-fibrant objects. And we define \( \pi C_c \) as the category module right homotopy equivalence between morphisms, dually for \( \pi C_f \).

Notice (3.7.1.7) assures \( \pi C_c, \pi C_f \) are truly categories.

Notice for \( C_{cf} \), left homotopy is equivalent to right homotopy by (3.7.1.8), so \( \pi C_{cf} \) is full subcategory for both \( \pi C_c \) and \( \pi C_f \).

**Lemma** (3.7.1.12) **[Fibrant and Cofibrant Replacement].** For an object \( X \) in a model category \( \mathcal{C} \), the axioms show there is a cofibrant object \( QX \) and a trivial fibration \( QX \to X \). Also there is a fibrant object \( RX \) and a trivial cofibration \( X \to RX \). We fix choices of \( Q, R \) that is identity on bifibrant objects, and consider it a mapping from \( \mathcal{C} \) to \( \mathcal{C} \).

Then given any morphism \( f : X \to Y \), there is a morphism \( \tilde{f} : QX \to QY \) lifting \( f \), and \( \tilde{f} \) depends up to left and right homotopy only on \( f \). And if \( Y \) is fibrant, then it depends up to left and right homotopy only on the left homotopy classes of \( f \).

Dually assertions also holds, so we have functors: \( Q : \mathcal{C} \to \pi \mathcal{C}_c \) and \( R : \mathcal{C} \to \pi \mathcal{C}_f \).

**Proof:** The existence of the lifting follows from the fact \( QX \) is fibrant and \( QY \to Y \) is trivial fibration. The uniqueness of left homotopy follows from (3.7.1.7), and also right homotopy, because \( QX \) is cofibrant and use (3.7.1.8). For the last assertion, notice when \( Y \) is fibrant, (3.7.1.7) shows the left homotopy class of \( QX \to Y \) is determined, and use (3.7.1.7) again, the class of \( \tilde{f} \) is also determined.

\[ \square \]

**Cor.** (3.7.1.13). The restrictions define functors \( Q' : \pi \mathcal{C}_c \to \pi \mathcal{C}_{cf} \) and \( R' : \pi \mathcal{C}_f \to \pi \mathcal{C}_{cf} \).
Def. (3.7.1.14) [Homotopy Category]. For any model category $\mathcal{C}$, we construct a homotopy category $\text{Ho}(\mathcal{C})$ whose objects are the same as $\mathcal{C}$, but $\text{Hom}_{\text{Ho}(\mathcal{C})}(X, Y) = \pi\text{c}_{\mathcal{C}}(RQX, RQY)$.

There is a functor $\gamma : \mathcal{C} \to \text{Ho}(\mathcal{C})$ by sending $X$ to $RQX$, by (3.7.1.12).

Prop. (3.7.1.15) [Weak Equivalence and Isomorphisms]. A morphism in $\mathcal{C}$ maps to an isomorphism in $\text{Ho}(\mathcal{C})$ iff it is a weak equivalence. The morphisms in $\text{Ho}(\mathcal{C})$ are generated by the image of morphisms in $\mathcal{C}$ and the inverse of images of weak equivalences in $\mathcal{C}$.

Proof: If $f \in \mathcal{C}$ is a weak equivalence, then $f' = RQ(f)$ is also a weak equivalence, by two out of three lemma. Then Whitehead theorem (3.7.1.9) shows $f'$ is an isomorphism in $\pi\text{c}_{\mathcal{C}}$ hence in $\text{Ho}(\mathcal{C})$. Conversely, if $f'$ has an inverse in $\text{Ho}(\mathcal{C})$, then $f'$ is a weak equivalence by Whitehead (3.7.1.9) again, and so is $f$.

For the last assertion, just notice $\text{Hom}(RQX, RQY) \to \text{Hom}_{\text{Ho}(\mathcal{C})}(X, Y)$ is a surjection, and $X \to RQX, Y \to RQY$ are weak equivalence hence are isomorphisms in $\text{Ho}(\mathcal{C})$. □

Cor. (3.7.1.16). If $F, G : \text{Ho}(\mathcal{C}) \to \mathcal{D}$ are two functors and $t : F \circ \gamma \to G \circ \gamma$ is a natural transformation, then $t$ also gives a natural transformation $F \to G$.

Proof: This is because the objects of $\text{Ho}(\mathcal{C})$ are the same as that of $\mathcal{C}$, and the morphisms are generated by $\gamma(f)$ and $\gamma(g)^{-1}$ where $g$ is a weak equivalence. Then the desired transformation commutative diagrams commute. □

Lemma (3.7.1.17). Let $\mathcal{C}$ be a model category and $F : \mathcal{C} \to \mathcal{D}$ be a functor taking weak equivalences to isomorphisms, then if $f \sim^l g$ or $f \sim^r g$, $F(f) = F(g)$.

Proof: We only prove for left homotopy and the right homotopy is dual: given the cylinder object $A \wedge I$, just need to prove that $F(\partial_0) = F(\partial_1)$. □

Prop. (3.7.1.18). Suppose $A$ is cofibrant and $X$ is fibrant, then the map $\gamma : \text{Hom}(A, X) \to \text{Hom}_{\text{Ho}(\mathcal{C})}(A, X)$ is surjective, and induces a bijection $\pi(A, X) \cong \text{Hom}_{\text{Ho}(\mathcal{C})}(A, X)$.

Proof: (3.7.1.17) shows $\gamma$ identifies homotopic maps. Consider the following commutative diagram:

\[
\begin{array}{ccc}
\pi(RA, QX) & \longrightarrow & \pi(A, X) \\
\downarrow \gamma & & \downarrow \gamma \\
\text{Hom}_{\text{Ho}(\mathcal{C})}(RA, QX) & \longrightarrow & \text{Hom}_{\text{Ho}(\mathcal{C})}(A, X)
\end{array}
\]

The second vertical arrow is isomorphism by (3.7.1.15), the first arrow is isomorphism by (3.7.1.7). The left vertical arrow is identity by construction, so the right vertical arrow is also isomorphism. □

Prop. (3.7.1.19) [Homotopy Category as Localizing Category]. Let $\mathcal{C}$ be a model category and $W$ the class of weak equivalences, then the functor $\gamma : \mathcal{C} \to \text{Ho}(\mathcal{C})$ is the localizing category of $\mathcal{C}$ w.r.t $S$.

Proof: Cf. [Homotopy Theories and Model Categories, P29]. □
2 Quillen Functors and Derived Functors

Def. (3.7.2.1) [Quillen Adjunctions]. An adjoint pair of functors \((F, G)\) between model categories is called a Quillen adjunction if \(F\) preserves cofibrations and \(G\) preserves fibrations. By adjointness and (3.7.0.4), in fact \(F\) preserves also trivial cofibrations and \(G\) preserves trivial fibrations.

It is called a Quillen equivalence if for any cofibrant object \(C\) and fibrant object \(D\), a map \(C \to G(D)\) is a weak equivalence iff the adjoint map \(F(C) \to D\) is a weak equivalence.

Def. (3.7.2.2) [Derived Functors]. Let \(\mathcal{C}\) be a model category and \(F: \mathcal{C} \to \mathcal{D}\) a functor, then a left derived functor of \(F\) is a left Kan extension of \(F\) along \(\gamma: \mathcal{C} \to \text{Ho}(\mathcal{C})\).

Dually we can define right derived functors.

Prop. (3.7.2.3) [Existence of Derived Functors]. In the situation of (3.7.2.2), if \(F\) maps weak equivalences between cofibrant objects to isomorphisms in \(\mathcal{D}\), then the left derived functor \((LF, t)\) exists, and for each cofibrant object \(X\), the morphism \(t_X: LF(X) \to F(X)\) is an isomorphism.

Dually for the right derived functor case.

Proof: Cf. [Homotopy Theories and Model Categories, P42].

Lemma (3.7.2.4). Let \(\mathcal{C}\) be a model category and \(F: \mathcal{C}_c \to \mathcal{D}\) be a functor that maps trivial cofibrations in \(\mathcal{C}_c\) to isomorphisms, then \(F\) maps right-homotopic morphisms to the same morphism.

Proof: Let \(H: A \to B^I\) be a right homotopy between \(f\) and \(g\), where \(B^I\) is a very good path object (3.7.1.5), then \(B \to B^I\) is a trivial cofibration, and thus mapped by \(F\) to an isomorphism. Then we can show \(F(\partial_0) = F(\partial_1)\), and then \(F(f) = F(g)\).

Def. (3.7.2.5) [Total Left Derived Functors]. Let \(F: \mathcal{C} \to \mathcal{D}\) be a morphism of model categories, then a total derived functor

\[ LF: \text{Ho}(\mathcal{C}) \to \text{Ho}(\mathcal{D}) \]

is defined to be a left derived functor of the morphism \(\mathcal{C} \to \mathcal{D} \to \text{Ho}(\mathcal{D})\).

Lemma (3.7.2.6) [Brown]. Let \(F\) be a morphism of model categories that maps trivial cofibration between cofibrant objects to weak equivalences, then it preserves weak equivalences between cofibrant objects.

Proof: If \(f: A \to B\) is a weak equivalence between cofibrant objects, then we can factor the morphism \((f, \text{id}): A \coprod B \to B\) as \(A \coprod B \xrightarrow{q} C \xrightarrow{p} B\) that \(q\) is cofibration and \(p\) is trivial fibration. It can be shown that \(q \circ \partial_i: B \to C\) are trivial fibrations and \(C\) is cofibrant, thus \(F(q \circ \partial_i)\) are weak equivalences, and hence also \(F(p)\) is weak equivalence and so does \(F(f)\).

Prop. (3.7.2.7) [Total Derived Functors and Quillen Equivalence]. If \((F, G)\) is a pair of Quillen functors between two model categories \(\mathcal{C}, \mathcal{D}\), then total derived functors

\[ LF: \text{Ho}(\mathcal{C}) \rightleftharpoons \text{Ho}(\mathcal{D}) : RG \]

exists and form an adjoint pair. And if \((F, G)\) is a Quillen equivalence, then \((LF, RG)\) defines an equivalence of homotopy categories.
Proof: By (3.7.2.3) and its dual and (3.7.2.6), the total derived functors \( LF, RG \) exist.

Next for \( A \) cofibrant in \( \mathcal{C} \) and \( X \) fibrant in \( \mathcal{D} \), we can show the adjunction map \( \text{Hom}(A, G(X)) \cong \text{Hom}(F(A), X) \) preserves homotopy equivalence relations (3.7.1.8) and induces an isomorphism \( \pi(A, G(X)) \cong \pi(F(A), X) \): If \( H : A \land I \to X \) is a good homotopy between \( f, g \), then \( A \land I \) is cofibrant, and because \( F \) preserves colimits and because of (3.7.2.6), \( F(A \land I) \) is cylinder object for \( F(A) \), thus \( f^\flat \sim g^\flat \). A dual argument shows the converse.

Now for any \( A \in \mathcal{C} \) and \( X \in \mathcal{D} \), there is a bijection
\[
\text{Hom}_{\text{Ho}(\mathcal{C})}(A, RG(X)) \cong \pi(QA, G(SX)) \cong \pi(F(QA), SX) \cong \text{Hom}_{\text{Ho}(\mathcal{D})}(LF(A), X)
\]
where the first isomorphism is due to the fact \( QA \to RQA \) is trivial cofibration and \( G(SX) \) is fibrant, thus we can use (3.7.1.7), dually for the last isomorphism.

Finally if \((F, G)\) is a Quillen equivalence, then consider the unit map:
\[
A \to RG(LF(A)).
\]
If \( A \) is cofibrant, then this is \( A \to G(SF(A)) \) which is a weak equivalence because \( F(A) \to SF(A) \) does, so it is an isomorphism in \( \text{Ho}(\mathcal{C}) \). Now any object in \( \text{Ho}(\mathcal{C}) \) is isomorphic to a cofibrant object, we know the unit map is an isomorphism. Dually the counit map is an isomorphism, thus \( LF, GF \) are a pair of equivalences.

3 Combinatorial Model Structure

Cf.[HTT, A.2.6]

Def.(3.7.3.1)[Combinatorial Model Category]. A cofibrantly generated model category is a model category \( \mathcal{C} \) that
- there is a set \( I \) of generating cofibrations that generates the class of cofibrations as the minimal weakly saturated class containing \( I \).
- there is a set \( J \) of generating trivial cofibrations that generates the class of trivial cofibrations as the minimal weakly saturated class containing \( J \).
A combinatorial model category is a cofibrantly generated and presentable model category.

4 Generating new Model Categories

Prop.(3.7.4.1). If \( \mathcal{C} \) is a model category and \( A \) is an object, then the undercategory \( \mathcal{C}_{/A} \) and the overcategory \( \mathcal{C}_{A\setminus} \) have natural model structures.

Prop.(3.7.4.2)[Transfer Model Structures via Left Adjoint]. Let
\[
F : \mathcal{C} \rightleftarrows \mathcal{D} : G
\]
be an adjoint pair of categories and
- \( \mathcal{C}, \mathcal{D} \) are complete and cocomplete,
- \( \mathcal{C} \) is a cofibrantly generated model category,
- \( \mathcal{C}, \mathcal{D} \) are presentable categories and \( G \) is an accessible functor.
- If we define a morphism \( f \) in \( \mathcal{B} \) a fibration/weak equivalent iff \( G(f) \) is a fibration/weak equivalence, and a cofibration iff it has left lifting property w.r.t. trivial fibrations, then \( \mathcal{B} \) has a path object factorization and a fibrant replacement operator.
Then this defines a cofibrantly generated model category on \( \mathcal{B} \), and makes \((F,G)\) a Quillen adjunction.

**Proof:** It suffices to show that the factorization property holds: In fact, it suffices to show if \( I, J \) are generating classes of cofibrations and trivial cofibrations, then \( F(I), F(J) \) are generating classes of cofibrations and trivial cofibrations. But this suffices to show \( F(J) \) is are weak equivalence. For this, show that any morphism in \( \mathcal{B} \) that has left lifting properties w.r.t. all fibrations is a weak equivalence using hypothesis item 4.

\[ \square \]

## 5 Diagram Categories and Homotopy (Co)Limits

Cf. [HTT, A.3.3, A.3.5].

**Def. (3.7.5.1).** Let \( \mathcal{C} \) be a small \( \mathcal{S} \)-enriched category and \( \mathcal{A} \) a combinatorial \( \mathcal{S} \)-enriched model category, then a natural transformation \( \alpha : F \to G \) in \( \mathcal{A}^{\mathcal{C}} \) is called

- an **injective cofibration** if \( F(C) \to G(C) \) is a cofibration in \( \mathcal{A} \) for each \( C \).
- a **projective fibration** if \( F(C) \to G(C) \) is a fibration in \( \mathcal{A} \) for each \( C \).
- a **weak equivalence** if \( F(C) \to G(C) \) is a weak equivalence in \( \mathcal{A} \) for each \( C \).

**Prop. (3.7.5.2).** Let \( \mathcal{S} \) be an excellent model category and \( \mathcal{A} \) a combinatorial \( \mathcal{S} \)-enriched model category, \( \mathcal{C} \) a small \( \mathcal{S} \)-enriched category, then there are two model structures on \( \mathcal{A}^{\mathcal{C}} \):

- The **projective model category** determined by the projective cofibrations and weak equivalences,
- The **injective model category** determined by the injective cofibrations and weak equivalences.

**Proof:** Cf. [HTT, P868].

**Prop. (3.7.5.3).** Let \( \mathcal{C} \) be a model category and let

\[
\begin{array}{ccc}
A & \xrightarrow{j} & A_1 \\
\downarrow{i} & & \downarrow{} \\
A_0 & \longrightarrow & A_0 \amalg_A A_1
\end{array}
\]

be a pushout diagram, then it is a homotopy pushout diagram if either of the following is satisfied:

- \( j \) is a cofibration and \( A, A_0 \) are cofibrant.
- \( j \) is a cofibration and \( \mathcal{C} \) is left proper.

**Proof:**

\[ \square \]

## 6 Enriched and Monoidal Model Categories

**Def. (3.7.6.1)[Left Quillen Bifunctor].** Let \( \mathcal{A}, \mathcal{B}, \mathcal{C} \) be model categories, then a functor \( \mathcal{A} \times \mathcal{B} \to \mathcal{C} \) is called a **left Quillen bifunctor** if
• For any cofibrations \( i : A \rightarrow A' \in A, B \rightarrow B' \in B \), the induced map

\[
i \land j : F(A', B) \coprod_{F(A, B)} F(A, B') \rightarrow F(A', B')
\]

is a cofibration in \( 
\).

• \( F \) preserves small colimits separably in each variables.

**Def. (3.7.6.2) [Monoidal Model Category].** A monoidal model category is a monoidal category \( S \) equipped with a model structure that:

- The tensor product \( \otimes : S \times S \rightarrow S \) is a left Quillen bifunctor.
- The unit objects \( 1 \in S \) is cofibrant.
- The monoidal structure is closed.

**Def. (3.7.6.3) [Enriched Model Category].** Given a monoidal model category \( S \), an \( S \)-enriched model category is an \( S \)-enriched category \( A \) with a model structure satisfying:

- \( A \) is tensored and cotensored over \( S \).
- the tensor product \( A \times S \rightarrow S \) is a left Quillen bifunctor.

**Prop. (3.7.6.4).** The second condition in (3.7.6.3) is equivalent to the following: For a cofibration \( i : U \rightarrow V \) and a fibration \( p : X \rightarrow Y \), the induced map

\[
\text{Map}(V, X) \xrightarrow{(i^*, p_*)} \text{Map}(U, X) \times_{\text{Map}(U, Y)} \text{Map}(V, Y)
\]

is a fibration in \( S \), and trivial fibration if any of \( i, p \) is weak equivalence.

**Proof:** Use the adjunction relations to write it out.

**Def. (3.7.6.5) [Fibrant Enriched Categories].** Let \( A \) be a \( S \)-enriched category, the we denote \( A^\circ \) the subcategory of bifibrant objects of \( A \), which is also a \( S \)-enriched category.

**Prop. (3.7.6.6).** Let \( \mathcal{C}, \mathcal{D} \) be \( S \)-enriched model categories and

\[
F : \mathcal{C} \rightleftharpoons \mathcal{D} : G
\]

is a Quillen adjunction of underlying model categories. Assume every objects of \( \mathcal{C} \) is cofibrant and the maps \( \beta_{X, S} : S \otimes F(X) \rightarrow F(S \otimes X) \) is a weak equivalence for \( X \in \mathcal{C}, S \in S \) cofibrant, then the following are equivalent:

- \((F, G)\) is a Quillen equivalence.
- \( G \) determines a weak equivalence of the underlying \( S \)-enriched categories \( \mathcal{D}^\circ \rightarrow \mathcal{C}^\circ \).

**Proof:** Cf.[HTT, P853].

**Lemma (3.7.6.7).** Let \( S = \text{Set}_\Delta \), then the map \( \beta_{X, S} \) is a weak equivalence for every cofibrant object \( X \in \mathcal{C} \).

**Proof:** Cf.[HTT, P853].
Prop. (3.7.6.8). Let $\mathcal{C}, \mathcal{D}$ be simplicial model categories and $$ F : \mathcal{C} \rightleftarrows \mathcal{D} : G $$ is a Quillen equivalence, and every element of $\mathcal{C}$ is cofibrant, then $G$ induces an equivalence of $\infty$-categories $N(\mathcal{D}^\circ) \cong N(\mathcal{C}^\circ)$.  

Proof: This is because $G : \mathcal{D}^\circ \to \mathcal{C}^\circ$ is an equivalence of simplicial categories, by (3.7.6.6) and (3.7.6.7), and then (3.12.4.14) shows $N(G) : N(\mathcal{D}^\circ) \to N(\mathcal{C}^\circ)$ is an equivalence of $\infty$-categories. □

7 $S$-enriched Categories

Def. (3.7.7.1) [Homotopy Category]. Let $S$ be a monoidal model category, then there is a natural monoidal structure on the homotopy category $hS$ (3.7.1.14), and the functor $S \mapsto hS$ is monoidal, thus we can transfer from a category $\mathcal{C}$ enriched over $S$ to an $hS$-enriched category, called the homotopy category of $\mathcal{C}$.

Def. (3.7.7.2) [Weak Equivalences]. Let $S$ be a monoidal model category and $\mathcal{C}$ be the category of categories enriched over $S$, then a morphism in $\mathcal{C}$ is called a weak equivalence if it induced an isomorphism of their homotopy categories.

Def. (3.7.7.3) [Generating Cofibrations in $\mathcal{C}_S$]. Let $S$ be a monoidal model category, $A$ is an object of $S$, then we can denote $[1]_A$ the $S$-enriched category consists of objects $\{X, Y\}$ and that $\text{Hom}(X, X) = \text{Hom}(Y, Y) = 1_S, \text{Hom}(X, Y) = A, \text{Hom}(Y, X) = \emptyset$. And if $1_S$ is the initial object of $S$, then we denote $[1]_1$ by $[1]_S$. Also we denote $[0]_S$ the $S$-enriched category consisting of one element and the morphism space is $1_S$.

Let $[1]_S$ be the category consisting of two objects $\{X, Y\}$ that $\text{Hom}(Z_1, Z_2) = 1_S$ for any $Z_1, Z_2 \in S$.

Let $C_0$ be the class of morphisms in $\mathcal{C}_S$ consisting of

- $\emptyset \to [0]_S$.
- The induced map $[1]_S \to [1]_{S'}$ where $S \to S'$ ranges over a generating class of cofibrations of $S$.

Prop. (3.7.7.4) [Model Category on $\mathcal{C}_S$]. Let $S$ be a combinatorial monoidal model category that every object of $S$ is cofibrant and the collection of weak equivalences of $S$ is stable under filtered colimits, then there exists a left proper combinatorial model structure on $\mathcal{C}_S$ that

- The class of cofibrations in $\mathcal{C}_S$ is the smallest weakly saturated class generated by $C_0$ defined in (3.7.7.3),
- The weak equivalences are as defined in (3.7.7.2).

Proof: Cf. [HTT, P856]. □

Cor. (3.7.7.5). Let $$ f : S \rightleftarrows S' : g $$

be a Quillen adjunction between monoidal model categories satisfying conditions in (3.7.7.4), then they induces a Quillen adjunction $$ F : \mathcal{C}_S \rightleftarrows \mathcal{C}_{S'} : G $$

and this is a Quillen equivalence if $(f, g)$ is.
**Proof:**

**Def. (3.7.7.6) [Local Fibrations].** Let $\mathcal{C}$ be an $S$-enriched category where $S$ is a monoidal model category, then a morphism $f \in \mathcal{C}$ is called an **equivalence** if it maps to an isomorphism in $h\mathcal{C}$.

$\mathcal{C}$ is called **locally fibrant** if for any $X, Y \in \mathcal{C}$, the mapping space $\text{Map}(X, Y)$ is fibrant in $S$.

An $S$-enriched functor $F : \mathcal{C} \to \mathcal{C}'$ is called a **local fibration** if the following conditions are satisfied:

- for any $X, Y \in \mathcal{C}$, the induced map $\text{Map}(X, Y) \to \text{Map}(FX, FY)$ is a fibration in $S$.
- the induced map $h\mathcal{C} \to h\mathcal{C}'$ is a quasi-fibration of categories.

**Def. (3.7.7.7) [Invertibility Hypothesis].** We say a monoidal model category $S$ satisfies the **invertibility hypothesis** if: For any cofibrant morphism $[1]_S \to \mathcal{C}(3.7.7.3)$ of $S$-enriched categories, and maps to a morphism $f$ which is invertible in the homotopy category $h\mathcal{C}$, take the pushout:

$$
\begin{array}{ccc}
[1]_S & \xrightarrow{i} & \mathcal{C} \\
\downarrow & & \downarrow j \\
[1]_S \tilde{\gamma} & \to \mathcal{C}(f^{-1})
\end{array}
$$

then $j$ is a weak equivalence of $S$-enriched categories.(3.7.7.2).

**Def. (3.7.7.8) [Excellent Model Category].** An **excellent model category** is a monoidal model category $S$ that The monoidal structure is symmetric.

- $S$ is combinatorial,
- Every monomorphism in $S$ is a cofibration, and the collection of cofibrations is stable under products,
- The class of weak equivalences in $S$ is stable under filtered colimits,
- $S$ satisfies the invertibility condition(3.7.7.7)

**Lemma (3.7.7.9).** Let $T : S \to S'$ be a monoidal functor between monoidal model categories satisfies axioms besides invertibility hypothesis, that is also a left Quillen functor, then if $S'$ satisfies invertibility hypothesis, so does $S$.

**Proof:** Cf.[HTT, P862].

**Prop. (3.7.7.10) [Dwyer, Kan].** The category of simplicial sets is an excellent model category with the Kan model structure and the Cartesian monoidal structures.

**Proof:**

**Prop. (3.7.7.11) [Fibration and Local Fibration].** If $S$ is an excellent model category, then

- An $S$-enriched category $\mathcal{C}$ is a fibrant object in $\text{Cat}_S$ iff it is locally fibrant.(3.7.7.6).
- Let $F : \mathcal{C} \to \mathcal{D}$ be an $S$-enriched functor and $\mathcal{D}$ is fibrant in $\text{Cat}_S$, then $F$ is fibrant in $\text{Cat}_S$ iff it is a local fibration.

**Proof:** Cf.[HTT, P863].
8 Examples

Prop. (3.7.8.1) [Kan Model Structure]. The category of Simplicial sets $\text{Set}_{\Delta}$ is a combinatorial left and right proper model category with
- Weak homotopy equivalences as weak equivalences.
- Inclusions as cofibrations,
- Kan fibrations as fibrations,

Proof: Cf. [Jardine P62].

Prop. (3.7.8.2). $\text{Set}_{\Delta}$ is a monoidal model category w.r.t the Cartesian product and the Kan model structure.

Proof: □

Prop. (3.7.8.3) [$q$-Model Structure]. For a unital ring $R$, then the category $\text{Comp}_{n \geq 0} R$ has the structure of a model category with a morphism $f : M \rightarrow N$ being
- a weak equivalence if $H_n(f)$ is isomorphism for any $n$.
- a fibration if $M_n \rightarrow N_n$ is surjective for any $n \geq 1$.
- a cofibration if $M_n \rightarrow N_n$ is injective with projective cokernel for any $n \geq 0$.

Proof: [Model category and simplicial methods, P5] or [Homotopy Theories and Model Categories].

Prop. (3.7.8.4) [Serre-Quillen]. The category $\text{Top}$ can be given a Serre-Quillen model structure with
- Weak equivalences: weak homotopy equivalence,
- Fibrations: Serre fibrations,
- Cofibrations: Retracts of morphisms $X \rightarrow Y$ where $Y$ is obtained from $X$ by attaching cells. And this restricts to a model category on the category $\text{CGH}$ of compactly generated weak Hausdorff spaces.

Proof: See (3.9.6.28).

Prop. (3.7.8.5) [Hurewicz-Strøm]. The category $\text{Top}$ can be given a Hurewicz-Strøm model structure with
- Weak equivalences: homotopy equivalences.
- Cofibrations: closed Hurewicz cofibrations.
- Fibrations: Hurewitz fibrations.

Proof: See (3.9.6.31).

Prop. (3.7.8.6) [Derived Category Model]. If $\mathcal{A}$ is an Abelian category with enough injectives, then $K^+(\mathcal{A})$ is a model category with
- Weak equivalence: quasi-isomorphisms,
- Fibration: epimorphisms with ker in $K^+(\mathcal{I})$,
- Cofibration: monomorphisms.
Proof: □

Prop. (3.7.8.7) [Joyal]. The

Prop. (3.7.8.8) [Reedy Model Structures]. Cf. [HTT, A.2.9].
3.8 Topology II

1 Topological Groups

Def. (3.8.1.1). A topological group is a group object in the category of groups (3.1.1.61).

Prop. (3.8.1.2). If $U$ is a nbhd of 1 in a topological group, then there is a nbhd $V$ of 1 that $VV \subset U$.

Proof: Consider the map $G \times G \to G$ continuous, and it maps $(1, 1)$ to $1 \in U$, so the preimage of $U$ contains a nbhd of $(1, 1)$, thus some $V_1 \times V_2$, then choose $V = V_1 \cap V_2$. □

Prop. (3.8.1.3). Let $G$ be a connected topological group, then for any nbhd $U$ of $e$, $G = \bigcup_{n=1}^{\infty} (U \cup U^{-1})^n$. In particular, any open subgroup of $G$ equals $G$.

Proof: This is because the RHS is an open subgroup of $G$, so all its cosets in $G$ are also open, so it equals $G$ as $G$ is connected. □

Prop. (3.8.1.4) [Separating Axioms]. For a topological group $G$, the following are equivalent:

- $e$ is a closed pt.
- $G$ is $T_1$.
- $G$ is Hausdorff($T_2$).
- $G$ is regular.
- $G$ is completely regular

Proof:

Prop. (3.8.1.5). Hausdorff topological group is completely regular.

Proof: Use a sequence of neighbourhood of identity to construct a uniform metric on $G$. Then set $\phi(x) = \min\{1, 2\sigma(a, x)\}$. Cf. [Abstract Harmonic Analysis Ross §8.4] □

Prop. (3.8.1.6). For a compact subset $K$ and a nbhd $U$ of $e$ in a topological group, there exists a nbhd $V$ of $e$ that $xVx^{-1} \subset U$ for any $x \in K$.

Proof: For any $x$, there exists a nbhd $W_x$ of $x$ and a nbhd $V_x$ of $e$ that $txt^{-1} \in U$ for any $t \in W_x$ and $y \in V_x$. Let f.m. $W_{x_i}$ cover $K$, then $V = \cap V_{x_i}$ satisfies the condition. □

Prop. (3.8.1.7). A compact open nbhd of $e$ in a Hausdorff topological group contains an open subgroup of $G$.

Proof: Cf. [Etale Cohomology Fulei P147] □

Prop. (3.8.1.8) [Homogenous Space]. Let $G$ be a topological group and $H$ a closed subgroup. $G/H$ is the quotient space in the quotient topology (3.6.1.8), then it is Hausdorff.

Proof: If $x \neq y$, then consider a preimage $xy^{-1} \in G\setminus H$, then we can find some open subset $V$ that $VV \subset G\setminus H$ by (3.8.1.2), thus $x + \overline{V} \cap \overline{y} + \overline{V} = \emptyset$. Hence $G/H$ is Hausdorff. □
Group Actions

Prop. (3.8.1.9) [Quotient by Group Action is Open]. Let \( G \times X \to X \) be a group action, then the quotient map \( \pi : X \to X/G \) is open.

Proof: This is because the \( \pi^{-1}(\pi(U)) = \bigcup_{g \in G} gU \).

Def. (3.8.1.10) [Regular Action]. An regular action is an action \( \gamma : G \times X \to X \) that satisfies the following equivalent conditions:
- the graph of \( \gamma \) in \( X \times X \) is closed.
- The diagonal \( \Delta \subset X \times X \) is closed.
- \( X/G \) is Hausdorff.

Proof: \( 2 \iff 3 \) is clear, for \( 1 \), notice \( X/G \times X/G \simeq (X \times X)/(G \times G) \), and the inverse image of \( \Delta \) in \( X \times X \) is just the graph of \( \gamma \).

Def. (3.8.1.11) [Proper Action]. A proper action is an action \( \gamma : G \times X \to X \) that the graph map \( \Gamma : G \times X \to X \times X \) is a proper map.

Prop. (3.8.1.12) [Proper Action is Regular]. A proper action of a group \( G \) on a locally compact Hausdorff space \( X \) is a regular action.

Proof: This follows from (3.6.2.12).

Def. (3.8.1.13) [Proper Discontinuous Actions]. A group action is called proper discontinuous iff any elements \( x, y \in H \) there are nbhds \( U_x, U_y \) that \( \{ g \in G | g(U_x) \cap U_y \neq \emptyset \} \) is finite.

Def. (3.8.1.14) [Covering Space Action]. A covering space action is action of a topological group \( G \) on a topological space \( Y \) is called if for any \( y \in Y \), there is a nbhd \( U \) that \( g(U) \cap U = \emptyset \) if \( g \neq 1 \).

Prop. (3.8.1.15) [Characterization of Proper Actions]. Let \( \gamma : G \times X \to X \) be a group action that \( X \) is Hausdorff, then \( \gamma \) is a proper action iff any \( K \subset X \) compact, the set \( G_K = \{ g \in G | g(K) \cap K \neq \emptyset \} \) is compact.

Proof: Let \( \Gamma : G \times X \to X \times X \) be the graph.

1 \to 2: \( G_K = \pi_1(\Gamma^{-1}(K \times K)) \), thus it is compact.

2 \to 1: Let \( L \subset M \times M \) be compact, then \( L \subset \pi_1(L) \times \pi_2(L) \), and \( L \) is closed. Let \( K = \pi_1(L) \cup \pi_2(L) \), then \( \Gamma^{-1}(L) \subset \Gamma^{-1}(\pi_1(L) \times \pi_2(L)) \subset G_K \times K \), which is a closed subset of a compact set, so \( \Gamma^{-1}(L) \) is compact, and \( \Gamma \) is a proper map.

Prop. (3.8.1.16). If \( G \) is a compact topological group, then any group action \( \gamma : G \times X \to X \) on a Hausdorff space \( X \) is proper.

Prop. (3.8.1.17) [Orbit of Proper Maps]. Let \( \theta \) be a proper action of \( G \) on a Hausdorff space \( X \), then each orbit map \( \theta^{(p)} \) is proper. In particular, if \( X \) is locally compact, then the orbits are all closed (3.6.2.12).

Proof: For any compact subset \( K \subset X \), \( (\theta^{(p)})^{-1}(K) \) is closed by continuity and is contained in \( G_K \cup \{p\} \), thus is compact.
Prop.(3.8.1.18)[Properly Discontinuous Map is Proper]. If $G$ acts properly discontinuously on a topological space $H$, then for any compact subsets $K_1, K_2 \in H$, $\{g \in G | K_2 \cap g(K_1) \neq \emptyset \}$ is finite. In particular, if $H$ is Hausdorff, then it is a proper action.

Proof: Notice for any two points we can find nbhds that f.m. $g$ intersects these two nbhds, so we can use the compactness to find f.m. pair of nbhds to cover $K_2$, and then use these nbhds to cover $K_1$ and finite the proof. □

Prop.(3.8.1.19)[Proper Free Action is a Covering Space Action]. Let $G \times X \to X$ be a proper free action on a locally compact Hausdorff space, then it is a covering space action.

Proof: For any $p \in X$, choose a precompact nbhd $U$ of $x$, then $G_U$ is finite, then shrink $U$. □

Prop.(3.8.1.20)[Continuity]. Let a topological group $G$ acts freely and properly on a space $X$. If $G$ and $X \rtimes G$ are both connected, then $X$ is connected.

Proof: If $U,V$ are open subsets of $X$ that $U \cap V = \emptyset, U \cup V = X$, then $\pi(U), \pi(V)$ are open by (3.8.1.9). Now $\pi(U) \cap \pi(V) = \emptyset$, because otherwise there is a $G$-orbit of $X$ intersecting both $U$ and $V$, contradiction the fact $G$ is connected. Then $\pi(U) = \emptyset$ or $\pi(V) = \emptyset$, thus $U = \emptyset$ or $V = \emptyset$, and $X$ is connected. □

Def.(3.8.1.21)[Constructible Action]. An action of a topological group $G$ on a topological space $X$ is called constructible if its graph is constructible in $X \times X$ (3.8.3.10).

Prop.(3.8.1.22). Let $\gamma : G \times X \to X$ be an action

- $\gamma$ is constructible iff the diagonal $\Delta_{X/G} \subset X/G \times X/G$ is constructible.
- If $\gamma$ is constructible and $X$ is non-empty, then there is a $G$-invariant open subset $U \subset X$ that $G$ acts regularly.
- For a constructible action, each $G$-orbit is locally closed.

Proof: Cf.[Bernstein-Zelevinsky, P54]. □

Totally Disconnectedness

Prop.(3.8.1.23). A compact topological group is totally disconnected iff the intersection of all compact open nbhds of $e$ equals $\{e\}$.

Proof: If it is totally disconnected, then $\{1\}$ is closed, so $G$ is Hausdorff (3.8.1.4), so by (3.6.1.24), the assertion is true. Conversely, if the intersection of all compact open nbhds of $e$ equals $\{e\}$, then $\{1\}$ is closed because $G$ is a group. □


Proof: Cf.[Etale Cohomology Fulei P147]. □
2 Hausdorff Geometry

Def. (3.8.2.1). The **Hausdorff distance** for two subset \( Y_1, Y_2 \in X \) is the
\[
d^H_X(Y_1,Y_2) = \inf \{ \varepsilon | Y_2 \subset B(Y_1,\varepsilon), Y_1 \subset B(Y_2,\varepsilon) \}.
\]
The **Gromov-Hausdorff metric** for two metric space is
\[
d^{GH}(X_1,X_2) = \inf \{ d^H_Z(i_1(X_1),i_2(X_2)) \}
\]
where \( i_1, i_2 \) are isometry of \( X_1, X_2 \) into a metric space \( Z \).

This metric makes the set of all compact metric space into a complete Hausdorff space \( M\mathcal{ET} \).

Def. (3.8.2.2). A map from \( X \) to \( Y \) is called a \( \varepsilon \) **approximation** iff \( B(f(X),\varepsilon) = Y \) and \( |d(x,y) - d(f(x),f(y))| \leq \varepsilon \).

We have: if there is a \( \varepsilon \) approximation, then \( d^{GH}(X,Y) \leq 3\varepsilon \), and if \( d^{GH}(X,Y) \leq \varepsilon \), there is a \( 3\varepsilon \) approximation.

Prop. (3.8.2.3). The set of isometries of

3 Spaces from Algebraic Geometry

Noetherian Space

Def. (3.8.3.1) [Noetherian Spaces]. A **Noetherian space** is a space \( X \in \mathcal{Top} \) that any descending chain of closed subsets stabilizes. A **locally Noetherian space** is a space \( X \in \mathcal{Top} \) that every point has a nbhd \( U \) s.t. \( U \) is a Noetherian space.

Prop. (3.8.3.2). A Noetherian space is quasi-compact and all subsets of it in the induced topology is Noetherian hence quasi-compact.

Proof: Let \( T \subset X \), for a chain of closed subsets \( Z_i \cap T \) of \( T, Z_1, Z_1 \cap Z_2, \ldots \) stabilize in \( X \), hence the chain stabilize in \( T \). \( \square \)

Prop. (3.8.3.3). If \( X \) can be covered by f.m. Noetherian subspaces, then \( X \) is Noetherian.

Proof: \( \square \)

Prop. (3.8.3.4) [Noetherian Space F.M. Irreducible Components]. A Noetherian space has only f.m. irreducible component, hence it has only f.m. connected components.

Proof: Let \( C \) be the family of closed subset that has infinitely many component, then there is a minimal object, but it is not irreducible, one of the component has infinitely many components and be smaller. \( \square \)

Quasi-Separated

Def. (3.8.3.5) [Quasi-Separated]. A space \( X \) is called **quasi-separated** if the diagonal morphism is quasi-compact(3.6.2.2). If \( X \) has a basis consisting of quasi-compact open subsets, then this is equivalent to any intersection of two quasi-compact open subsets is quasi-separated open.
Specialization & Generalization

Def.(3.8.3.6)[Specializations and Generalizations]. Let $X \in \text{Top}$ then $x$ is said to be a specialization of $y$ if $x \in \{y\}$. And in this case $y$ is said to be a generalization of $x$.

And they are called immediate specializations/generalizations if there are no other points $z \in X$ s.t. $y \to z \to x$.

Def.(3.8.3.7)[Going Up and Down]. A map $f$ of spaces is said to satisfy the going-up property iff specialization lifts along $f$. It is said to satisfy the going-down property iff generalization lifts along $f$.

Prop.(3.8.3.8). A closed map satisfies going-up.

Proof: If $y \to y'$, $f(x) = y$, consider $f(\{x\})$, it is closed and contains $y$, so it contains $y'$, thus the result. \qed

Constructible Set

Def.(3.8.3.9)[Retrocompact Subset]. A subset of $X$ is called retrocompact if the inclusion map is quasi-compact (3.6.2.2).

Def.(3.8.3.10)[Constructible Subset]. A subset of $X$ is called constructible if it is a finite union of sets of the form $U \cap V^c$ where $U,V$ are open and retrocompact in $X$. In the case when $X$ is Noetherian, by (3.8.3.2), all subsets are retrocompact hence constructible sets are just union of locally closed subsets of $X$.

A set of $X$ is called locally constructible if locally it is constructible. If $X$ is quasi-compact, then a locally constructible set is just a constructible set.

Prop.(3.8.3.11). Constructible subsets of $X$ forms a Boolean algebra.

Proof: Cf.[Sta]005H. \qed

Prop.(3.8.3.12)[Constructible and Subsets].

- If $U$ is open in $X$, then for any $E$ constructible in $X$, $E \cap U$ is constructible in $U$.
- If $U$ is retrocompact open and $E$ is constructible in $U$, then $E$ is constructible in $X$.

Proof: Easy. \qed

Prop.(3.8.3.13). Any constructible subsets of $X$ is retrocompact.

Proof: It suffices to prove $U_i \cap V_i^c \cap W$ is quasi-compact for $W$ quasi-compact, but this is because it is a closed subspace of the quasi-compact subspace $U_i \cap W$. \qed

Cor.(3.8.3.14). An open subset of $X$ is constructible iff it is retrocompact, a closed subset of $X$ is constructible iff its complement is retrocompact.((3.8.3.11) used).

Def.(3.8.3.15)[Constructible topology]. The constructible topology $X_{cons}$ on a quasi-compact space $X$ is generated by the open subsets $U, U^c$, where $U$ is a quasi-compact open.

Notice that the space is quasi-compact, so the constructible topology is the coarsest topology that every constructible subset of $X$ is both open and closed.
Prop. (3.8.3.16). Let $X$ be quasi-compact and quasi-separated, then any constructible subset of $X$ is quasi-compact. In particular, if $Y$ is closed in $X$, then $Y$ is constructible iff it is quasi-compact.

Proof: For $Y = \bigcup_{i=1}^{n} (U_i - V_i)$, with $U_i, V_j$ quasi-compact open in $X$, then $U_i - V_i$ is closed in $U_i$ thus quasi-compact, and then $Y$ is quasi-compact. \hfill \Box

Prop. (3.8.3.17). Let $E$ be a constructible subset of a space $X$, if $E$ is dense in then $E$ contains some open dense subset of its closure.

Proof: Let $Y = \bigcup_{i=1}^{k} Y_i$ where $Y_i$ are locally closed. Denote $Z_i = Y_i \setminus Y_i$, $Z = \bigcup Z_i$, $W = Y \setminus Z$. Then $W \subset Y$, and we show that $W$ is open dense in $Y$: As $Y_i$ are locally closed, $Y_i$ is open in $\overline{Y_i}$, thus $Z_i$ is closed, and $Z$ is closed, so $W$ is open in $Y$. To show $W$ is dense in $Y$: If some open subset $U$ of $Y$ satisfies $U \cup Z_i$, then $U$ cannot be contained in any $Z_i$, so we can inductively show $U \setminus Z_1, U \setminus (Z_1 \cup Z_2), \ldots$ are non-empty, which is a contradiction. \hfill \Box

Irreducible

Def. (3.8.3.18) [Irreducible Space]. A space is called irreducible iff there are no two nonempty nonintersecting open subsets. Thus an open subset of an irreducible set is dense and irreducible.

Prop. (3.8.3.19). If $Y$ is irreducible in $X$, then $\overline{Y}$ is also irreducible.

Proof: Any two nonempty open sets of $\overline{Y}$ must intersect $Y$ thus must intersect. \hfill \Box

Prop. (3.8.3.20). If $X \in \mathcal{Top}$ and $U \subset X$ is open, then $Y \mapsto \overline{Y}$ is a order preserving bijection between irreducible closed subspaces of $U$ and irreducible closed subspaces of $X$ meeting $U$.

Jacobson Space

Def. (3.8.3.21). Let $X$ be a space and $X_0$ the set of closed pts of $X$, then $X$ is called Jacobson iff $Z \cap X_0 = Z$ for every closed subset $Z$ of $X$. This is equivalent to every non-empty locally closed subset of $X$ contains a closed pt.

Thus there is a correspondence between closed subsets of $X_0$ and closed subsets of $X$, so they have the same Krull dimension.

Prop. (3.8.3.22). Being Jacobson is local. And for an open covering $U_i$ of $X$, $X_0 = \bigcup U_i$.

Proof: Firstly, if $X = \bigcup U_i$ where $U_i$ are Jacobson, $X_0 \cap U_i = U_i$. One direction is trivial, for the other, let $x$ be closed in $U_i$, then consider $\{x\} \cap U_j$. If $x \notin U_j$, then $x$ is closed in $U_j$, consider $T = \{x\} \cup (U_j - U_i \cap U_j)$, then $T$ is closed in $U_j$, so by hypothesis, closed pts of $U_j$ are dense in $T$, so $x$ must be closed in $U_j$, so $x$ is closed in $X$. Now clearly $X$ is Jacobson.

Conversely, if $X$ is Jacobson, for a closed subset $Z$ of $U_i$, $X_0 \cap Z$ is dense in $Z$, so $X_0 \cap Z$ is dense in $Z$, then clearly $U_i$ is Jacobson. \hfill \Box

Cor. (3.8.3.23). If $X$ is Jacobson, then any locally constructible sets of $X$ is Jacobson. And its closed pts are closed in $X$.

Proof: By the proposition, we only have to prove for constructible sets. For $T = \bigcup T_i$ where $T_i$ is locally closed, then a locally closed set in $T$ has a non-empty intersection $T \cap T_i$ which is also locally closed for some $i$.

Hence is has a closed pt in $X$ hence in $T$, so $T$ is Jacobson. The second assertion is implicit in the proof. \hfill \Box
**Prop. (3.8.3.24).** If $X$ is Jacobson, then an open set $U$ of $X$ is compact iff $U \cap X_0$ is compact, hence an open set $U$ is retrocompact iff $U \cap X_0$ is retrocompact.

Hence the constructible sets of $X$ correspond to the constructible sets of $X_0$. And irreducible closed subsets correspond to irreducible subsets of $X_0$.

**Krull Dimension**

**Def. (3.8.3.25).** The Krull dimension of a topological space is the length of the longest chain of closed irreducible subsets.

The local dimension $\dim_x(X) = \min\{\dim U | x \in U \subset X \text{ open in } X\}$.

**Prop. (3.8.3.26).** If $Y \subset X$, then $\dim Y \leq \dim X$, because the closure of any chain of $Y$ is a chain of $X$ by (3.8.3.19).

For an open covering $\{U_i\}$ of $X$, $\dim X = \sup \dim U_i$, because for any chain of closed irreducible subsets, if $U_i$ intersects the minimal one, then $\dim U_i = \text{length of this chain}$.

**Prop. (3.8.3.27).** $\dim X = \sup \dim_x(X)$.

**Proof:** The right is smaller than the left by (3.8.3.26), and for any chain $Z_0 \subset Z_1 \subset \ldots \subset Z_n$ of irreducible closed subset of $X$, if I choose a point $x \in Z_0$, then $\dim_x(X) \geq n$. □

**Prop. (3.8.3.28).** In case $X = \text{Spec } A$ for a Noetherian ring $A$, $\dim X = \sup \dim A_p$, because $A$ is of finite ?

**Def. (3.8.3.29) [Codimensions].** Let $X \in \text{Top}$ and $Y \subset X$ be an irreducible closed subspace, then the codimension of $Y$ in $X$ is defined to be the supremum of lengths $e$ of chains $Y = Y_0 \subset Y_1 \subset \ldots \subset Y_e = X$, denoted by $\text{codim}(Y, X)$.

**Sober Spaces**

**Def. (3.8.3.30) [Sober Spaces].** A space $X$ is called sober if every irreducible closed subset has a unique generic point.

**Prop. (3.8.3.31).** A sober space is $T_1$. Conversely, a finite $T_0$ space is sober.

**Proof:** The first assertion is because if $x \in \{y\}$ and $y \in \{x\}$, then $\{x\} = \{y\}$, and this irreducible closed subset has two generic point, contradiction.

If the space is finite, then for a closed irreducible subset $T = \{x_1, \ldots, x_n\}$, $T = \cup \{x_i\}$, as it is irreducible, $T = \{x_i\}$ for some $x_i$, and $i$ is unique as it is $T_1$, so $X$ is sober. □

**Prop. (3.8.3.32) [Soberization].** There is a left adjoint $t$ to the forgetful functor from the Sober spaces. $t(X)$ consists of irreducible closed subsets of $X$, and use $t(Y)$ for $Y$ closed as closed subsets. For a map $f : X \to Z$ to a sober space $Z$, the extension maps the generic point of an irreducible $Y$ to the generic point of the closure of $f(Y)$.

**Def. (3.8.3.33) [Zariski Space].** A Noetherian Sober space is called a Zariski space.
Catenary spaces and Dimension Functions

**Def. (3.8.3.34) [Catenary Space].** A space $X$ is called **catenary** iff for any inclusion of irreducible closed subsets of $X$, their codimension is finite and every maximal chain of irreducible closed subsets has the same dimension. This is equivalent to $\text{codim}(X,Y) + \text{codim}(Y,Z) = \text{codim}(X,Z)$.

**Prop. (3.8.3.35).** Catenary is a local property, by (3.8.3.20).

**Def. (3.8.3.36) [Dimension Function].** For $X \in \mathcal{T}_\text{op}$, consider the specialization relation (3.8.3.6), a **dimension function** is a function $\delta : |X| \to \mathbb{Z}$ that

- if $y$ is a specialization of $x$ in $X$, then $\delta(y) < \delta(x)$.
- if it is a direct specialization, then $\delta(y) = \delta(x) - 1$.

The dimension function is usually considered only when the space is sober.

**Prop. (3.8.3.37).** Let $X \in \mathcal{T}_\text{op}$ be sober and catenary with a catenary function, then $X$ is catenary, and if $x$ is a specialization of $x$ in $X$, then

$$\delta(x) - \delta(y) = \text{codim} \left( \overline{\{y\}}, \overline{\{x\}} \right).$$

**Proof:** This is clear from the definitions (3.8.3.29).

**Prop. (3.8.3.38).** If $X \in \mathcal{T}_\text{op}$ be locally Noetherian and sober, and $\delta, \delta'$ are two dimension functions on $X$, then $\delta - \delta'$ is locally constant on $X$.

**Proof:** We may assume $X$ is Noetherian, so it has only f.m. irreducible components by (3.8.3.4), then $\delta - \delta'$ is locally constant on the $X$ minus the irreducible components not passing through $x$ by (3.8.3.37).

**Prop. (3.8.3.39) [Catenary and Sober].** Let $X \in \mathcal{T}_\text{op}$ be locally Noetherian, sober, then $X$ is catenary iff any point $x \in X$ has a nbhd $U$ which has a dimension function.

**Proof:** Cf. [Sta]02IC. The other direction follows from (3.8.3.37) and (3.8.3.35).

Sober Spaces

**Def. (3.8.3.40) [Sober Spaces].** A space $X$ is called **sober** if every irreducible closed subset has a unique generic point.

**Prop. (3.8.3.41).** A sober space is $T_1$. Conversely, a finite $T_0$ space is sober.

**Proof:** The first assertion is because if $x \in \overline{\{y\}}$ and $y \in \overline{\{x\}}$, then $\overline{\{x\}} = \overline{\{y\}}$, and this irreducible closed subset has two generic point, contradiction.

**Prop. (3.8.3.42) [Catenary and Sober].** Let $X \in \mathcal{T}_\text{op}$ be locally Noetherian, sober and catenary, then any point $x \in X$ has a nbhd $U$ which has a dimension function.

**Proof:** Cf. [Sta]02IC.
4 Spectral Spaces

References are [Sta]5.23 and [Adic Spaces].

**Def. (3.8.4.1) [Spectral Space]**. A space is called spectral iff it is quasi-compact, quasi-separated(3.8.3.5), sober and the quasi-compact opens form a basis for the topology.

A space is called locally spectral iff it has an open covering by spectral spaces.

A morphism \( f : X \to Y \) between locally spectral spaces is called spectral if for any open spectral spaces \( U \subset f^{-1}(V) \), \( f : U \to V \) is quasi-compact.

**Prop. (3.8.4.2) [Connected Components]**. Let \( X \) be a spectral space, then any connected subset of \( X \) is an intersection of clopen subsets.

**Proof**: Let \( x \in X \) and \( S \) be the intersection of all clopen subsets of \( X \) containing \( x \), then it suffices to show \( S \) is connected. Suppose \( S = B \amalg C \) with \( B, C \) closed, then \( B, C \) are compact, thus there exist quasi-compact opens \( U, V \subset X \) that \( B = U \cap S, C = V \cap S \). Then \( U \cap V \cap S = \emptyset \). Now \( U \cap V \) is quasi-compact also, so there exists some clopen \( Z_\alpha \) containing \( x \) that \( Z_\alpha \cap U \cap V = \emptyset \).

Similarly, there exists some clopen \( Z_\beta \) containing \( x \) that \( Z_\beta \subset U \cup V \). Then \( Z_\gamma = Z_\alpha \cap Z_\beta \) is clopen and contained in \( U \Delta V \). Then both \( Z_\gamma \cap U \) and \( Z_\gamma \cap V \) is clopen, so \( U = \emptyset \) or \( V = \emptyset \).

**Cor. (3.8.4.3)**. Let \( X \) be a spectral space, then for a subset \( T \) of \( X \), \( T \) is an intersection of clopen subsets of \( X \) iff \( T \) is closed in \( X \) and is a union of connected components of \( X \).

**Proof**: If \( T \) is an intersection of clopen subsets, then \( T \) is clearly a union of connected components of \( X \). Conversely, if \( T \) is a union of connected components of \( X \), if \( x \notin T \), let \( C \) be a connected components containing \( x \). Then \( C \) is an intersection of clopen subsets, by (3.8.4.2). These subsets are closed under finite intersections, so by the compactness of \( T \), there is a clopen subset containing \( T \) but not \( x \), so we are done.

**Constructible Topology**

**Lemma (3.8.4.4)**. If \( X \) is a finite \( T_0 \) space, then it is spectral and every subset of \( X \) is constructible.

**Proof**: Cf.[Adic Space Morel, P26].

**Prop. (3.8.4.5)**. If \( X \) is a spectral space, then the constructible topology(3.8.3.15) is Hausdorff, totally disconnected and quasi-compact.

**Proof**: The space is sober hence \( T_0(3.8.3.41) \), and then the constructible topology is Hausdorff and totally disconnected.

To show quasi-compactness, it suffices to show that the family \( C \) of quasi-compact open and complement quasi-compact open subsets has the finite intersection property(3.6.2.3). Notice elements in \( C \) are all quasi-compact. Now if there is a family that has the finite intersection property by has intersection 0, by Zorn’s lemma, there is a maximal one of them, \( B \). Let \( Z \) be the intersection of all the closed subsets in \( B \), then it is non-empty as \( X \) is quasi-compact. And we claim \( Z \) is irreducible: otherwise \( Z = Z_1 \cup Z_2 \), thus there are quasi-compact open sets \( U_1, U_2 \) that \( U_1 \cap Z_1 \neq \emptyset, U_1 \cap Z_2 = \emptyset, U_2 \cap Z_2 \neq \emptyset, U_2 \cap Z_1 = \emptyset \). then let \( B_i = X - U_i \), then \( B_1, B_2 \) cannot by added to \( B \) by maximality, so there is a finite intersection \( T_1, T_2 \) that \( B_1 \cap T_1 = 0 \). But then \( Z \cap T_1 \cap T_2 = 0 \), but \( Z \) is an intersection of closed subsets, thus some finite intersection of closed subsets in \( B \) will \( \cap T_1 \cap T_2 = 0 \), contradiction.

So now \( Z \) is irreducible, but then for every element \( B \in B \), \( Z \cap B \) contains the generic point of \( Z \), thus the intersection of \( B \) is not empty, contradiction.
Cor. (3.8.4.6). Let $X$ be a spectral space, then
- The constructible topology is finer than the original topology.
- A subset $X$ is constructible iff it is clopen in the constructible topology of $X$.
- If $U$ is open in $X$, then the constructible topology induces the constructible topology on $U$.

Proof:
1: Every open subset of $X$ is a union of its quasi-compact open subsets, so it is open in the constructible topology.
2: Clearly constructible subset is clopen in the constructible topology. Conversely, if $Y$ is clopen, then $Y$ is a union of constructible subsets, but also it is quasi-compact, so it is a finite union of constructible subsets, thus constructible.

Prop. (3.8.4.7). If $E \subset X$ is closed in the constructible topology, then it is a spectral space with the induced topology, and the inclusion map is spectral.

Proof:  Cf. [Mor19] P34.

Prop. (3.8.4.8). For a set $E$ closed in the constructible topology in a spectral space,
- every point of $\overline{E}$ is a specialization of elements in $E$. Thus if $E$ is stable under specialization, then it is closed.
- If $E$ is open in the constructible topology and stable under generalization, then it is open.

Proof:  Cf. [Sta]0903.

Prop. (3.8.4.9). For a map between spectral spaces $f : X \to Y$, the following are equivalent:
- $f$ is spectral.
- $f$ is quasi-compact.
- $f : X_{cons} \to Y_{cons}$ is continuous.

And if this is true, then $f : X_{cons} \to Y_{cons}$ is proper.

Proof:  $1 \to 2 \to 3$ is trivial, an open subset of $X$ is quasi-compact iff it is clopen in the constructible topology (3.8.4.6), so $3 \to 2$. For $2 \to 1$, notice that if $U \subset f^{-1}(V)$ are open spectrals, and $W \subset U$ is quasi-compact open, then $f^{-1}W \cap U$ is quasi-compact open, because $X$ is quasi-separated.

Finally, $f$ is proper because $X_{cons}, Y_{cons}$ is compact Hausdorff (3.8.4.5), then use (3.6.2.10).

Criterion of Spectralness

Lemma (3.8.4.10). Let $X$ be a quasi-compact $T_0$ space that is has a subbasis consisting of quasi-compact open subsets that is stable under finite intersections. Let $X'$ be the topology generated by the quasi-compact open subsets and their complements, then the following are equivalent:
- $X$ is spectral.
- $X'$ is compact Hausdorff, and its topology has a basis consisting of open and closed subsets.
- $X'$ is quasi-compact.

Proof:  Cf. [Adic Space Morel P30].
Prop.(3.8.4.11) [Hochster’s Criterion of Spectrality]. Let $X' = (X_0, T')$ be a quasi-compact topological space, and let $\mathcal{U}$ be the family of clopen subsets of $T'$, let $T$ be the topology generated by $\mathcal{U}$, let $X = (X_0, T)$.

Then if $X$ is $T_0$, then it is spectral, and every element of $\mathcal{U}$ is quasi-compact open in $X$, and $X' = X_{cons}$.

Proof: Cf.[Adic Space Morel, P29]. □

Prop.(3.8.4.12) [Spectral and Inverse Limit]. A space is spectral iff it is a direct limit of finite sober($T_{1}(3.8.3.41)$) spaces.

Proof: Cf.[Sta]09XX. □

Prop.(3.8.4.13) [Spec and Spectral Space]. A spectral space is exactly the underlying space of spectrum of some ring.

Proof: The spectrum of a ring is qc: if $\cup D(f_i) = \text{Spec} A$, then $(f_i) = (1)$, so f.m. of them generate (1). And similarly it is quasi-separable and $D(f) = \text{Spec} A_f$ is quasi-compact. For the other direction, Cf.[M. Hochster. Prime ideal structure in commutative rings, Thm6]?.

Cor.(3.8.4.14). Every quasi-compact irreducible scheme is homeomorphic to an affine scheme.

Cor.(3.8.4.15) [Characterization of Spectral Spaces]. The following are equivalent for a topological space $T$:

1. $T \cong \text{Spec} R$ for some ring $R$.
2. $T \cong \varprojlim T_i$ where $\{T_i\}$ is an inverse system of finite $T_0$ spaces.
3. $T$ is spectral.

Proof: This follows from (3.8.4.13) and (3.8.4.12). □

w-localness

Def.(3.8.4.16) [pro-Zariski Localization]. A map of spectral spaces $f : W \to V$ is called a Zariski localization if $W = \coprod U_i$ where $U_i \to V$ is a quasi-compact open immersion. A pro-Zariski localization is a cofiltered limit of Zariski localizations of $V$.

Def.(3.8.4.17) [w-Local]. A spectral space is called w-local if the set of closed pts of $X$ is closed and any point of $X$ specializes to a unique closed pt. A morphism of w-local spaces are called w-local if it is spectral and maps closed pts to closed pts.

Prop.(3.8.4.18). If $X$ is w-local and $Y \subset X$ is a closed subset, then $Y$ is also w-local.

Proof: $Y$ is spectral by (3.8.4.7). $Y_0$ is closed because $Y_0 = Y \cap X_0$. And the second assertion is also trivial. □

Prop.(3.8.4.19). Let $X$ be a spectral space and $T$ profinite, then $Y = X \times_{\pi_0(X)} T$ is also spectral and $T = \pi_0(Y)$. If moreover $X$ is w-local, then $Y$ is also w-local and $Y \to X$ is w-local.

Proof: Cf.[Sta]096C. □
Def. (3.8.4.20) [Localization Along a Closed Set]. Given a closed set \( Z \) of a spectral set \( X \), the pro-open subset of \( X \) consisting of all points that specializes to a point of \( Z \) is called the localization of \( X \) along \( Z \). And \( X \) is called local along \( Z \) if \( X_0 \subset Z \).

Prop. (3.8.4.21). A spectral space that is local along a closed w-local subset \( Z \subset X \) with \( \pi_0(Z) \cong \pi_0(X) \), is also w-local.

Proof: \( X_0 = Z_0 \) is clearly closed, and if a pt \( x \) of \( X \) specializes to two closed pts of \( Z \), then the \( \pi_0 \) map is not injective, contradiction. \( \square \)
3.9 Algebraic Topology I: Homotopies

Main references are [Hat02], [AGP02], [同调论, 姜伯驹], [May99], [https://ncatlab.org/nlab/show/Introduction+to+Homotopy+Theory#HomotopyGroupsOftopologicalSpaces].

Notations (3.9.0.1).
- Use notations defined in Topology I.
- All spaces are assumed to be compactly generated, and products and mapping spaces are assumed to be compact generated versions.

1 Homotopy Types

Def. (3.9.1.1) [Retraction]. A retraction of a space $X$ to a subspace $A$ is a map $r : X \to A$ that $r|_A = \text{id}_A$.

Def. (3.9.1.2) [Homotopy]. A homotopy $f_t : X \to Y$ is a family of maps $f_t$ for every $t \in I$ that $f : X \times I \to Y$ is continuous. For two homotopies $F : X \times I \to Y$ and $F' : X \times I \to Y$ s.t. $F_1 = F'_0$, we can define the composite homotopy $F' \cdot F : X \times I \to Y$.

Two maps $f_0, f_1 : X \to Y$ are called homotopic if there is a homotopy $f_t : X \to Y$ connecting them. Homotopy relations are denoted by $f_0 \simeq f_1$.

Let $A$ be a subspace of $X$, then a homotopy relative to $A$ is a homotopy $f_t : X \to Y$ whose restriction to $A$ is fixed.

Let $E_1, E_2$ be spaces over $B$, then maps $f_0, f_1 : E_1 \to E_2$ over $B$ are called fiber homotopic if there is a homotopy $f_t : E_1 \to Y$ connecting them such that each $f_t$ are maps over $B$. Homotopy relations over $B$ are denoted by $f_0 \simeq_B f_1$.

Def. (3.9.1.3) [Homotopy Equivalences]. A map $f : X \to Y$ is called a homotopy equivalence if there is a map $g : Y \to X$ that $f \circ g \simeq \text{id}$ and $g \circ f \simeq \text{id}$.

A space having the homotopy type of a point is called contractible.

A map $f : X \to Y$ over $B$ is called a fiber homotopy equivalence if there is a map $g : Y \to X$ over $B$ that $f \circ g \simeq_B \text{id}$ and $g \circ f \simeq_B \text{id}$.

Def. (3.9.1.4) [Deformation Retraction]. A deformation retraction of a space $X$ onto a subspace $A$ is a homotopy $f_t : X \to X, t \in I$ that $f_0 = \text{id}, f_1(X) = A$ and $f_t|_A = \text{id}_A$ for all $t$.

Prop. (3.9.1.5). A map $X \to Y$ is a homotopy equivalence iff the mapping cylinder deformation retracts onto $X$.

Proof: ?

Def. (3.9.1.6) [Excisive Triads]. A triad of spaces is a triple $(X; A, B)$ s.t. $A \subset X, B \subset X$. An excisive triad is a triad $(X; A, B)$ s.t. $A^o \cup B^o = X$.

Relative Spaces

Def. (3.9.1.7) [Relative Spaces]. The category $\mathcal{G}_\text{rel}$ is the category of pairs $(X, A)$ where $A \subset X \in \mathcal{G}$, and morphisms in $\mathcal{G}_\text{rel}$ are equivariant maps.

Def. (3.9.1.8) [Smash Products]. smash products in $\mathcal{G}_\text{rel}$ are defined to be $(X, A) \land (Y, B) = (X \times Y, (X, A) \vee (Y, B))$, where $(X, A) \cup (Y, B) = X \times B \cup A \times Y \subset X \times Y$. 

Show/Introduction+to+Homotopy+Theory#HomotopyGroupsOftopologicalSpaces
Def. (3.9.1.9) [Cones and Suspensions]. For \((X, A) \in \mathcal{Top}^{\text{rel}}\), the cone over \((X, A)\) is defined to be \(C(X, A) = (X, A) \wedge (I, \{1\})\). The suspension of \((X, A)\) is defined to be \(\Sigma(X, A) = (X, A) \wedge S^1\).

Prop. (3.9.1.10) [\(\mathcal{CG}^{\text{rel}}\) is Closed]. For \((X, A), (Y, B), (Z, C) \in \mathcal{CG}^{\text{rel}}\), by (3.6.3.15) there is a homeomorphism
\[
\text{Map}((X, A) \wedge (Y, B), (Z, C)) \cong \text{Map}((X, A), \text{Map}(Y, B), (Z, C)).
\]
In particular, \(\mathcal{CG}^{\text{rel}}\) is a closed symmetric monoidal category.

Def. (3.9.1.11) [Pointed Spaces]. The category \(\mathcal{CG}^{\text{pt}}\) is the subcategory of \(\mathcal{CG}^{\text{rel}}\) consisting of pairs \((X, A)\) s.t. \(A \cong \text{pt}\). It is stable under finite products.

We can define similarly homotopies of maps between pointed spaces, and denote \((X, Y)\) the homotopy classes of maps from \(X\) to \(Y\).

Def. (3.9.1.12) [Smash Products]. For \(X, Y \in \mathcal{CG}^{\text{pt}}\), the smash product \(X \wedge Y\) is defined to be \(X \wedge Y = X \times Y / X \wedge Y\), where \(X \vee Y = X \coprod Y\), called the wedge sum of \(X\) and \(Y\). Similar to (3.9.1.9), we can define cones and suspensions of pointed spaces.

Then the smash product and wedge sums are commutative and associative, and they satisfy
\[
(X \vee Y) \wedge Z = X \wedge Z \vee Z \wedge Z.
\]
Because of (3.9.1.14), the smash product and wedge sums are also denoted by \(X \otimes Y\) and \(X \oplus Y\).

Proof: For the identities, use the fact product commutes with colimits (3.6.3.16).

Prop. (3.9.1.13) [Smash Products, and Homotopy]. Suspensions preserves homotopy, as \(\Sigma(X \wedge I) = X \wedge I \wedge S^1 \cong (X \wedge S^1) \wedge I\).

Prop. (3.9.1.14) [\(\mathcal{CG}^{\text{pt}}\) is Closed]. For \(X, Y, Z \in \mathcal{CG}^{\text{pt}}\), by (3.9.1.10), there is a bijection
\[
\text{Map}(X \wedge Y, Z) \cong \text{Map}(X, \text{Map}(Y, Z)).
\]
In particular, \(\mathcal{CG}^{\text{pt}}\) is a closed symmetric monoidal category.

Def. (3.9.1.15) [Well-Pointed Spaces]. A pointed space \((X, *) \in \mathcal{CG}^{\text{pt}}\) is called a well-pointed space if \(* \to X\) is a cofibration. The category of well-pointed spaces is denoted by \(\mathcal{CG}^{\text{well-pt}}\).

Def. (3.9.1.16) [Augmentation]. There is a functor \(\mathcal{CG} \to \mathcal{CG}^{\text{well-pt}} : X \mapsto X_+ = (X \coprod \text{pt}, \text{pt})\).

Prop. (3.9.1.17). The cone construction
\[
\mathcal{Top}^{\text{rel}} \to \mathcal{Top} : (X, A) \mapsto C(A \to X)
\]
preserves homotopy equivalence.

Prop. (3.9.1.18) [Path Spaces and Loop Spaces]. For \(X \in \mathcal{CG}^{\text{pt}}\), define the path space \(P(X) = \text{Map}((I, \{0\}), X)\), and define the loop space \(\Omega(X) = \text{Map}(S^1, X)\).

Then by (3.9.1.14), there are homeomorphism of spaces
\[
\text{Map}(\Sigma(X), Y) \cong \text{Map}(X, \Omega(Y)).
\]
Thus also
\[
\langle \Sigma(X), Y \rangle \cong \langle X, \Omega(Y) \rangle.
\]

Def. (3.9.1.19) [Weak Products]. For \(\{X_\alpha\}_\Sigma \in \mathcal{CG}^{\text{pt}}\), define the weak product \(\prod' X_\alpha\) as
\[
\prod' X_\alpha = \lim_{S \subset \Sigma, \#S < \infty} \bigvee_{i \in S} X_i
\]
with base point \(\prod *\).
2 Isotopies

Prop.(3.9.2.1)[Alexander’s Trick]. If \( f, g : \mathbb{D}^n \to \mathbb{D}^n \) be two self-homeomorphisms that there is an isotopy \( F : \mathbb{D}^n \times I \to \mathbb{D}^n \) between \( f|_{\partial \mathbb{D}^n} \) and \( g|_{\partial \mathbb{D}^n} \), then there exists an isotopy between \( f \) and \( g \) extending \( F \).

Proof: Firstly, if \( g = \text{id}_{\mathbb{D}^n} \) and \( f \) fixes every points on the boundary, then an isotopy connecting \( f \) to the identity is given by

\[
J(x, t) = \begin{cases} 
  tf(x/t), & 0 \leq ||x|| < t \\
  x, & t \leq ||x|| \leq 1
\end{cases}
\]

In general, isotopy \( g^{-1}F : \mathbb{D}^n \times I \to \mathbb{D}^n \) between \( g^{-1}f|_{\partial \mathbb{D}^n} \) and \( \text{id}_{\mathbb{D}^n} \) can be extended to an isotopy from \( F' : \text{Cone}(g^{-1}f|_{\partial \mathbb{D}^n}) \) to \( \text{id}_{\mathbb{D}^n} \). Then \( \text{Cone}(g^{-1}f|_{\partial \mathbb{D}^n}) \) and \( g^{-1}f \) are identical on \( \partial \mathbb{D}^n \), so by the argument above, they are isotopic. Then \( g^{-1}f \cong \text{id}_{\mathbb{D}^n} \), which gives an isotopy between \( f \) and \( g \). □

Prop.(3.9.2.2). Any orientation-preserving self-homeomorphism \( f \) of \( S^d \) is isotopic to \( \text{id}_{S^d} \).

Proof: By the decomposition of \( S^d \) into two hemispheres and using the annulus theorem (3.6.11.2), we see we can isotopy \( f \) to a map that fixes the equator. Then we can use Alexander’s trick (3.9.2.1). □

3 CW Complexes

Def.(3.9.3.1)[CW Complexes]. A CW complex is a space \( X \) that \( \varnothing \to X \) is cofibrantly generated by \( S^n \to \mathbb{D}^n \).

For a CW complex \( X \), a representation of \( X \) is given as follows:

- \( \text{sk}_0 X \) is a discrete set, whose elements are regarded as 0-cells.
- Inductively, form the \( n \)-skeleton \( \text{sk}_n X \) from \( \text{sk}_{n-1} X \) by adding \( n \)-cells \( e^n_\alpha \) via maps \( \varphi_\alpha : S^{n-1} \to \text{sk}_{n-1} X \).
- Let \( X = \bigcup \text{sk}_n X \) be given the quotient topology from \( \coprod \text{sk}_n X \).

We will also call the image of \( e^n_\alpha \) as an \( n \)-cell. The category of CW complexes is denoted by \( \mathcal{CW} \). Any CW complex is compactly generated, by definition.

Def.(3.9.3.2)[Sub-CW Complexes]. For a CW complex \( X \), a subcomplex \( Y \subseteq X \) is a subspace \( Y \subseteq X \) s.t. the cells with images in \( Y \) makes \( Y \) a CW complex.

Def.(3.9.3.3)[Finite CW Complexes].

- A CW complex of finite dimension is a CW complex \( X \) s.t. \( X = \text{sk}_n X \) for some \( n \in \mathbb{N} \).
- A CW complex of finite type is a CW complex \( X \) that has only finitely many \( n \)-cells for each \( n \).
- A finite CW complex is a CW complex that is both of finite dimensional and of finite type.
- A locally finite CW complex is a CW complex that each cell intersect only f.m. other cells.

Prop.(3.9.3.4)[Dimension of CW Complexes]. Given a representation of a CW complex of finite dimension \( X \), \( \text{dim} X \) is defined to be the minimal \( n \) s.t. \( X = \text{sk}_n X \). Then this dimension is independent of the presentation given.
Proof:

Prop. (3.9.3.5). Any compact subspace $K$ of a CW complex $X$ is contained in a finite subcomplex. In particular, a CW complex is compact iff it is finite.

Proof: Firstly $K$ intersects with only f.m. interiors of cells of $X$ (where we assume the interior of a point in $sk_0 X$ is the point itself): otherwise take $S = \{x_1, x_2, \ldots\}$ be an infinite sequence of points lying in different cells, then $S \cap e_\alpha$ is closed for any cell $e_\alpha$ of $X$, so $S$ is closed. But the same argument show any single point of $S$ is also closed, so $S$ is discrete, so $S$ is finite, contradiction.

Then it suffices to show that any cell meets only f.m. cells: for this we can use induction on dim $X$, and notice that for any cell $e_\alpha$, the image of its attaching map is compact.

Prop. (3.9.3.6) [Miyazaki]. Any CW complex is paracompact Hausdorff, thus also normal by (3.6.7.6).

Proof: To show it is Hausdorff, for any two points $x, y$, it is not hard to find disjoint precompact nbhds of $x, y$ by induction on cells.

To show it is paracompact, Cf. [Rudolph Fritsch and Renzo Piccinini, Cellular Structures in Topology] Thm1.3.5.

Prop. (3.9.3.7). A CW complex is locally compact iff it is locally finite. A connected CW complex is metrizable iff it is locally finite.


Prop. (3.9.3.8) [Product of CW Complexes]. For $X, Y \in CW$, then the compactly generated product space $X \times_c Y$ admits a CW complex structure with

$$sk_n X = \bigcup_{i+j=n} sk_i X \times sk_j Y.$$ 

And if either $X$ or $Y$ is locally compact or both $X, Y$ have countably many cells, then $X \times_c Y = X \times Y$.

Proof: Given presentations of CW complexes of $X, Y$, we can define the CW complex structure on $X \times Y$ by choosing homeomorphisms of pairs

$$(D^n, S^n) \cong (D^p \times D^q, D^p \times S^{q-1} \cup S^{p-1} \times D^q),$$

where $p + q = n$. Then it is a CW structure on $X \times_c Y$ by (3.6.3.16).

For the last assertion, the case $X$ is locally compact follows from (3.6.2.33). The case that $X, Y$ both have countably many cells follow from [Hatcher, P524].

Prop. (3.9.3.9) [Cellular Maps]. Given $X, Y \in CW$, a cellular map $f : X \to Y \in CW$ is a map s.t. $f(sk_n X) \subset sk_n Y$ for any $n \in \mathbb{N}$. And a cellular homotopy between two cellular maps $f, g : X \to Y$ is a homotopy $F : X \times I \to Y$ between $f$ and $g$ s.t. $F$ is a cellular map.

Prop. (3.9.3.10) [CW Structure on Compact Manifolds]. $\text{Mani}_{\text{cpt}} \in CW^{\text{fin}}$.

Proof:
Prop. (3.9.3.12) [Pathspace is CW Complex]. The homotopy fibers (3.6.3.18) of any map \( f: A \to B \) between CW complexes are homotopic to a CW complex.

Proof: [Milnor, 1959]. or [Rudolph Fritsch and Renzo Piccinini, Cellular Structures in Topology]. □

Cor. (3.9.3.13) [Loop Space]. For \( X \in CW^pt \), the loop space (3.6.3.19) \( \Omega X \) is homotopic to a pointed CW complex. In particular, if \( X \) is of f.t., then so does \( \Omega X \).

Proof: This is a special case of (3.9.3.12) applied to \( A = \{*\} \), by (3.6.3.20). □

Common CW complexes

Def. (3.9.3.14) [Infinite Vector Spaces]. Let \( K = \mathbb{R}, \mathbb{C} \) or \( \mathbb{H} \), then the **infinite vector space** \( K^\infty \) is the CW complex \( \lim_n^\infty K^n \).

There can be given a norm map on \( K^\infty \), as the canonical embedding is norm preserving.

Prop. (3.9.3.15) [Grassmannian]. Let \( K = \mathbb{R}, \mathbb{C} \) or \( \mathbb{H} \), then the **Grassmannian** \( \text{Gra}(k, K^n) \) admits a CW complex structure.

Proof: Cf. [Algebraic Topology Miller, P46] or [Characteristic Classes, Milnor]. □

Def. (3.9.3.16) [Infinite Grassmannian]. Let \( K = \mathbb{R}, \mathbb{C} \) or \( \mathbb{H} \), then the **infinite Grassmannian** \( \text{Gra}(k, K^\infty) \) is the CW complex \( \lim_n^\infty \text{Gra}(k, K^n) \) (11.6.2.12).

In particular, \( \text{Gra}(1, K^\infty) \cong \lim_n^\infty K P^n \) is defined to be the **infinite projective space** \( K P^\infty \).

Def. (3.9.3.17) [Infinite Stiefel Manifold]. Let \( K = \mathbb{R}, \mathbb{C} \) or \( \mathbb{H} \), then the **infinite Stiefel Manifold** \( V_k(K^\infty) \) is the CW complex \( \lim_n^\infty V_k(K^n) \) where \( V_k(K^n) \) is the set of orthonormal \( k \)-frames (11.6.2.12).

\( V_1(K^\infty) = \lim_n^\infty S^n \) is called the **infinite sphere**. It is isomorphic to

\[
S^\infty = \lim_n^\infty S^{2k+1} = \lim_k^\infty C^{2k+1}\backslash \{0\}/\mathbb{R}^+ = (C^\infty\backslash \{0\})/\mathbb{R}^+.
\]

Prop. (3.9.3.18). \( V_k(K^\infty) \) is contractible.

Proof: We prove for \( S^\infty \), the proof for \( V_k(K^\infty) \) is verbatim, using Smith orthogonalization.

There is a map \( H: S^\infty \times I \to S^\infty \) defined by

\[
H((x_1, x_2, \ldots), t) = ((1 - t)x_1, tx_2 + (1 - t)x_1, tx_3 + (1 - t)x_2, \ldots)/N
\]

where \( N \) is the norm of the non-zero element \( ((1 - t)x_1, tx_2 + (1 - t)x_1, tx_3 + (1 - t)x_2, \ldots) \). The image of \( H_1 \) is in the subspace \( S^\infty_0 \) of elements \( (x_1, x_2, \ldots) \) with \( x_1 = 0 \). Notice there is another map \( H': S^\infty_1 \times I \to S^\infty \) defined by

\[
H'((0, x_2, \ldots), t) = (t, (1 - t)x_2, (1 - t)x_3, \ldots)/N'
\]

where \( N' \) is the norm of the non-zero element \( (t, (1 - t)x_2, (1 - t)x_3, \ldots) \). Then the composition homotopy \( (H' \circ H_1) \cdot H \) gives the desired homotopy from \( \text{id}_{S^\infty} \) to a constant map. □
Prop. (3.9.3.19). $\mathbb{R}P^\infty = S^\infty/\{\pm 1\} = (\mathbb{C}^\infty \backslash \{0\})/\mathbb{R}^\times$.

Def. (3.9.3.20) [James Reduced Product]. Let $X$ be a space with a basepoint $e$, let the James reduced product space $J(X)$ be the quotient of $\prod_n X^n$ under the identification $(x_1, \ldots, x_j, \ldots, x_n) \sim (x_1, \ldots, \hat{x}_j, \ldots, x_n)$ if $x_j = e$.

$J(X)$ is a union of subspaces $J_m(X)$, where $J_m(X)$ is the quotient space of $X^m$ under the identification $(x_1, \ldots, x_j, \ldots, x_n) \sim (x_1, \ldots, e, x_j, \ldots, x_n)$. If $(X, e)$ is a CW-pair, then $J_m$ is obtained from $X^m$ by gluing together its $m$ subcomplexes where one of the coordinates is $e$. It is then clear $J$ is a CW complex.

Def. (3.9.3.21) [Infinite Symmetric Product]. Let $X$ be a space with a basepoint $e$, define the infinite symmetric product as the quotient of $J(X)$ by permutations. If $X$ is a simplicial complex, then $SP(X)$ is a CW-complex.

Proof: Cf.[Hat02]P482.

4 Homotopy Groups

Def. (3.9.4.1) [Homotopy Groups]. For $(X, *) \subset \mathcal{Top}^pt$ and $n \in \mathbb{N}$, define the homotopy groups $\pi_n(X) = \pi_n(X, *) = \langle S^n, X \rangle$, which is a pointed set.

And $\pi_1(X)$ is a group as $S^1$ has a cogroup structure: $S^1 \to S^1 \wedge S^1$. Similarly, $\pi_n(X) = \pi_1(\Omega^{n-1} X)$ are also groups, and the group structure are given by the cogroup structure $S^n \to S^n \wedge S^n$.

Prop. (3.9.4.2) [Loop Spaces and Homotopy Groups]. $\pi_{i+1}(M) \cong \pi_i(\Omega(M))$.

Proof: This follows from the fact $S^n = \Sigma^n(S^0)$ and (3.9.1.18).

Prop. (3.9.4.3) [Homotopy Groups are Abelian]. For $X \in \mathcal{CG}^pt$, the homotopy group $\pi_n(X)$ is an Abelian group for $n \geq 2$.

Proof: By (3.9.4.2), it suffices to show for $n = 2$, and $\pi_2(X) = \pi_1(\Omega X)$ is Abelian by (3.10.2.30) and (3.10.2.24).

Cor. (3.9.4.4). For any $X \in \mathcal{CG}$, $\langle \Sigma(X), Y \rangle$ is a group and $\langle \Sigma^2(X), Y \rangle$ is an Abelian group.

Prop. (3.9.4.5) [Homotopy Groups and Change of Basepoints]. Let $X \in \mathcal{CG}$ and $\gamma : I \to X$ be a path from $a$ to $b$, then for any $n \in \mathbb{Z}_+$, we can define a map $\gamma_\# : \pi_n(X, a) \to \pi_n(X, b)$ as follows: For any $f : (I^n, \partial I^n) \to (X, a)$, identity $I^n$ with the subspace of $\mathbb{R}^n$ consisting of vectors $x$ s.t. $d(x) \leq \frac{1}{2}$, where $d((x_1, \ldots, x_n)) = \min(|x_i|)$, and

$$\gamma_\#(f) : (I^n, \partial I^n) \to X : x \mapsto \begin{cases} f(2x), & ||x|| \leq \frac{1}{4} \\ \gamma(4||x|| - 1), & \frac{1}{4} \leq ||x|| \leq 1 \end{cases}$$

Then for any $x_0 \in X$, this defines an actions of $\pi_1(X, x_0)$ on $\pi_n(X, x_0)$ by group homomorphisms for any $n \in \mathbb{Z}_+$. And for $n = 1$, this is just the conjugation action.

Proof: It is a well-defined action because any homotopy between two maps $f_1, f_2 : (I^n, \partial I^n) \to (X, a)$ can generate a homotopy between $\gamma_\#(f_1)$ and $\gamma_\#(f_2)$, and it is an action by group homomorphism because there is a homotopy between $\gamma_\#(f) \cdot \gamma_\#(g)$ and $\gamma_\#(f \cdot g)$, which is easy to write out.
Def.(3.9.4.6)[Simple Spaces]. A space $X \in \mathcal{S}$ is called a simple topological space if for any $x_0 \in X$, the action of $\pi_1(X, x_0)$ defined in (3.9.4.5) is trivial.

Def.(3.9.4.7)[Weak Homotopy Equivalences]. $f : X \rightarrow Y \in \mathcal{S}$ is called a weak homotopy equivalence if it induces isomorphism $\pi_n((X, x_0)) \cong \pi_n(Y, f(x_0))$ for any $n \in \mathbb{N}$ and $x_0 \in X$.

Prop.(3.9.4.8). Let $f_0, f_1 : X \rightarrow Y \in \mathcal{S}$ be maps and $h : I \times X \rightarrow Y$ be a homotopy $x_0 \in X$, then if $\gamma : I \rightarrow Y : t \mapsto h(t, x_0)$, then

$$\gamma_\# \circ \gamma_\#(f_0)_* = (f_1)_*.$$

Proof: For $f : f : (I^n, \partial I^n) \rightarrow (X, x_0)$ is easy to write out a homotopy between $\gamma_\#(f_0)_*(f)$ and $(f_1)_*(f)$. \qed

Cor.(3.9.4.9). Any homotopy equivalence is a weak homotopy equivalence.

Def.(3.9.4.10)[Relative Homotopy Groups]. For an inclusion $i : (A, *) \subset (X, *) \in \mathcal{Top}_{pt}$, $n \in \mathbb{Z}_+$, define the relative homotopy groups $\pi_n(X, A) = \pi_n(X, A, *) = \pi_{n-1}(P(X; *, A))$, where $P(X; *, A)$ is the homotopy fiber of $i$. Equivalently, if we denote $J^n = \partial I^n \times I \cup I^{n-1} \times \{0\} \subset I^n$ for $n \geq 2$ and $J^1 = \{0\} \subset I^1$, then

$$\pi_n(X, A) = [(I^n, \partial I^n, J^n), (X, A, *)].$$

This is a pointed set for $n = 1$, a group for $n = 2$, and an Abelian group for $n \geq 3$.

Prop.(3.9.4.11)[Long Exact Sequence of Relative Homotopy Groups].

Proof: \qed

Cor.(3.9.4.12)[Covering Spaces and Homotopy Groups]. If $E \rightarrow B$ is a covering space, then $\pi_n(E) \rightarrow \pi_n(B)$ is an isomorphism for $n \geq 2$.

Prop.(3.9.4.13). If $X \in \mathcal{S}_{pt}$ is contractible, then $\pi_n(X) = 0$ for any $n \geq 0$.

Prop.(3.9.4.14)[Products and Homotopy Groups]. For $X, Y \in \mathcal{S}_{pt}$, $\pi_n(X \times Y) = \pi_n(X) \times \pi_n(Y)$ for any $n \in \mathbb{N}$.

Prop.(3.9.4.15)[Colimits and Homotopy Groups]. If $X = \lim\nolimits_i X_i \in \mathcal{S}_{pt}$ is a filtered colimits, there are natural isomorphisms

$$\lim\nolimits_i \pi_n(X_i) \cong \pi_n(X)$$

for each $n \in \mathbb{N}$.

Proof: This follows from the fact any compact subset of $X$ is contained in some $X_i$. \qed

Def.(3.9.4.16)[n-Connectedness]. For $n \in \mathbb{N}$, $(X, A) \in \mathcal{S}_{rel, pt}$ is called $n$-connected if $\pi_i(X, A) = *$ for any $i \leq n$. $X \in \mathcal{Top}_{pt}$ is called $n$-connected if $\pi_i(X) = *$ for any $i \leq n$.

Def.(3.9.4.17) [$n$-Equivalences]. For $n \in \mathbb{Z}_+$, $f : (X, A) \rightarrow (Y, B) \in \mathcal{Top}_{rel}$ is called an $n$-equivalence if $f_* : \pi_p(X, A) \rightarrow \pi_p(Y, B)$ are isomorphisms for $p < n$, and surjective for $p = n$.

Thm.(3.9.4.18)[Excision for Homotopy Groups]. If $m, n \geq 0$, $(X; A, B)$ is an excise triad s.t. $(A, A \cap B)$ is $m$-connected and $(B, A \cap B)$ is $n$-connected, then $(A, A \cap B) \rightarrow (A \cup B, A)$ is an $m + n$-equivalence.
Proof: Cf.[Hatcher P360].

**Cor. (3.9.4.19).** For \( n > 1 \), \( \pi_n(\bigvee S^n) \) is free Abelian with \( \pi_n(S^n) \) as generators. This is because \( (\prod S^n, \bigvee S^n) \) is \((2n - 1)\)-connected thus use excision, because \( \pi_n(\prod S^n) \) is easy to calculate.

**Prop. (3.9.4.20).** If \( f : X \to Y \) is an \( n \)-equivalence between \((n - 1)\)-connected spaces, then the quotient map \( pr : (M(f),X) \to (C(f),*) \) is an \( 2n \)-equivalence. And if \( X,Y \) are both \( n \)-connected, then \( pr \) is an \( 2n + 1 \)-equivalence.

**Proof:**

**Cor. (3.9.4.21) [Quotients and Homotopy Groups].** For \( n \in \mathbb{Z}_+ \), if \( i : A \to X \) is a cofibration that is a \( (n - 1) \)-equivalence of \((n - 1)\)-connected space, then the map \( (X,A) \to (X/A,*) \) is an \( 2n \)-equivalence. And if \( A, X \) are \( n \)-connected, then this is a \( 2n + 1 \)-equivalence.

**Proof:** This follows from the commutative diagram

\[
\begin{align*}
(M(i), A) & \longrightarrow (C(i), *) \\
\downarrow & \\
(X, A) & \longrightarrow (X/A, *)
\end{align*}
\]

where the vertical maps are homotopy equivalences, by (3.9.6.7).

**Prop. (3.9.4.22) [Suspension and Homotopy Groups, Freudenthal].** For \( X \in \mathcal{G}^{\text{well-pt}} \), there are maps

\[
\Sigma_* : \pi_p(X) \to \pi_{p+1}(\Sigma(X)) : f \in \langle S^p, X \rangle \mapsto \Sigma(f) \in \langle S^{p+1} \cong \Sigma(S^p), \Sigma(X) \rangle
\]

Then if \( n \in \mathbb{N}, X \in \mathcal{G}^{\text{well-pt}} \) and \( X \) is \( n \)-connected, then \( \Sigma_* \) is bijective for \( p \leq 2n \) and surjective for \( p = 2n + 1 \).

In particular, \( \Sigma^n(X) \) is \((n - 1)\)-connected.

**Proof:** Cf.[May, P85].

**Def. (3.9.4.23) [Stable Homotopy].** For \( X \in \mathcal{G}^{\text{well-pt}} \), using the suspension (3.9.4.22), we can form the colimit

\[
\pi^*_p(X) = \lim_{n \in \mathbb{N}} \pi_{p+n}(\Sigma^n(X)).
\]

Then by (3.9.4.22),

\[
\pi^*_p(X) = \pi_{p+n}(\Sigma^n(X)), \quad n \geq p + 2.
\]

**Prop. (3.9.4.24).** The homotopic direct limit of a family of homotopy equivalence is a homotopy equivalence. Cf.[Morse Theory Milnor].

**Fundamental Groups**

**Def. (3.9.4.25) [Simply Connected].** A space is called **simply connected** if it is connected and \( \pi_1(X, x) = 0 \) for some point \( x \in X \).

**Def. (3.9.4.26) [Semilocally Simply Connected].** A space is called **semilocally simply connected** if for any point \( x \in X \), there is a nbhd \( U \) of \( x \) that the image of the inclusion-induced map \( \pi_1(U, x) \to \pi_1(X, x) \) is trivial.
Prop. (3.9.4.27) [Van Kampen]. If $X$ is a union of path-connected subsets $A_{\alpha}$ all containing $x_{0}$ that $A_{\alpha} \cap A_{\beta}$ and $A_{\alpha} \cap A_{\gamma}$ are all path-connected, then $\ast \pi_{1}(A_{\alpha})/\sim$ where $\sim$ is generated by $i_{\ast}(\pi_{1}(A_{\alpha} \cap A_{\beta})) \in \pi_{1}(A_{\alpha}) \sim i_{\ast}(\pi_{1}(A_{\alpha} \cap A_{\beta})) \in A_{\beta}$ for every $\alpha, \beta$.

Proof: Cf. [Hatcher P52].

Prop. (3.9.4.28) [Wedge Sums]. If $X_{i} \in \mathcal{C}^{\text{well-pt}}$ and $X = \bigvee X_{i}$, then $\pi_{1}(X) = \ast_{i} \pi_{1}(X_{i})$.

5 CW Approximations

Prop. (3.9.5.1) [CW Complex has Homotopy Extension Property]. For $(X, A) \in \mathcal{C}^{\text{rel}}$, $X \times \{0\} \cup A \times I$ is a deformation retract of $X \times I$, thus $(X, A)$ has the homotopy extension property (3.9.6.1).

Proof: Cf. [Hat02]P15.

Lemma (3.9.5.2) [Compression and Homotopies]. For $n \in \mathbb{Z}_{+}$, $f : B \to Y \in \mathcal{C}$, the following are equivalent:

- $f_{\ast}$ induces an injection on $\pi_{n}$ and a surjection on $\pi_{n+1}$.
- Any map $(D^{n}, S^{n}) \to (Y, B) \in \mathcal{Top}^{\text{rel}}$ is homotopic rel $S^{n}$ to a map $D^{n} \to B$.

Proof: Cf. [May, P70].

Thm. (3.9.5.3) [Compression Theorem]. If $n \in \mathbb{Z}_{+}$, $(X, A) \in \mathcal{C}^{\text{rel}}$ has relative dimension $\leq n$ and $f : B \to Y$ an $n$-equivalence, then any map $(X, A) \to (Y, B) \in \mathcal{C}^{\text{rel}}$ is homotopic rel $A$ to a map $X \to B$.

In particular, (relative) homotopy doesn’t depend on (2-degree) higher dimensional cells, (but might on lower one).

Proof: Use (3.9.5.2) on each cells.

Thm. (3.9.5.4) [Whitehead]. If $f : Y \to Z \in \mathcal{C}$ is an $n$-equivalence, then $[X, Y] \to [X, Z]$ is bijective for $X \in \mathcal{C}^{\text{pt}}$ of dimension $\leq n - 1$, and surjective for $\dim X = n$.

Proof: The surjectivity follows from the compression theorem for the pair $(\emptyset, X) \in \mathcal{C}^{\text{rel}}$, and the injectivity follows from the compression theorem applied to $(X \times I, X \times \partial I) \in \mathcal{C}^{\text{rel}}$.

Cor. (3.9.5.5). If $Y \to Z \in \mathcal{Top}^{\text{pt}}$ is a weak-equivalence, then $(X, Y) \to (X, Z)$ is an equivalence for any $X \in \mathcal{C}^{\text{pt}}$.

Cor. (3.9.5.6) [Whitehead]. For $n \in \mathbb{Z}_{+}$, an $n$-equivalence of CW complexes of dimension $\leq n - 1$ is a homotopy equivalence.

A weak equivalence of CW complexes is a homotopy equivalence.

Proof: Let $e : Y \to Z \in \mathcal{C}$ satisfies the hypothesis, then because $e_{\ast} : [Z, Y] \to [Z, Z]$ is a bijection by compression theorem (3.9.5.3), there exists $f : Z \to Y$ s.t. $e \circ f \cong \text{id}$. Thus $e \circ f \circ e \cong e$. Then since $e_{\ast} : [Y, Y] \to [Y, Z]$ is also a bijection by compression theorem, $f \circ e \cong \text{id}$.

Cor. (3.9.5.7). If $X \in \mathcal{C}^{\text{pt}}$ and $\pi_{n}(X) = 0$ for all $n$, then $X$ is contractible.
Cor. (3.9.5.8) [Whitehead Combinatorial Homotopy Theorem I]. If $M$ and $K$ is dominated by CW complexes, then any weak homotopy equivalence is an homotopy equivalence. If the map is an inclusion, then it is a deformation retract. In particular, if $M$ is manifold, then it is dominated by its tubular nbhd, so this theorem is applied.

Proof: For inclusion, use compression, and in general use mapping cylinder and cellular approximation.

Cellular and CW Approximations

Lemma (3.9.5.9). For $n \in \mathbb{Z}_+$, $f (X, A) \in \mathcal{CW}^{rel}$ has no $m$-cells for $m \leq n$, then $(X, A)$ is $n$-connected. In particular, $(X, X^n)$ is $n$-connected.

Proof: It suffices to show that any map $f : (\mathbb{D}^n, \partial \mathbb{D}^n, \mathbb{S}^n) \to (X, A, \ast)$ is homotopic to a map $(\mathbb{D}^n, \mathbb{S}^n) \to (A, \ast)$ rel $\mathbb{S}^n$ (3.9.1.1). For this, notice that the image is compact, thus we can assume that $(X, A)$ is finite. Thus by doing one cell by one cell, it suffices to show for $X = A \coprod_{f \mathbb{S}^n} \mathbb{D}^n$. In this case, notice that by simplicial approximation, we can find a homotopic map $f \simeq f'$ that $f'$ avoids some point in $(\mathbb{D}^n)^\circ$. Then we can use projection to construct a homotopy.

Thm. (3.9.5.10) [Cellular Approximationss]. Any map $f : (X, A) \to (Y, B) \in \mathcal{CW}^{rel}$ is homotopic rel $A$ to a cellular map.

In particular, any $f : X \to Y \in \mathcal{CW}$ is homotopic to a cellular map.

Proof: This follows from (3.9.5.9).

Remark (3.9.5.11). The cellular approximation makes the computation of homotopy theoretically easier, but the difficulty comes from the complexity of the homotopy group of the sphere.

Remark (3.9.5.12). In fact, all the rest of this subsubsection can be rewritten by the geometric realization functor $\Gamma(X) \to X$ (3.12.3.7). It is functorial in the level of spaces.

Prop. (3.9.5.13) [n-Connected CW Models]. For a pair $(A, X)$, if $A$ is CW complex, then there is a n-connected (3.9.4.16) CW pairs $(Z, A) \to (X, A)$ that is identity on $A$, and $\pi_i(Z) \to \pi_i(X)$ is isomorphism for $i > n$ and injection for $i = n$.

Such a pair $(Z, A)$ is called a n-connected CW model of $(X, A)$, and moreover it can be constructed from $A$ by attaching cells of dimension greater than $n$.

Proof: Cf. [Hatcher P353].

Cor. (3.9.5.14). For an $n$-connected CW pair $(X, A)$, there exist a homotopic $(Z, A) \cong (X, A)$ rel $A$ that $Z \setminus A$ has only cells of dimension greater than $n$.

Proof: Choose the $n$-connected approximation as above. The map induce and isomorphism on $\pi_{>n}$ by definition and on $\pi_{<n}$ because $\pi_i(A) \to \pi_i(Z)$ and $\pi_i(A) \to \pi_i(X)$ are isomorphisms. And on $\pi_n$, it is injective by definition and surjective because $\pi_n(A) \to \pi_n(Z) \to \pi_n(X)$ is isomorphism.

Hence we know that the collapsed mapping cylinder at is weak-homotopy equivalent to $Z$, thus it deforms into $Z$ by (3.9.5.8), thus $Z \to X$ rel $A$ by (3.9.1.5).
**Cor. (3.9.5.15)** [Functorial CW Approximations]. A CW approximation of a space $X$ is a CW complex $Z$ and a weak homotopy equivalence $Z \to X$. A CW approximation of a pair $(X, A)$ is pair of CW complexes $(Z, Z_0)$ and a morphism $(Z, Z_0) \to (X, A)$ that induces isomorphisms on both relative and absolute homotopy groups.

Thus there exists a CW approximation for any space $A$, and also there exists a CW approximation for any pair $(X, X_0)$.

*Proof:* Just choose $A$ to be a set containing a point for each connected component of $X$, then $\pi_0(Z) \to \pi_0(X)$ is surjective hence injective.

For pairs, first approximate $X_0$ and use the mapping cylinder to get a embedding. 

**Prop. (3.9.5.16)** [Functoriality of CW Models]. Given $n$-connected CW model $f : (Z, A) \to (X, A)$ and $f' : (Z', A') \to (X', A')$, then any map of pairs $g : (X, A) \to (X', A')$ can be extended to a map of pairs $h : (Z, A) \to (Z', A')$ that $gf \cong f'h$ rel $A$. And such a map $h$ is unique up to homotopy rel $A$.

*Proof:* Cf.[Hatcher, P355].

**Cor. (3.9.5.17)** [Uniqueness of CW approximation]. The CW approximation is unique up to homotopy.

**Cor. (3.9.5.18)** [Localizing Category]. Together with Whitehead combinatorial homotopy theorem (3.9.5.8) the homotopy category of spaces defined in (3.12.2.3) is the category of spaces $\mathcal{CG}$ localized by the class of weak homotopy equivalence classes.

**Prop. (3.9.5.19)** [CW Approximation of Excisive Triads]. Cf.[May, 79].

### 6 Fibrations and Cofibrations

**Cofibrations**

**Def. (3.9.6.1)** [Homotopy Extension Property]. $(X, A) \in \text{Top}^{\text{rel}}$ is said to satisfy the **homotopy extension property** if every map $X \times \{0\} \sqcup A \times I \to Y$ can be extended to a map $X \times I \to Y$.

**Def. (3.9.6.2)** [Cofibrations]. A **cofibration** is a map $j : A \to X$ that for every map $X \times \{0\} \sqcup A \times I \to Y$ can be extended to a map $X \times I \to Y$.

This implies $X \times \{0\} \cup A \times I \to X \times I$ has a left inverse. And the converse is clearly true.

Then a cofibration is just a topological embedding with closed image that $(X, A)$ has the homotopy extension property (3.9.6.1).

Cofibrations is stable under cobase change and coproducts.

*Proof:* 

**Def. (3.9.6.3)** [NDR-Pairs]. An neighborhood deformation retraction pair, or an **NDR-pair** is a pair $(X, A) \in \text{Top}^{\text{rel}}$ s.t. there is a map $u : X \to I$ s.t. $u^{-1}(0) = A$, and a homotopy $f_t : X \to X$ rel $A$ s.t. $f_0 = \text{id}_X$, and $f_1(u^{-1}([0, 1])) \subset A$.

**Prop. (3.9.6.4)** [NDR Pairs and Cofibrations]. If $A \subset X$ is closed, then $(X, A)$ is a NDR-pair (3.9.6.3) iff $A \to X$ is a cofibration.

*Proof:* Cf.[May, P45].


Prop. (3.9.6.5) [CW-Pairs are Cofibrations]. By compression theorem (3.9.5.3), for any CW-pair \((A, X)\), \(A \to X\) is a cofibration.

Def. (3.9.6.6) [Hurewitz Cofibration]. A closed Hurewicz cofibration \(i : A \subset B\) is a closed inclusion of spaces that \(B \times \{0\} \amalg A \times I \to B \times I\) has left extension property w.r.t any map \(Y \to \text{pt}\).

Prop. (3.9.6.7) [Quotient a Contractible Cofibration]. If \(A \to X\) is a cofibration and \(A\) is contractible, then the quotient map \(X \to X/A\) is a homotopy equivalence. In particular, this applies to \((X, A) \in \text{CW}^\text{rel}\), by (3.9.5.1).

Proof: Let \(f_t : X \to Y\) be a homotopy extending a contraction of \(A\) to a point, with \(f_0 = \text{id}\). Since \(f_t(A) \subset A\), they descend to a homotopy \(\overline{f}_t : X/A \to X/A\). Because \(f_1(A)\) is a point, there is a map \(g\) in the following diagram

\[
\begin{array}{ccc}
X & \xrightarrow{f_1} & X \\
\downarrow{\pi} & & \downarrow{\pi} \\
X/A & \xrightarrow{\overline{f}_1} & X/A
\end{array}
\]

So \(g\) and \(\pi\) are inverse homotopy equivalences, because \(f_1 \cong f_0 = \text{id}\) and \(\overline{f}_1 \cong \overline{f}_0 = \text{id}\). \(\square\)

Prop. (3.9.6.8). Let \(X\) be a normal space, then an inclusion \(j : A \hookrightarrow X\) is a cofibration iff \(A \hookrightarrow V\) is a cofibration for some open nbhd \(V\) of \(j(A) \subset X\).

Proof: Cf. [AGP02] P92. \(\square\)

Prop. (3.9.6.9) [Homotopic Glueing Functions]. Let \(A \to X_1\) be a cofibration with \(X\) Hausdorff, and we have attaching maps \(f, g : A \to X_0\) that is homotopic, then \(X \amalg_f X_1 \cong X \amalg_g X_1\) rel \(X_0\).

Proof: Now choose a homotopy \(H : A \times I \to X_0\) connecting \(f\) and \(g\), then \(H\) induces a quotient space \(Z = X_0 \amalg_H (X_1 \times I)\). Let \(X = X_0 \amalg_f X_1, Y = X_0 \amalg_g X_1\), then there are natural inclusion maps \(i : X_1 \to Z, j : Y \to Z\), and there are also deformation retractions \(Z \to X, Z \to Y\) constructed as follows:

Choose a deformation retraction \(r\) of \(X_1 \times I\) onto \(X_1 \times \{0\}\) \(\amalg A \times I\) (3.9.6.1), and \(H\) induces a map \(\overline{H} : D^n \times \{0\} \amalg S^n \times I \to S^n \amalg_f D^n\), making the following diagram commutative

\[
\begin{array}{ccc}
A \times I & \xrightarrow{r} & X_1 \times I \\
\downarrow{H} & & \downarrow{\overline{H}} \\
X_0 & \xrightarrow{id} & X_0 \amalg_f X_1
\end{array}
\]

which by definition defines a deformation retraction \(r_1 : X_0 \amalg_H (X_1 \times I) \to X_0 \amalg_f X_1\). Similarly we have deformation retraction \(r_2 : Z \to Y\). So \(r_2 \circ i\) and \(r_1 \circ j\) induce an homotopy equivalence between \(X\) and \(Y\). \(\square\)

Prop. (3.9.6.10). If \(A \to X, A \to Y\) are cofibrations, and \(f : X \to Y\) is a homotopy equivalence that \(f|_A = \text{id}_A\), then \(f\) is a homotopy equivalence rel \(A\).

Proof: Cf. [Hatcher] P16. \(\square\)

Cor. (3.9.6.11). If \(j : A \to X\) is a cofibration which is also a homotopy equivalence, and \(X\) is Hausdorff, then \(A\) is a deformation retraction of \(X\).
Serre Fibrations

Def. (3.9.6.12) [Serre Fibration]. A Serre fibration is the right lifting class of $D^n \times \{0\} \to D^n \times I$ for every $n$. This is equivalent to: for any homotopy of $\partial D^n$ and a image $D^n$, there is a homotopy of $D^n$.

In particular, Serre fibrations are stable under base change, by (3.7.0.1).

Prop. (3.9.6.13). Being a Serre fibration is local on the target.

Proof: Cf. [Homotopical Point of View] P127. □

Prop. (3.9.6.14) [Long Exact Sequence of Serre Fibration]. Let $\pi : E \to X$ be a Serre fibration, let $b_0 \in B$ and $x_0 \in F = \pi^{-1}(b_0)$, then the map $\pi_* : \pi_n(E, F, x_0) \to \pi_n(B, b_0)$ is an isomorphism for all $n \geq 1$. In particular, there is a long exact sequence

$$\cdots \to \pi_n(F, x_0) \to \pi_n(E, x_0) \to \pi_n(B, b_0) \to \pi_{n-1}(F, x_0) \to \cdots \to \pi_0(B, b_0) \to 0.$$ 

by (3.9.4.11).

Proof: Cf. [Hat02] P376. [nLab]. □

Hurewicz Fibrations

Def. (3.9.6.15) [Hurewicz Fibrations]. A Hurewicz fibration is a map $p : X \to Y \in \mathcal{G}$ that has right lifting property w.r.t maps $A \times \{0\} \to A \times [0, 1]$ for any $A \in \mathcal{G}$. In particular, a Hurewicz fibration is a Serre fibration (3.9.6.12).

Hurewicz fibrations are stable under base change.

Prop. (3.9.6.16) [Comparing Fibers of a Hurewicz Fibration]. If $\pi : E \to B$ is a Hurewicz fibration, then for any arc $\gamma$ in $B$ with $\gamma(0) = a, \gamma(1) = b$, there is a homotopy equivalence $f_\gamma : \pi^{-1}(a) \cong \pi^{-1}B$, and the homotopy class of $f_\gamma$ only depends on the homotopy class of $\gamma$.

In other words, a Hurewicz fibration over $B$ determines a contravariant functor $\Pi_1(B) \to \text{Ho}(\mathcal{G})$.

Proof: This follows from the homotopy lifting property. □

Cor. (3.9.6.17). For a Hurewicz fibration $E \to B$, if $B$ is contractible, then it is fiber homotopy equivalent to a trivial fiber bundle.

Prop. (3.9.6.18). Let $\pi : E \to B, \pi' : E' \to B$ be Hurewicz fibrations and $f : E \to E'$ be a map over $B$ that is also a homotopy equivalence, then $f$ is a fiber homotopy equivalence.

Proof: Cf. [Miller, P141] ?

Prop. (3.9.6.19) [Homotopy Invariance of Pullbacks]. Let $\pi : E \to X$ be a Hurewicz fibration and $f_0, f_1 : Y \to X \in \mathcal{G}$ are two maps that are homotopic, then the two Hurewicz fibrations $f_0^*E/Y, f_1^*E/Y$ are fiber homotopy equivalent.

Proof: Cf. [Miller, P140] ?

Prop. (3.9.6.20) [Homotopy Fiber of Contractible Fibration]. Let $f : E \to B$ be a Hurewicz fibration with $E$ contractible, then the homotopy fibers (3.6.3.18) $F$ over $b_0$ is weak homotopy equivalent to $\Omega(B, b_0)$. 
Proof: Let \( x_0 \in \pi^{-1}(b_0) \). If we compose the contraction of \( E \) to \( x_0 \) with \( \pi \), then we get for each \( x \in E \) a path \( \gamma_x \) from \( \pi(x) \) to \( b_0 \). Then these give a map \( E \to PB : x \mapsto \pi \gamma_x^{-1} \), which is a lift of \( \pi \).

Then this map gives a commutative diagram

\[
\begin{array}{ccc}
F & \to & E \\
\downarrow & & \downarrow \\
\Omega(B, b_0) & \to & PB \\
\end{array}
\]

corresponding long exact sequences (3.9.6.14). Thus \( F \to \Omega(B, b_0) \) is a weak homotopy equivalence because \( E, PB \) are both contractible (3.6.3.20).

Prop. (3.9.6.21) [Pathspaces are Hurewicz Fibrations]. For any map \( f : A \to B \), the map \( \pi : E_f \to B : (a, \gamma) \mapsto \gamma(1) \) from the pathspace (3.6.3.18) is a Hurewicz fibration.

In particular, take \( A = \{x_0\} \), then the path space \( PB \to B \) is a Hurewicz fibration.

Proof: Firstly this map is continuous by (3.6.3.5). To verify the homotopy lifting property, let \( g : X \to B \) be a homotopy and \( \tilde{g}_0 : X \to E_f \) be a lifting, let \( \tilde{g}_0(x) = (h(x), \gamma_x) \). Define a lift \( \tilde{g}_t : X \to E_f \) by \( \tilde{g}_t(x) = (h(x), \gamma_x \cdot g_{0,t}(x)) \). The second term is concatenation, which can be defined because \( g_0(x) = \pi \tilde{g}_0(x) = \gamma_x(1) \).

To check this is a continuous homotopy, by (3.6.3.7), it suffices to show \( A \times I \times I \to B : (x, s, t) \mapsto \gamma_x \cdot g_{0,s}(x)(t) = \begin{cases} \gamma(x, (1 + t)s) & s \leq \frac{1}{1 + t} \\ g_{(1+t)s-1}(x) & s \geq \frac{1}{1 + t} \end{cases} \) is continuous.

Cor. (3.9.6.22) [Homotopy Fibers]. We can embed \( A \) into \( E_f \) by mapping \( x \) to \( (x, \gamma_x) \), where \( \gamma_x \) is the trivial loop at \( x \). Then \( A \) is a deformation contraction of \( E_f \), by restricting to shorter and shorter initial segments: \( H_t : E_f \to E_f : (a, \gamma) \mapsto (a, \gamma_t) \), where \( \gamma_t(x) = \gamma(t x) \).

Then we factored \( f \) as a homotopy equivalence followed by a fibration: \( A \to E_f \to B \).

If \( x_0 \in X \) and \( F_f \) is the fiber of \( E_f \) over \( x_0 \), then a map \( (I^{i+1}, \partial I^{i+1}, J^i) \to (A, B, x_0) \) is the same as a map \( (I^i, \partial I^i) \to (F_f, \gamma_0) \), where \( \gamma_0 \) is the trivial loop at \( x_0 \). Thus \( \pi_{i+1}(A, B, x_0) = \pi_i(F_f, \gamma_0) \).

Prop. (3.9.6.23) [Pathspace of a Hurewicz Fibration]. If \( \pi : E \to B \) is a fibration, then the inclusion \( E \to E_\pi \) (3.6.22) is a fiber homotopy equivalence. In particular, the homotopy fibers of \( \pi \) are homotopy equivalent to the actual fibers.

Proof: \( \square \)

Prop. (3.9.6.24) [Fibration Sequence]. Given a fibration \( \pi : E \to B \) with \( F = \pi^{-1}(b_0), x_0 \in F \), there is a sequence

\[
\ldots \to \Omega^2(B, b_0) \to \Omega(F, x_0) \to \Omega(E, x_0) \to \Omega(B, b_0) \to F \to E \to B \to 0
\]

where any two consecutive maps form a fibration, up to homotopy.

Proof: By (3.9.6.23), the inclusion \( i \) of \( F \) to the homotopy fiber \( F_\pi \) over \( \pi \) over \( p \) is a homotopy equivalence, and it extends to a map \( i : F_p \to E : (x, \gamma) \mapsto x \), which is also a Hurewicz fibration, because it is the pullback of the fibration \( PB \to B \) (3.9.6.21).

Thus we can take the homotopy fiber \( F_i \) of \( i : F_p \to E \) over \( x_0 \), and similarly there is a fibration \( j : F_i \to F \), and \( F \) is naturally homotopic to the actual fiber of \( i \), which is just \( \Omega(B, b_0) \). \( \square \)
Model Category Structure

**Lemma (3.9.6.25) [Cofibrant Replacement]**. Any map \( f : X \to Y \) is a composition \( X \to M_f \to Y \). Notice \( M_f \to Y \) is a homotopy equivalence and \( X \to M_f \) is cofibrant by (3.9.6.4).

**Cor. (3.9.6.26) [Homotopy equivalence and mapping cylinder]**. A map \( f : X \to Y \) is a homotopy equivalence iff \( X \) is a deformation retraction of the mapping cylinder \( M_f \). In particular, two spaces are homotopically equivalent iff there is a third space containing both of them as deformation retracts.

*Proof:* Cf.[Hatcher] P16.

**Lemma (3.9.6.27) [Fibrant Replacement]**. Any map \( f : X \to Y \) is a composition \( X \to N(f) \to Y \), where \( N(f) = X \times_Y Y^I \), where \( Y^I \to Y \) is evaluation at \( \{0\} \), and \( X \to N(f) \) is given by \( x \mapsto (x, c_f(x)) \), where \( c_f(x) \in Y^I \) is the constant map \( f(x) \).

It is true that \( N(f) \to Y \) is a fibration, Cf.[May, 50].

*Proof:* \( X \to N(f) \) is homotopy inverse to the projection map: We can use the homotopy \( N(f) \times I \to N(f) : (x, a) \mapsto \chi : t \mapsto \chi(at) \).

To show that \( N(f) \to Y \) is a fibration, Cf.[May, 50].

**Prop. (3.9.6.28) [Serre-Quillen]**. The category \( CG \) can be given a Serre-Quillen model structure with
- Weak equivalences: weak homotopy equivalence,
- Fibrations: Serre fibrations,
- Cofibrations: Retracts of morphisms \( X \to Y \) where \( Y \) is obtained from \( X \) by attaching cells.

*Proof:* Cf.[Homotopy Theories and Model Categories, Chap8].

**Prop. (3.9.6.29)**. The homotopy category \( Ho(\mathcal{Top}) \) of the Serre-Quillen model structure is equivalent to the homotopy category of spaces \( \mathcal{H} \).

*Proof:* □

**Lemma (3.9.6.30)**. Every map can be decomposed as a homotopy equivalence followed by a fibration, by the construction of homotopy fibers.

*Proof:* □

**Prop. (3.9.6.31) [Hurewicz-Ström]**. The category \( CG \) can be given a Hurewicz-Ström model structure with
- Weak equivalences: homotopy equivalences.
- Cofibrations: closed Hurewicz cofibrations.
- Fibrations: Hurewitz fibrations.

*Proof:* Cf.[strum paper].

**Prop. (3.9.6.32)**. The homotopy category of the Hurewicz-Ström model structure is equivalent to the usual category of homotopy types.
7 Calculations of Homotopy Groups

**Prop.(3.9.7.1).** For $0 < k < n \in \mathbb{Z}$, $\pi_k(S^n) = 0$. And for $0 < n$, $\pi_0(S^n) = \ast$.

**Proof:** This follows from cellular approximation (3.9.5.10) and the canonical CW structure on $S^n$. □

**Prop.(3.9.7.2).** For $i \geq 2$, $\pi_1(\mathbb{RP}^i) \cong \mathbb{Z}/(2)$, and $\pi_n(\mathbb{RP}^i) \cong \pi_n(S^i)$ for $n \neq 1$.

**Proof:** This follows from the fiber sequence $\mathbb{Z}/(2) \to S^n \to \mathbb{RP}^n$ and (3.9.4.12). □

**Lemma(3.9.7.3).** There is a covering space $\mathbb{R} \to S^1$ with fiber $\mathbb{Z}$, thus $\pi_1(S^1) \cong \mathbb{Z}$.

**Prop.(3.9.7.4)[Hopf Fibration].** By (3.11.1.12) and (3.9.6.14), there is a long exact sequence

$$\ldots \to \pi_i(S^1) \to \pi_i(S^3) \to \pi_i(S^2) \to \pi_{i-1}(S^1) \to \ldots \to \pi_0(S^2) \to 1.$$

Thus $\pi_i(S^3) \cong \pi_i(S^2)$ for $i \geq 3$, and $\pi_2(S^2) \cong \pi_1(S^1) \cong \mathbb{Z}(3.9.7.3)$.

**Prop.(3.9.7.5)[Finiteness of Sphere Homotopy].** For $p > n > 1$, $\pi_p(S^n)$ are all finite except for $\pi_{4n-1}(S^{2n})$.

**Proof:**

**Prop.(3.9.7.6)[Basic Sphere Homotopy].** For $n \in \mathbb{Z}_+$, there are maps $\pi_i(S^n) \to \pi_{i+1}(S^{n+1})$ that is an isomorphism for $i < 2n - 1$ and surjective for $i = 2n - 1$.

In particular, $\pi_n(S^n) \cong \pi_2(S^2) \cong \mathbb{Z}$ for any $n \geq 2$.

**Proof:** This follows from Freudenthal suspension theorem (3.9.4.22). The last assertion follows from (3.9.7.3). □

**Prop.(3.9.7.7).** $\pi_4(S^3) \cong \pi_4(S^2) \cong \mathbb{Z}/(2)$.

**Proof:** □

**Prop.(3.9.7.8).** For $i \leq 2m$, $\pi_i G_m(\mathbb{C}^{2m}) \cong \pi_{i-1} U(m)$, and

$$\pi_{i-1} U(m) \cong \pi_{i-1} U(m + 1) \cong \ldots .$$

and for $j \neq 1$, $\pi_j U(m) \cong \pi_j SU(m)$.

Similarly, $\pi_i \Omega(2m) \cong \pi_{i+1} \Omega(2m)$ for $i \leq n - 4.(11.3.1.12)$, Cf[Morse Theory Milnor Prop23.4].

**Cor.(3.9.7.9)[Bott Periodicity theorem for Unitary Groups].** The stable homotopy group $\pi U$ has period 2. $\pi_{2k+1} U \cong 0$ and $\pi_{2k} U \cong \mathbb{Z}$.

**Proof:** Use the last proposition and long exact sequence to show that for $1 \leq i \leq 2m$,

$$\pi_{i-1} U = \pi_{i-1} U(m) \cong \pi_i G_m(\mathbb{C}^{2m}) \cong \pi_{i+1} SU(2m) \cong \pi_{i+1} U.$$ Notice that $U(m) \to U(2m)/U(m) \to G_m(\mathbb{C}^{2m})$ □

**Prop.(3.9.7.10) [Bott Periodicity for $O$].** For the infinite dimensional orthogonal space $O$, $\Omega_8(16r) \cong O(r)$, $\Omega_4(8r) \cong Sp(2r)$. So $\Omega_8 \cong O$ and $\Omega_4 O \cong Sp$. Thus by (3.9.4.2),

$$\pi_i(O) = \mathbb{Z}/(2), \mathbb{Z}/(2), 0, \mathbb{Z}, 0, 0, 0, \mathbb{Z}\ldots , \quad \pi_i(Sp) = 0, 0, 0, \mathbb{Z}, \mathbb{Z}/(2), \mathbb{Z}/(2), 0, \mathbb{Z}\ldots$$

respectively. (Use (11.3.1.13)) Cf.[Morse Theory Prop24.7].

**Prop.(3.9.7.11).** If a simply-connected finite complex $X$ is not contractible, then infinitely many of its homotopy groups are non-zero.

**Proof:** Cf.[Jean-Pierre Serre, Cohomologie modulo 2 des complexes d'Eilenberg-Maclane] □
3.10 Algebraic Topology II: Homologies and Cohomologies

Notations (3.10.0.1).
- Use notations defined in Algebraic Topology I: Homotopies.

1 Homologies

Axiomatic Homologies

Def. (3.10.1.1) [Eilenberg-Steenrod Homology Theories]. A Eilenberg-Steenrod homology theory is given by the following data:
- A functor $E_p(\_): \text{Ho}(\text{Top}^{\text{rel}}) \rightarrow \text{Ab}$ for any $p \in \mathbb{Z}$. For $X \in \text{Top}$, denote $H_p(X, \emptyset)$ by $E_p(X)$.
- For any $p \in \mathbb{Z}$, an equivariant boundary map $\partial: E_p(X, A) \rightarrow E_{p-1}(A)$ for any $(X, A) \in \text{Ho}(\text{Top}^{\text{rel}})$.

that satisfies

Exact Sequence: For $(X, A) \in \text{Top}^{\text{rel}}$, there is a natural long exact sequence
\[
\cdots \rightarrow E_p(A) \rightarrow E_p(X) \rightarrow E_p(X, A) \xrightarrow{\partial} E_{p-1}(A) \rightarrow \cdots.
\]

Excision: For any excisive triad $(X; A, B) (3.9.1.6)$, the inclusion $(A, A \cap B) \rightarrow (X, B)$ induces an isomorphism
\[
E_p(A, A \cap B) \cong E_p(X, B).
\]

Additivity: If $(X, A) = \coprod_{\alpha} (X_{\alpha}, A_{\alpha})$, then there are natural isomorphisms
\[
\bigoplus_{\alpha} E_p(X_{\alpha}, A_{\alpha}) \cong E_p(X, A).
\]

By functorial CW approximations on relative spaces (3.9.5.15), CW approximation of excisive triads (3.9.5.19) and Whitehead theorem (3.9.5.6), such a theory is equivalent to a theory restricted to all CW complexes with cellular maps as morphisms.

Prop. (3.10.1.2) [Cofibrations]. Given an Eilenberg-Steenrod homology theory $E_*$, for any cofibration $i: A \rightarrow X \in \text{Top}$, there is a natural isomorphism
\[
E_*(X, A) \cong E_*(X/A, \text{*)}.
\]

Proof: As $i$ is a cofibration, $C(A) \rightarrow C(i) = X \coprod_{A \times \{0\}} C(A)$ is also a cofibration. Consider the commutative diagram
\[
\begin{array}{ccc}
E_*(X \coprod_{A \times \{0\}} (A \times [0, 2/3]), A \times [1/3, 2/3]) & \rightarrow & E_*(C(i), (A \times [1/3, 1])/(A \times \{1\})) \\
\downarrow & & \downarrow \\
E_*(X, A) & \rightarrow & E_*(X/A, \text{*)}
\end{array}
\]

Then the upper horizontal map is an isomorphism by excision, and the vertical maps are isomorphisms by homotopy invariance. The right vertical map is
\[
(C(i), (A \times [1/3, 1])/(A \times \{1\})) \cong (C(i), C(A)) \cong (X/A, \text{*)}
\]
by (3.9.6.7). Then the lower horizontal map is also an isomorphism. \qed
**Def. (3.10.1.3) [Reduced Homology Theories]**. A reduced Eilenberg-Steenrod homology theory is given by the following data: A functor $\tilde{E}_*(\;): \text{Ho}(\mathcal{C}^\text{well-pt}) \to \text{Ab}$ for any $p \in \mathbb{Z}$ that satisfies

**Exactness**: For any cofibration $i : A \to X \in \mathcal{C}^\text{well-pt}$, the sequences

$$\tilde{E}_p(A) \to \tilde{E}_p(X) \to \tilde{E}_p(X/A)$$

are exact.

**Suspension**: For any $X \in \mathcal{C}^\text{well-pt}$, there are natural isomorphisms

$$\Sigma_* : \tilde{E}_p(X) \cong \tilde{E}_{p+1}(\Sigma X).$$

**Additivity**: If $X = \bigvee_{\alpha} X_{\alpha}$, then there are natural isomorphisms

$$\bigoplus_{\alpha} \tilde{E}_p(X_{\alpha}) \cong \tilde{E}_p(X).$$

By functorial CW approximations on pointed spaces (3.9.5.15), such a theory is equivalent to a theory restricted to all CW complexes with cellular maps as morphisms.

**Prop. (3.10.1.4) [Reduction to Reduced Homology Theories]**. Giving an Eilenberg-Steenrod homology theory is equivalent to giving a reduced Eilenberg-Steenrod homology theory. Thus from now on we will not distinguish from a reduced ES-homology theory and an ES-homology theory.

**Proof**: Given an ES homology theory $E_*$, for $X \in \text{Top}^\text{pt}$, define $\tilde{E}_*(X) = E_*(X, \ast)$, then the maps $\ast \to X \to \ast$ induce a natural splitting $E_*(X) \cong \tilde{E}_*(X) \oplus E_*(\ast)$. Then it is easy to show $\tilde{E}_*$ is a reduced ES homology theory by (3.10.1.2): For suspension, because $C(X)$ is contractible and $X \to C(X)$ is a cofibration, the long exact sequence for $C(X)/X \cong \Sigma(X)$ and (3.10.1.2) implies the isomorphism

$$\Sigma^{-1} : \tilde{E}_{p+1}(\Sigma(X)) \cong \tilde{E}_{p+1}(C(X)/X) \cong E_{p+1}(C(X), X) \xrightarrow{\partial} \tilde{E}_p(X).$$

Conversely, if $\tilde{E}_*$ is a reduced ES homology theory, define $E_*(X, A) = \tilde{E}_*(C(A \to X))$ where $C(A \to X)$ is pointed over the cone point. In particular, $E_*(X) = \tilde{E}_*(X_+)$ (3.9.1.16). We also define the boundary map as

$$\partial : E_*(X, A) \cong \tilde{E}_*(C(i_+)) \xrightarrow{\partial} \tilde{E}_*(\Sigma(A_+)) \xrightarrow{\Sigma^{-1}} E_{*-1}(A_+),$$

where $\partial$ comes from $\Sigma(A_+) \cong C(i_+)/X_+$.

To show $E_*$ is a ES homology theory: additivity is clear. The homotopy invariance follows from (3.9.1.17). To show exactness?. To show excision?. Cf. [May, P110].

To show that these two constructions are inverse to each other, it suffices to show that the $\partial$ and $\Sigma$ defined are inverse to each other?.

**Lemma (3.10.1.5)**. Let $E$ be an ES-homology theory and $B \subset A \subset X$, then there is a functorial long exact sequence

$$\cdots \to E_p(A, B) \to E_p(X, B) \to E_p(X, A) \xrightarrow{\partial} E_{p-1}(A, B) \to \cdots,$$

where $\partial : E_p(X, A) \to E_{p-1}(A) \to E_{p-1}(A, B)$. 

Proof: This follows from diagram chase or using the functorial CW approximations (3.9.5.15).

**Lemma (3.10.1.6).** If $E$ be an ES-homology theory and $(X; A, B)$ is an excisive triad, then the natural map
\[ E_*(A, A \cap B) \oplus E_*(B, A \cap B) \to E_*(X, A \cap B) \]
is an isomorphism.

Proof: This is done by using the CW approximations for excisive triads (3.9.5.19).

**Prop. (3.10.1.7) [Mayer-Vietoris Sequences].** Let $E$ be an ES-homology theory and $(X; A, B)$ be an excisive triad, then there is a long exact sequence
\[
\cdots \to E_p(A \cap B) \xrightarrow{((i_1)_*,(i_2)_*)} E_p(A) \oplus E_p(B) \xrightarrow{(j_1)_*-(j_2)_*} E_p(X) \xrightarrow{\Delta} E_{p-1}(A \cap B) \to \cdots ,
\]
where $\Delta$ is the composite
\[ E_p(X) \to E_p(X, B) \cong E_p(A, A \cap B) \xrightarrow{\partial} E_{p-1}(A \cap B). \]

Proof: Cf. [May, P112].

**Prop. (3.10.1.8) [Relative Mayer-Vietoris Sequences].** The relative MV-sequence is related to the MV-sequence (3.10.1.7) by
\[
\cdots \to E_p(Y, A \cap B) \xrightarrow{\partial} E_p(Y, A) \oplus E_p(Y, B) \xrightarrow{\partial \oplus \partial} E_p(Y, X) \xrightarrow{\partial} E_{p-1}(Y, A \cap B) \to \cdots 
\]

**Prop. (3.10.1.9) [Colimits].** If $X = \lim_{i \in \mathbb{N}} X_i$, then there is a natural isomorphism
\[ \lim_{i \in \mathbb{N}} E_*(X_i) \cong E_*(X). \]

Proof: Cf. [May, P115].

**Cor. (3.10.1.10).** For a reduced ES-homology theory $\tilde{E}_*$ and $(X_i)_{i \in \mathbb{N}} \in \text{Top}^{pt}$, there are natural isomorphisms
\[ \lim_{i \in \mathbb{N}} \tilde{E}_*(X_i) \cong \tilde{E}_*(\coprod_i X_i) (3.9.1.19). \]

The Ordinary Homology Theory

**Def. (3.10.1.11) [Ordinary Homology Theories].** For $\Lambda \in \text{Ab}$, an ordinary homology theory with coefficients in $\Lambda$ is a generalized homology theory (3.10.2.1) that satisfies the additional axiom

**Dimension:**
\[ E_p(pt) = \begin{cases} \Lambda, & p = 0 \\ 0, & p \neq 0 \end{cases}. \]

**Def. (3.10.1.12) [Ordinary Reduced Homology Theories].** For $\Lambda \in \text{Ab}$, an ordinary reduced homology theory with coefficients in $\Lambda$ is a reduced homology theory (3.10.1.3) that satisfies the additional axiom
Dimension: \( \tilde{E}_p(S^0) = \begin{cases} \Lambda & , p = 0 \\ 0 & , p \neq 0 \end{cases} \).

Def. (3.10.1.13) [Hurewicz Homomorphism]. For an ordinary homology theory \( H_* \), if we denote the generator of \( \tilde{H}_0(S^0) \) by \( a_0 \), and \( a_n = \Sigma^n(a) \in \tilde{H}_n(S^n) \), then for any \( X \in \mathcal{C}^{\text{pt}} \), define the Hurewicz homomorphism

\[ \text{Hur}_X : \pi_n(X) \to \tilde{H}_n(X) : f \mapsto f_*(a_n). \]

Prop. (3.10.1.14). For \( n \in \mathbb{Z}_+ \), \( X \in \text{Top}^{\text{pt}} \), \( \text{Hur}_X \) is a homomorphism of groups.

Proof: Cf. [May, P117]. \( \square \)

Prop. (3.10.1.15) [Generalized Hurewicz theorem]. If \( n \geq 2 \) and \( (X, A) \) is a \((n - 1)\)-connected pair of spaces, then the Hurewicz map induces an isomorphism

\[ \pi_n(X, A) / \sim \pi_1(A) \cong H_n(X, A), \]

and \( H_k(X, A) = 0 \), \( k < n \). Moreover, the Hurewicz map \( \pi_{n+1}(X, A) \to H_{n+1}(X, A) \) is surjective.

Proof: Cf. [Hatcher P371 and 390Ex23]. \( \square \)

Cor. (3.10.1.16) [Converse Whitehead]. If \( f : X \to Y \) is a map of simple pointed spaces that induces isomorphisms on all homology groups, then \( f \) is a weak homotopy equivalence.

Proof: We may change \( Y \) to the mapping cylinder of \( f \), then notice all the relative homology groups \( H_n(Y, X) \) vanishes by long exact sequence, and then by the generalized Hurewicz theorem, \( \pi_n(Y, X) = 0 \), and then \( f \) is a weak homotopy equivalence, by (3.9.4.11). \( \square \)

Thm. (3.10.1.17) [Hurewicz]. For \( n \in \mathbb{Z}_+ \), if \( X \in \mathcal{C}^{\text{pt}} \) is \((n - 1)\)-connected, then \( \text{Hur}_X : \pi_n(X) \to \tilde{H}_n(X) \) induces an isomorphism \( \pi_n(X)^{\text{ab}} \cong \tilde{H}_n(X) \). In particular, if \( n > 1 \), \( \pi_n(X) \cong \tilde{H}_n(X)(3.9.4.1) \).

Proof: Cf. [May, P118]. \( \square \)

The Cellular and Singular Realizations

Def. (3.10.1.18) [Degree of Maps]. For any \( f : S^n \to S^n \in \text{Top} \), we can choose a base point and use cellular approximation to make it homotopic to a cellular map \((S^n, \star) \to (S^n, \star)\), and define the degree of \( f \) to be the multiplying factor of \( f_* : \pi_n(S^n) \cong \mathbb{Z} \to \pi_n(S^n) \cong \mathbb{Z}(3.9.7.6) \).

Then this degree is independent of the base point chosen simply by rotation.

Prop. (3.10.1.19). The antipodal map \( S^n \to S^n \) has degree \((-1)^{n-1}\).

Proof: This is because the antipodal map is a composition of \( n+1 \) reflections, and each reflection is an \( n \)-suspension of a reflection on \( S^1 \to S^1 \), which clearly has degree \(-1\). Thus we finish by (3.9.7.6). \( \square \)
Def. (3.10.1.20) [Cellular Complex on $\mathbb{C}W$]. Given $X \in \mathbb{C}W$ with presentation $X = \bigcup_i X^i$, we can define the cellular homology groups as follows: Let $C_\bullet(X)$ be the complex with $C_p(X)$ the free Abelian group generated by the $p$-cells of $X$, and the map $C_p(X) \to C_{p-1}(X)$ is given by $e_\alpha \mapsto a_{\alpha \beta} e_\beta$, where for any $n$-cell $\alpha$ and $n-1$-cell $\beta$, $a_{\alpha \beta}$ is the degree (3.10.1.18) of the map

$$S^{p-1} \stackrel{\alpha}{\to} X^{p-1} \to X^{p-1} / X^{p-2} \xrightarrow{\beta^{-1}} S^{p-1}.$$ 

Then $C_\bullet(X)$ is truly a complex. More generally, for any $\Lambda \in \text{Ab}$, we can define $C_\bullet(X; \Lambda) = C_\bullet(X) \otimes \Lambda$.

Proof: Cf. [May, P99]. □

Def. (3.10.1.21) [Cellular Homology Groups]. For $X \in \mathbb{C}W$ and a subcomplex $A \subset X$, there is an inclusion $C_\bullet(A) \to C_\bullet(X)$. If we define $C_\bullet(X, A) = C_\bullet(X) / C_\bullet(A)$. Define the homology groups

$$H_p(X) = H_p(C_\bullet(X)), H_p(X, A) = H_p(C_\bullet(X, A)).$$

Then the long exact sequence associated to the exact sequence $0 \to C_\bullet(A) \to C_\bullet(X) \to C_\bullet(X, A) \to 0$ gives a boundary map $\partial : H_p(X, A) \to H_{p-1}(A)$.

More generally, for any $\Lambda \in \text{Ab}$, we can define $C_\bullet(X, A; \Lambda)$ and also $H_p(X; \Lambda), H_p(X, A; \Lambda)$.

Def. (3.10.1.22) [Cellular Complex of Products]. For $X, Y \in \mathbb{C}W$, with the CW structure on $X \times Y$ given in (3.9.3.8), then

$$C_\bullet(X) \otimes C_\bullet(Y) \cong C_\bullet(X \times Y).$$

Proof: The map $C_\bullet(X) \otimes C_\bullet(Y) \cong C_\bullet(X \times Y)$ is given by $e_\alpha \otimes e_\beta \mapsto (-1)^{|\alpha||\beta|} e_{\alpha \beta}$.

It is clear that this is an isomorphism up to sign. For the sign problem, see [May, P101]. □

Prop. (3.10.1.23). The cellular homology groups in (3.10.1.21) defines a ES-homology theory (3.10.1.21).

Proof: For homotopy invariance, notice a homotopy $X \times I \to Y$ between $f, g : X \to Y$ will induce a map

$$C_\bullet(X) \otimes C_\bullet(I) \to C_\bullet(Y)$$

by (3.10.1.22), and with the canonical CW structure, $C_\bullet(I)$ is just $0 \to \mathbb{Z} \xrightarrow{(1,-1)} \mathbb{Z} \oplus \mathbb{Z} \to 0$. By writing it out, this gives exactly a homotopy between the two maps $f_*, g_*$. Additivity, excision and exactness is clear. □

Def. (3.10.1.24) [Singular Homologies]. For $X \in \text{Top}$, $\Lambda \in \text{Ab}$, the singular cohomology groups with coefficients in $R$ is defined to be $H_{\text{sing}*}(X; \Lambda) = H_*(\Gamma(X); R)$ (3.12.3.7). This is the just the homology on $\text{Top}^{\text{red}}$ corresponding to the cellular homology on CW-pairs.

Thm. (3.10.1.25) [Uniqueness of Ordinary Homology Theories]. There exists a unique ordinary homology theory, i.e. the one defined in (3.10.1.21).

Proof: Cf. [May, P119]. □
2 Cohomologies

Remark (3.10.2.1)[Eilenberg-Steenrod Cohomology Theories]. The whole basic theory of cohomologies is dual to that of homologies, so it is omitted here. We only focus on new features appearing.

Def. (3.10.2.2)[Cohomological Operators]. Given reduced ES-cohomology theories \( \tilde{E}^* \), \( \tilde{F}^* \), \( p, n \in \mathbb{Z} \), a cohomological operator of type \( p \) and degree \( n \) is a natural homomorphism \( \tilde{E}^p \to \tilde{F}^{p+n} \).

A stable cohomological operator of degree \( n \) is a sequence of cohomological operators \( \Phi^p_n \) of type \( p \) and degree \( n \) that commutes with the suspension isomorphism.

Ordinary Cohomology Theories

Thm. (3.10.2.3)[Uniqueness of Ordinary Homology Theories]. There exists a unique ordinary cohomology theory, i.e. the one given by cellular cohomology groups.

Proof: The proof is the same as that of (3.10.1.25).

Prop. (3.10.2.4)[Universal Coefficient Theorem]. See (3.3.4.6).

Cor. (3.10.2.5). A map between topological spaces that induce isomorphism on arbitrary homology group induce isomorphisms on cohomology groups.

Def. (3.10.2.6)[Cup Product]. For \( X, Y \in \mathcal{CW} \), as \( C_\bullet(X) \otimes C_\bullet(Y) \cong C_\bullet(X \times Y) \) (3.10.1.22), for any \( R \in \mathcal{CAlg} \), there is a chain homomorphism

\[
\text{Hom}^\bullet(C_\bullet(X), R) \otimes \text{Hom}^\bullet(C_\bullet(Y), R) \to \text{Hom}^\bullet(C_\bullet(X \times Y), R),
\]

which induces a natural cross product map

\[
H^*(X; R) \otimes H^*(Y; R) \to H^*(X \times Y; R).
\]

And composing with the diagonal map \( \Delta_X : X \to X \times X \) gives a cup product map

\[
H^*(X; R) \times H^*(X; R) \to H^*(X \times Y; R)
\]

that makes \( H^*(X; R) \) into a unital commutative graded \( R \)-algebra.

Proof: Cf. [May, P139].

Def. (3.10.2.7)[Bockstein Homomorphism].

Prop. (3.10.2.8). The square of the Bockstein homomorphism \( H^n(X, \mathbb{F}_p) \to H^{n+2}(X, \mathbb{F}_p) \) is trivial.

Proof: There is a commutative diagram of commutative rings

\[
\begin{array}{cccccc}
0 & \to & \mathbb{Z} & \xrightarrow{x^m} & \mathbb{Z} & \to & \mathbb{Z}/(m) & \to & 0 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow \\
0 & \to & \mathbb{Z}/(m) & \xrightarrow{x^m} & \mathbb{Z}/(m^2) & \to & \mathbb{Z}/(m) & \to & 0
\end{array}
\]
which induces commutative diagrams

\[
\begin{array}{ccc}
H^n(X, \mathbb{Z}/(m)) & \xrightarrow{\bar{\beta}} & H^{n+1}(X, \mathbb{Z}) \\
\downarrow & & \downarrow \rho \\
H^n(X, \mathbb{Z}/(m)) & \xrightarrow{\beta} & H^n(X, \mathbb{Z}/(m))
\end{array}
\]

so \( \beta = \rho \bar{\beta} \), and \( \beta^2 = \rho \beta \rho \bar{\beta} = 0 \), as \( \bar{\beta} \rho = 0 \) by long exact sequence.

\( \square \)

**Prop. (3.10.2.9)** [Lefschetz Fixed Point Theorem].

**Prop. (3.10.2.10)** [Wedge Sums]. For \( M, N \in \text{Top} \), \( \tilde{H}^i(M \vee N) = \tilde{H}^i(M) \otimes \tilde{H}^i(N) \).

**Proof:** As \( M \# N/S^{d-1} = M \vee N \), there is a long exact sequence

\[ \ldots \rightarrow \tilde{H}^i(M \vee N) \rightarrow \tilde{H}^i(M \# N) \rightarrow \tilde{H}^i(S^{d-1}) \rightarrow \tilde{H}^{i+1}(M \# N) \rightarrow \ldots \]

Thus by (3.10.2.10), \( \tilde{H}^i(M \# N) = \tilde{H}^i(M) \oplus \tilde{H}^i(N) \) for \( i \neq d-1, d \). And there is an exact sequence

\[ 0 \rightarrow \tilde{H}^{d-1}(M \vee N) \rightarrow \tilde{H}^{d-1}(M \# N) \rightarrow \mathbb{Z} \rightarrow \tilde{H}^d(M \vee N) \rightarrow \tilde{H}^d(M \# N) \rightarrow 0. \]

If \( M, N \) are both orientable, then so does \( M \# N \), and the sequence looks like

\[ 0 \rightarrow \tilde{H}^{d-1}(M \vee N) \rightarrow \tilde{H}^{d-1}(M \# N) \rightarrow \mathbb{Z} \rightarrow \tilde{H}^d(M \vee N) \rightarrow 0. \]

and \( \tilde{H}^{d-1}(M \# N) \cong \tilde{H}^{d-1}(M \# N) \).

If only one of \( M, N \) is orientable, then similarly, \( \tilde{H}^{d-1}(M \vee N) \cong \tilde{H}^{d-1}(M \# N) \).

If neither \( M, N \) are orientable, then nor does \( M \# N \), and the sequence looks like

\[ 0 \rightarrow \tilde{H}^{d-1}(M \vee N) \rightarrow \tilde{H}^{d-1}(M \# N) \rightarrow \mathbb{Z} \rightarrow 0 \otimes 0 \rightarrow 0 \rightarrow 0. \]

which splits \( \square \), so \( \tilde{H}^{d-1}(M \# N) \cong \tilde{H}^{d-1}(M \vee N) \oplus \mathbb{Z} \).

**Cup and Cap Products**

Main references are [Hat02]Chap3.2.

**Prop. (3.10.2.12).** The cup product will restrict to a relative version:

\[ H^*(X, A) \times H^*(X, B) \rightarrow H^*(X, A \cup B), \]

This implies that if \( X \) is a union of \( n \) contractible open set, then the cup product of \( n \)-elements vanish. In particular, the cup product in a suspension vanishes.

**Prop. (3.10.2.13)** [Künneth Formula]. The cross product \( H^*(X, R) \otimes_R H^*(Y, R) \rightarrow H^*(X \times Y, R) \) is an isomorphisms of rings if \( X, Y \) are CW complexes and \( H^*(Y, R) \) are a finite free \( R \)-modules for any \( k \).

**Proof:** Cf. [Hat02]P219.

**Def. (3.10.2.14)** [Cap Products].
Cohomology of Fiber Bundles

Prop. (3.10.2.15) [Leray-Hirsch]. For a fiber bundle $F \to E \to B$ and a ring $R$ s.t. $H^n(F, R)$ is f.g free for all $n$, and there exist classes $c_j$ of $H^*(E)$ that constitute a basis for each fiber $F$, then

$$H^*(B, R) \otimes H^*(F, R) \to H^*(E, R)$$

is an isomorphism of $H^*(B, R)$-modules.

Proof:

□

Cor. (3.10.2.16).

• $H^*(U(n); \mathbb{Z}) = \Lambda_{\mathbb{Z}}[x_1, x_3, \ldots, x_{2n-1}]$.

• $H^*(SU(n, \mathbb{R}); \mathbb{Z}) = \Lambda_{\mathbb{Z}}[x_3, \ldots, x_{2n-1}]$.

• $H^*(Sp(n); \mathbb{Z}) = \Lambda_{\mathbb{Z}}[x_3, x_7, \ldots, x_{4n-1}]$.

Prop. (3.10.2.17). $H^*(G(n, K^{\infty}); \mathbb{Z})$ where $K = \mathbb{R}, \mathbb{C}, \mathbb{H}$ is generated by the symmetric polynomials, where for $\mathbb{R}$ the coefficient is $\mathbb{Z}_2$.

Proof: Use the flag variety and first calculate for $\infty$. Then use Poincare duality to show it is mapped onto the symmetric polynomials. Cf. [Hatcher P435]. □

Prop. (3.10.2.18) [Leray-Serre]. For a Serre fibration, e.g. fiber bundle, $F \to E \to B$, that $B$ is simply connected, then there is a spectral sequence

$$E_2^{pq} = H_p(B, H_q(F)) \Rightarrow H_{p+q}(E)$$

$$E_2^{pq} = H^p(B, H^q(F)) \Rightarrow H^{p+q}(E)$$

Cor. (3.10.2.19) [Wang Sequence]. When $B = S^n$, there is a long exact sequence:

$$\cdots \to H_q(F) \to H_q(E) \to H_{q-n}(F) \to H_{q-1}(F) \to H_{q-1}(E) \to \cdots$$

Cor. (3.10.2.20) [Gysin Sequence]. When $F = S^n$, there is a long exact sequence:

$$\cdots \to H_{p-n}(B) \to H_p(E) \to H_p(B) \to H_{p-n-1}(B) \to H_{p-1}(E) \to \cdots$$

H-Spaces

Def. (3.10.2.21) [H-Spaces]. An **H-space** is a unital magma object in $\text{Ho}(\mathcal{G}^{pt})$. Equivalently, an H-space is a pointed space $X \in \mathcal{G}^{pt}$ with a map $\mu : X \times X \to X \in \text{Ho}(\mathcal{G}^{pt})$ s.t. $X \to \{\ast\} \times X \to X$ and $X \to X \times \{\ast\} \to X$ is homotopic to $\text{id}_X$.

An **associative H-space** is an H-space s.t. $\mu_X$ is associative in $\text{Top}^{pt} / \sim$. Similarly, we can define group-H-spaces and commutative H-spaces.

An H-space is called strictly associative (or a monoid space) if it comes from a unital associative object in the category of spaces.

Remark (3.10.2.22). The definition of a H-space structure can be modified when $X$ is a CW complex. In fact, when $(X, e)$ is a CW-pair, if there exists a map $\mu : X \times X \to X$ and a point $e \in X$ that $X \to \{e\} \times X \to X$ and $X \to X \times \{e\} \to X$ is homotopic to $\text{id}_X$, then $\mu$ can be homotoped that $e$ is a strict identity.
3.10. ALGEBRAIC TOPOLOGY II: HOMOLOGIES AND COHOMOLOGIES 303

Proof:  

Prop. (3.10.2.23). If $H$ is an H-space, then for any $X \in \text{Top}^\text{pt}$, $(X, H)$ is a magma. Moreover, if $H$ is a commutative associative group H-space, then $(X, H) \in \text{Ab}$. 

Prop. (3.10.2.24)[Loop Spaces are H-Spaces]. For any $X \in \text{Top}^\text{pt}$, $\Omega(X)$ is an associative group-H-space, and $\Omega^2(X)$ is a associative commutative group-H-space.

Proof: The multiplication is given by concatenation of loops. It is continuous by adjunction arguments. 

Prop. (3.10.2.25). $CP^\infty$ can be given a commutative strictly associative H-space structure. More generally, $B(Z/n) \cong (C^\infty \setminus \{0\})/(R^\times \mu_n)$(3.11.3.13) can be given a commutative strictly associative H-space structure. In particular this applies to $RP^\infty$. 

Proof: We can regard $C^\infty$ as the space of polynomials with complex coefficients, then the polynomial multiplication gives a map $(C^\infty \setminus \{0\}) \times (C^\infty \setminus \{0\}) \to C^\infty \setminus \{0\}$ that descends to a map $B(Z/n) \times B(Z/n) \to B(Z/n)$. And $e = (1, 0, \ldots, 0, \ldots)$ is the unit. 

Prop. (3.10.2.26). The James reduced product $J(X)$ is a strictly associative H-space with multiplication given by $(x_1, \ldots, x_n) (y_1, \ldots, y_m) = (x_1, \ldots, x_n, y_1, \ldots, y_m)$, and the identity $e$. This H-space structure also descends to a H-space structure on $SP(X)$(3.9.3.21). 

Prop. (3.10.2.27). The universal cover of a H-space is a H-space.

Proof: Take an arbitrary lift that maps $(\tilde{e}, \tilde{e})$ to $\tilde{e}$. Notice the homotopy can also be lifted. 

Prop. (3.10.2.28)[Cohomology Ring]. The cohomology ring of a H-space is a topologists’ Hopf algebra, by Kunneth formula and naturality. 

Cor. (3.10.2.29). $CP^n$ is not a H-space.

Proof: This is because $H^*(CP^n, Z) = Z[\alpha]/\alpha^n, |\alpha| = 2$, which is not a topologist’s Hopf algebra, by(2.9.1.14). 

Prop. (3.10.2.30). The fundamental group of an H-space is Abelian. 

Proof: This is because $\pi_1$ preserves products, so takes unital magma space to unital magma objects(3.1.1.66). And the unital magma objects in the category of groups is the Abelian groups(3.1.1.65). 

Prop. (3.10.2.31)[Adam]. $S^0, S^1, S^3, S^7$ are the only spheres that have H-structures. 

Proof: Firstly $S^1 \subset C, S^3 \subset H, S^7 \subset O$ are submonoids, so they have H-structures. 

Cor. (3.10.2.32). $RP^n$ has a H-structure iff $n = 1, 3, 7$. 

Proof: This is because the universal cover of a H-space is a H-space(3.10.2.27). Also $S^1, S^2, S^3, S^7$ are monoid spaces, and $-1$ are in their center, so the quotients are also monoid spaces.
Examples of Calculations

Cor. (3.10.2.33).

\[ H^*(\mathbb{R}P^n, F_2) = \mathbb{Z}/(2)[a]/a^{n+1}, |a| = 1, \quad H^*(\mathbb{C}P^n, \mathbb{Z}) = \mathbb{Z}[\alpha]/\alpha^{n+1}, |\alpha| = 2 \]

Proof: We prove for \( \mathbb{R}P^n \), the \( \mathbb{C}P^n \) case is similar. Use induction. For \( n = 1 \), this is clear. For \( n > 1 \), notice \( \mathbb{R}P^n \) is the \( n-1 \)-skeleton of \( \mathbb{R}P^n \), thus the map of rings \( H^*(\mathbb{R}P^n, F_2) \to H^*(\mathbb{R}P^{n-1}, F_2) \) maps the generator of \( H^2(\mathbb{R}P^n, F_2) \) to the generator \( a \) of \( H^2(\mathbb{R}P^{n-1}, F_2) \). Then by hypothesis \( a^{n-1} \neq 0 \). The \( H^{n-1}(\mathbb{R}P^n, F_2) \cong H_1(\mathbb{R}P^n, F_2) \cong \mathbb{Z}/(2) \) is generated by \( a^{n-1} \). Then the Poincaré duality shows that \( \alpha \cup a^{n-1} \neq 0 \), so we are done.

Cor. (3.10.2.34). For \( n > 1 \), the natural homomorphism \( H^n(\mathbb{R}P^n, \mathbb{Z}/2\mathbb{Z}) \to H^n(S^n, \mathbb{Z}/2\mathbb{Z}) \) is 0.

Proof: Because the cohomology ring map maps \( a \in H^1(\mathbb{R}P^n, \mathbb{Z}/2\mathbb{Z}) \) to 0 in \( H^1(S^n, \mathbb{Z}/2\mathbb{Z}) = 0 \).

Prop. (3.10.2.35) \([H^*(K, \mathbb{Z}/(2))]\). The cohomology ring of the Klein bottle \( K \) is \( H^*(K, \mathbb{Z}/(2)) = F_2[x, y]/(xy, x^2 - y^2, x^3, y^3) \).

Proof: Let \( \varphi \in C^0(K, \mathbb{Z}/(2)) \) be the dual of \( v \), \( \alpha, \beta, \gamma \in C^1(K, \mathbb{Z}/(2)) \) be the dual of \( a, b, c \), and \( \mu, \lambda \in C^2(K, \mathbb{Z}/(2)) \) be the dual of \( A, B \), then

\[ \partial(\varphi)(a) = \partial(\varphi)(b) = \partial(\varphi)(c) = 0 \]
\[ \delta(\alpha)(A) = \alpha(\partial(A)) = \alpha(a + b - c) = 1, \quad \delta(\alpha)(B) = \alpha(\partial B) = \alpha(b + c - a) = -1 \]
\[ \delta(\beta)(A) = \beta(\partial(A)) = \beta(a + b - c) = 1, \quad \delta(\beta)(B) = \beta(\partial B) = \beta(b + c - a) = 1 \]
\[ \delta(\gamma)(A) = \gamma(\partial(A)) = \gamma(a + b - c) = -1, \quad \delta(\gamma)(B) = \gamma(\partial B) = \gamma(b + c - a) = 1 \]

So

\[ H^0(K, \mathbb{Z}/(2)) = \mathbb{Z}/(2)\varphi, \quad H^1(K, F_2) = F_2(\alpha + \beta) \oplus F_2(\alpha + \gamma), \quad H^2(K, F_2) = (F_2 \mu \oplus F_2 \lambda)/(\mu + \lambda). \]

Now we calculate the cup product:

\[ (\alpha + \beta) \cup (\alpha + \beta)(A) = (\alpha + \beta)(a) \cdot (\alpha + \beta)(b) = 1 \]
\[ (\alpha + \beta) \cup (\alpha + \gamma)(A) = (\alpha + \beta)(a) \cdot (\alpha + \gamma)(b) = 0 \]
\[ (\alpha + \gamma) \cup (\alpha + \gamma)(A) = (\alpha + \gamma)(a) \cdot (\alpha + \gamma)(b) = 0 \]
\[ (\alpha + \beta) \cup (\alpha + \beta)(B) = (\alpha + \beta)(b) \cdot (\alpha + \beta)(c) = 0 \]
\[ (\alpha + \beta) \cup (\alpha + \gamma)(B) = (\alpha + \beta)(b) \cdot (\alpha + \gamma)(c) = 1 \]
\[ (\alpha + \gamma) \cup (\alpha + \gamma)(B) = (\alpha + \gamma)(b) \cdot (\alpha + \gamma)(c) = 0 \]

Then \( (\alpha + \beta) \cup (\alpha + \beta) = (\alpha + \beta) \cup (\alpha + \gamma) = \mu \in H^2(K, \mathbb{Z}/(2)) \). Now if we set \( \alpha + \beta = x, \beta + \gamma = y \), then the cohomology ring

\[ H^*(K, \mathbb{Z}/(2)) = \mathbb{Z}/(2)[x, y]/(xy, x^2 - y^2, x^3, y^3). \]

Prop. (3.10.2.36) \([H^*(L, \mathbb{Z}/(m))]\). Let \( L \) be the Lens space, then the cohomology ring is calculated at [?]P304.

Proof:
3 Manifolds

Orientations

Prop. (3.10.3.1). Let $d \in \mathbb{Z}_+, R \in \mathcal{C}\text{Alg}, M \in \text{Mani}^d, X \subset M$, then for any $x \in M$, choose a nbhd $U$ of $x \in M$ s.t. $U \cong \mathbb{R}^n$, then by excision and exactness,

$$H_d(M,M\setminus x) \cong H_d(U, U\setminus x) \cong \tilde{H}_{d-1}(U\setminus \{x\}) \cong \tilde{H}_{d-1}(S^{d-1}) \cong R.$$  

Prop. (3.10.3.2) [Vanishing]. For $M \in \text{Mani}_{\text{cpt, cntd, } \partial}^d, \Lambda \in \mathcal{A}b$, $H_i(M; \Lambda) = 0$ for $i > d$, and $\tilde{H}_d(M; \Lambda) = 0$ unless $M$ is compact without boundary.

Proof:

Def. (3.10.3.3)[$R$-Fundamental Class]. Let $R \in \mathcal{C}\text{Alg}, M \in \text{Mani}^d_{\text{cntd}}, X \subset M$, an $R$-fundamental class of $M$ at $X$ is an element $z \in H_d(M,M\setminus X)$ s.t. for any $x \in X$, the map

$$H_d(M,M\setminus X) \rightarrow H_d(M,M\setminus \{x\})$$

maps $z$ to a generator of $H_d(M,M\setminus \{x\}) \cong R(3.10.3.1)$.

Def. (3.10.3.4)[$R$-Orientation]. Let $R \in \mathcal{C}\text{Alg}, M \in \text{Mani}^d_{\text{cntd}}, X \subset M$, an $R$-orientation of $M$ is an open cover \{$U_i$\} of $M$ and $R$-fundamental classes $z_i$ of $M$ at $U_i$ s.t. $z_i, z_j$ restricts to the same element in $H_d(M,M\setminus (U_i \cup U_j))$.

For $M \in \text{Mani}^d_{\text{cntd, } \partial}$, an $R$-orientation is an $R$-orientation of $M^u$.

Prop. (3.10.3.5)[$R$-Fundamental Classes and $R$-Orientations]. For $R \in \mathcal{C}\text{Alg}, M \in \text{Mani}^d$ and $K \subset M$ compact, then

- $H_i(M,M\setminus K, R) = 0$ for $i > d$.
- Any $R$-orientation of $M$ defines an $R$-fundamental class of $M$ at $K$ that is compatible for $x \in K$.

In particular, if $M$ is compact, then an $R$-orientation is equivalent to an $R$-fundamental class.

Proof: Firstly, if $K \subset U$ and $U \cong \mathbb{R}^n$ is a coordinate chart on which the $R$-orientation is defined, then by excision and exactness,

$$H_i(M,M\setminus K, R) \cong H_i(U, U\setminus K, R) \cong H_{i-1}(U\setminus K, R)$$

which vanishes for $i > n$ by vanishing theorem(3.10.3.2). And the $R$-orientation restricts to $K$.

In general, $K$ can be written as a sum of compact subsets each contained in a coordinate chart on which the $R$-orientation is defined. Then using induction, it suffices to show that if the results hold for $K, L, K \cap L$, then it holds for $K \cup L$: item1 follows from the MV-sequence

$$H_{i+1}(M,M\setminus (K \cup L)) \rightarrow H_i(M,M\setminus (K \cup L)) \rightarrow H_i(M,M\setminus K) \oplus H_i(M,M\setminus L) \rightarrow H_i(M,M\setminus (K \cap L)).$$

For item2, the same MV-sequence with $R$-coefficients and $i = d$ together with the definition of $R$-orientation classes(3.10.3.4) shows there exists a fundamental class at $K \cap L$ that restricts to the fundamental classes at $K$ and $L$. 

Prop. (3.10.3.6) [Orientation Dichotomy]. For $d \in \mathbb{Z}_+, M \in \text{Mani}^d_{\text{cntd, cpt}}$, there are only two cases:
• $M$ is non-orientable, and $H_d(M) = 0$.

• $M$ is orientable, and the map $H_d(M) \to H_d(M, M\backslash\{x\}) \cong \mathbb{Z}(3.10.3.1)$ is an isomorphism for any $x \in M$.

Proof: For any $R \in \mathbb{C}\text{Alg}$, as $M\backslash\{x\}$ is connected and non-compact, $H_d(M\backslash\{x\}; R) = 0$ by(3.10.3.2), thus

$$H_d(M, R) \to H_d(M, M\backslash\{x\}; R) \cong R$$

is injective. Thus $H_d(M) \cong 0$ or $\mathbb{Z}$. In particular, by universal coefficients theorem,

$$H_d(M) \otimes \mathbb{F}_p \to H_d(M, M\backslash\{x\}) \otimes \mathbb{F}_p$$

is injective for any $p \in \mathbb{P}$. Then it is clear to see that $H_d(M) \to H_d(M, M\backslash\{x\})$ is an isomorphism for any $x \in M$.

\[\square\]

Prop.(3.10.3.7) [Fundamental Classes on Manifolds with Boundaries]. For $M \in \text{Mani}^d_\partial$, $\partial M \neq 0$, an $R$-orientation on $M$ determines an $R$-orientation of $\partial M$. Moreover, the fundamental class $[\partial M]_R$ defined by(3.10.3.5) comes from the partial of a unique element $[M]_R \in H_d(M, \partial M; R)$, called the $R$-fundamental class determined the orientation.

\[\begin{proof}\]

By collar nbhd theorem, $M \cong M^\circ$, and by vanishing theorem, $H_d(M) \cong H_d(M^\circ) = 0$, thus $H_d(M, \partial M; R) \to H_{d-1}(\partial M; R)$ is injective. Let $N$ be an open collar of $\partial M$, then $H_d(M^\circ, M^\circ \cap N; R) \cong H_n(M, \partial M; R)$. Also, $M \backslash N$ is compact, so the orientation on $M^\circ$ defines a fundamental class in $H_d(M, M^\circ \cap N; R) \cong H_n(M, \partial M; R)$. Then this class determined the orientation on every point of $M^\circ$, and determines the orientation on $\partial M$, Cf.[May, P170].

\[\square\]

Prop.(3.10.3.8) [Orientation Coverings].

\[\begin{proof}\]

\[\square\]

Cor.(3.10.3.9). If $M \in \text{Mani}^d_\text{cntd}$, then if $M$ is orientable, it has exactly two orientations. And if $M$ is simply connected or $\pi_1(M)$ has no subgroup of index 2, then $M$ is orientable.

Def.(3.10.3.10) [Connected Sums]. For $M, N \in \text{Mani}^d_\text{cntd, cplt}$, define the connected sum $M \# N$ as follows: Take a subset $D \subset M, D' \subset N$ that are contained in coordinate charts(orientable coordinates charts if $M, N$ are oriented). $\varphi : U \cong \mathbb{R}^d, \varphi' : U' \cong \mathbb{R}^d$ s.t. $\varphi(D) \cong D(0) \cong \varphi(D' \setminus D')$. Then define

$$M \# N = (M \backslash D) \bigsqcup_{\partial D \cong \partial D'} (N \backslash D')$$

where $\partial D \cong \partial D'$ is an orientation-reversing homeomorphism when $M, N$ are both orientable. This is independent of $D, D'$ and the homeomorphism $\partial D \cong \partial D'$ chosen.

\[\begin{proof}\]

Firstly we show that $M \backslash D$ is independent of $D$ chosen: As $M$ is locally path connected and connected, it is path connected, Then we can consider a chain of charts isomorphic to $\mathbb{R}^d$ that connects any two such subsets $D, D'$. Then reducing to affine charts, it suffices to show for the case $M \cong \mathbb{R}^d$. In this case, we can use isotopy of $M$ to make $D \subset D'$, and then use the coordinate charts and annulus theorems(3.6.11.2) to show that $D' \backslash D$ is isomorphic to $S^{d-1} \times I$. Then the homeomorphism $M \backslash D \cong M' \backslash D'$ can be easily given.

Now we show the connected sum is independent of the homeomorphism chosen: $\partial D$ and $\partial D'$ are given orientations by the coordinate charts, and in the non-orientable case, use the argument above
on the orientation covering of $M(3.10.3.8)$, we know there exists a self-homeomorphism of $M$ that is isotopic to $\text{id}_M$ that reverses the orientation on $\partial D$. Thus in both cases, we can assume $\partial D \cong \partial D'$ is orientation-preserving. Now (3.9.2.2) shows any such homeomorphism is isotopic, and using the coordinate charts, we can extend the isotopy to a nbhd of nbhd of $\partial D$. Thus the connected sum is well-defined.

\textbf{Remark (3.10.3.11).} WARNING: The connected sum may be different in the orientable case if we change one of the orientations: $\mathbb{C}P^2 \# \mathbb{C}P^2$ is not homeomorphic to $\mathbb{C}P^2 \# \overline{\mathbb{C}P^2}$.

\textit{Proof:}

\textbf{Poincaré Duality}

\textbf{Lemma (3.10.3.12) [Poincaré Duality].} For $R \in \mathcal{C}\text{Alg}$, if $M \in \text{Mani}^d_{\text{cndt, cpct}}$ is $R$-oriented, then for any $p \in \mathbb{Z}$, there is an isomorphism

$$D = - \cap [M]_R : H^p(M; R) \cong H_{n-p}(M; R).$$

In particular, $H^n(X, \mathbb{F}_2) \cong \mathbb{Z}/(2)$, and the non-trivial element is called the \textbf{fundamental homology class mod 2}, denoted by $[M]_2$.

\textit{Proof:} which follows immediately from (5.8.6.30) and (5.3.5.9). (Should also attain the compact cohomology case if we know the relation of compact sheaf cohomology better).

\textbf{Prop. (3.10.3.13) [Relative Poincaré Duality].} Let $R \in \mathcal{C}\text{Alg}$, $M \in \text{Mani}^d_{\text{cpct, cntd}}$ be $R$-orientable with fundamental class $[M]_R \in H_d(M, \partial M; R)$, then for any $\Lambda \in \text{Mod}_R$, capping with $[M]_R$ defines isomorphisms

$$H^p(M, \partial M; \Lambda) \cong H_{d-p}(M), \quad H^p(M; \Lambda) \cong H_{d-p}(M, \partial M; \Lambda).$$

\textit{Proof:} Cf. [May, P170].

\textbf{Cor. (3.10.3.14).} For $M \in \text{Mani}^d_{\text{cndt, cpct, orntd}}$, for any $p \in \mathbb{Z}$, there is a perfect pairing

$$H^p(M)_{\text{if}} \times H^{n-p}(M)_{\text{if}} \to \mathbb{Z} : (\alpha, \beta) \mapsto \langle \alpha \cup \beta, [M] \rangle.$$

\textit{Proof:} By universal coefficient theorem?, $H^p(M)_{\text{if}} \cong \text{Hom}(H_p(M), \mathbb{Z})$. So if $\alpha \in H^p(M)$ is non-zero in $H^p(M)_{\text{if}}$, there exists $a \in H_p(M)$ s.t. $\langle a, \alpha \rangle = 1$. Then by Poincaré duality (3.10.3.12), there exists $\beta \in H^{d-p}(M)$ s.t. $\beta \cap [M] = a$. Thus $\langle \alpha \cup \beta, [M] \rangle = \langle \alpha, \beta \cap [M] \rangle = 1$.

\textbf{Def. (3.10.3.15) [Intersection Pairing].} Let $k \in \mathbb{N}, M \in \text{Mani}^{2k}_{\text{cpct, orntd, cntd}}$. The Poincaré duality (3.10.3.14) shows the cup product pairing

$$H^k(M; \mathbb{Q}) \times H^k(N; \mathbb{Q}) \to \mathbb{Q} : (\alpha, \beta) \mapsto \langle \alpha \cup \beta, [M] \rangle$$

is non-degenerate, called the \textbf{intersection pairing} of $M$. Notice if $k$ is odd, it is skew-symmetric, and if $k$ is even, it is symmetric.

\textbf{Def. (3.10.3.16) [Index].} For $M \in \text{Mani}^d_{\text{cpct, orntd, cntd}}$, define the \textbf{index of $M$} as the index of the symmetric intersection pairing of $M$ if $d = 4k$, and 0 otherwise. The index of $M$ is denoted by $I(M)$.
Prop. (3.10.3.17). For $M, N \in \text{Mani}_{\text{cpt,orntd,cntd}}$, $I(M \times N) = I(M)I(N)$.

Proof: Cf.[May, P167]. □

Prop. (3.10.3.18). For $k \in \mathbb{N}, k \in \text{Field}, M \in \text{Mani}_{\text{cpt,\&}}^{2k+1}$, then

$$\dim_k H_k(\partial M; k) = 2 \dim \ker(H_k(\partial M; k) \xrightarrow{i_\ast} H_k(M; k)) = 2 \dim \text{Im}(H_k(\partial M; k) \xrightarrow{i_\ast} H^k(M; k)).$$

Proof: There is a commutative diagram

$$
\begin{array}{ccc}
H^k(\partial M; k) & \xrightarrow{i_\ast} & H^k(M; k) \\
\downarrow D & & \downarrow D \\
H_{k+1}(M, \partial M; k) & \xrightarrow{\partial} & H_k(M; k) \xrightarrow{i_\ast} H_k(\partial M; k)
\end{array}
$$

where the vertical arrows are isomorphisms and $i_\ast$ is the vector dual of $i^\ast$ by universal coefficient theorem. Thus the theorem follows. □

Prop. (3.10.3.19) [Gysin Sequence]. Cf.[姜伯驹同调论].

Euler Characteristic

Def. (3.10.3.20) [Euler Characteristic]. For any $X \in \text{Top}$ with finite $\mathbb{Z}$-homologies, define the Euler character of $X$ to be

$$\chi(X) = \sum_i (-1)^i H_i(X; \mathbb{Z}).$$

Then by universal coefficients theorem (3.10.2.4),

$$\chi(X) = \sum_i (-1)^i H_i(X; k)$$

for any $k \in \text{Field}$. The condition holds for $X \in \mathbb{C}W_{\text{fin}}$, in particular any $X \in \text{Mani}_{\text{cpt}}$ (3.9.3.10).

Prop. (3.10.3.21). For any $i \in \mathbb{N}, X \in \text{Mani}_{\text{cpt,orntd}}^{2i+1}$, $\chi(X) = 0$.

Proof: This follows from Poincaré duality for $\mathbb{F}_2$-coefficients. □

Prop. (3.10.3.22) [Euler Characteristic and Boundary]. For $i \in \mathbb{N}, M \in \text{Mani}_{\text{cpt,\&}}^{2i+1}$, then

$$\chi(\partial M) = 2\chi(M).$$

Proof: Consider the “double” $\widetilde{M}$ of $M$ along $\partial M$, then $\widetilde{M} \in \text{Mani}_{\text{cpt,\&}}^{2i+1}$. It is clear by excision and collar neighborhood theorem that $\chi(\widetilde{M}) + \chi(\partial M) = 2\chi(M)$. Then we use (3.10.3.21). □

Cor. (3.10.3.23). If $N \in \text{Mani}_{\text{cpt}}$ is a boundary of some other $M \in \text{Mani}_{\text{cpt,\&}}$, then $\chi(N) = 0$.

Proof: If dim $N$ is odd, this is (3.10.3.21). If dim $N$ is even, this is (3.10.3.22). □

Prop. (3.10.3.24). For any $i \in \mathbb{N}, M \in \text{Mani}_{\text{cpt,orntd}}^{4i+2}$, $\chi(M)$ is even.

Proof: The parity of $\chi(M)$ is the same as $H^{2i+1}(M, \mathbb{Q})$, which is odd by (3.10.3.15) and (2.3.8.7). □
Prop. (3.10.3.25) [Morse Inequality]. For any $X \in \mathcal{CW}$,
$$\chi(X) \leq \sum (-1)^i c_i(X),$$
where $c_i(X)$ is the number of $I$-dimensional cells. (Use the dimension counting of the long exact sequence).

**Prop. (3.10.3.26).** For $M \in \text{Mani}_{\text{cpt,orntd}}^d$, $I(M) \equiv \chi(M) (\mod 2)$.

**Proof:** If $d$ is odd, $I(M) = 0 = \chi(M)$ is even by (3.10.3.21). If $d = 4k + 2$, then $I(M) = 0$ and $\chi(M)$ is even by (3.10.3.24). If $d = 4k$, then $I(M) \equiv \chi(M) \equiv \dim H^{2k}(M, \mathbb{Q})$.

**deRham Cohomology**

**Prop. (3.10.3.27) [de Rham Comparison].** For $X \in \text{Mani}_{\text{sm}}$, $G \in \mathcal{Ab}$, by (5.3.5.11).
$$H^*_\text{dr}(X, G) \cong H^*(X, G).$$

**Prop. (3.10.3.28) [Homotopy Axiom for deRham Cohomology].** For two homotopic map between two smooth manifold, they induce the same map on deRham Cohomology.

**Proof:** We only have to prove the case of $M \times \mathbb{R} \to M$, where any constant section map induces an isomorphism $H^*_\text{dr}(M \times I) \cong H^*_\text{dr}(M)$. Because any homotopy is a morphism $M \times I \to N$ where $f$ and $g$ are the sections 0 and 1.

For the zero section, we define $K : a + bdt \mapsto \int_0^t b$. This is the desired homotopy, Cf.[Differential Forms in Algebraic Topology Bott Tu].

4 Applications

**Prop. (3.10.4.1) [No Contraction to the Boundary].** For $M \in \text{Mani}_{\text{cpt,fr}}^d$, there are no retraction from $M$ onto $\partial M$.

**Proof:** We may assume $\partial M$ is connected and non-empty, otherwise clearly there are no retraction. If it has a retraction, $H_{d-1}(\partial M, \mathbb{F}_2) \to H_{d-1}(M, \mathbb{F}_2)$ has a left inverse. Thus it suffices to show that $H_{d-1}(\partial M, \mathbb{Z}/(2)) \to H_{d-1}(M, \mathbb{Z}/(2))$ is 0. So it suffices to show that $H_d(M, \partial M, \mathbb{Z}/(2)) \to H_{d-1}(\partial M, \mathbb{Z}/(2))$ is surjective. And this follows from (3.10.3.7) and (3.10.3.6) as the image of $[M]_2$ is $[\partial M]_2$, which generates $H_{d-1}(\partial M, \mathbb{F}_2)$.

**Prop. (3.10.4.2) [Brouwer Fixed Point Theorem].** For any $f : \mathbb{D}^n \to \mathbb{D}^n \in \mathcal{Top}$, $\text{Fix}(f) \neq \emptyset$.

**Proof:** If $\text{Fix}(f) = \emptyset$, consider the intersection of the ray $f(x)x$ with $S^{n-1}$, then it depends continuously on $x$, and this defines a function from $D^n$ to $S^n$ that is identity on $S^n$, but then this is a retraction from $\mathbb{D}^n \to \mathbb{S}^n$, which is impossible by (3.10.4.1).

**Prop. (3.10.4.3).** If $M \in \text{Mani}_{\text{cntd,fr}}^d$, then if $M$ is contractible and $\partial M \neq \emptyset$, $\partial M$ is a homotopy sphere.

**Proof:** As $M^n \sim M$ is contractible, it is orientable by (3.10.3.9). Then by relative Poincaré duality (3.10.3.13) and the long exact sequence,
$$H_p(\partial M) \cong H_{p+1}(M, \partial M) \cong H^{d-p-1}(M) = 0.$$
Lemma (3.10.4.4). If $m > n \in \mathbb{Z}^+$, any map $f : \mathbb{R}P^m \to \mathbb{R}P^n$ induces $f_* = 0 : \pi_1(\mathbb{R}P^m) \to \pi_1(\mathbb{R}P^n)$.

Proof: As $\pi_1(\mathbb{R}P^m) = \begin{cases} \mathbb{Z}/(2), & m > 1 \\ \mathbb{Z}, & m = 1 \end{cases}$. The assertion is clearly true for $n = 1$. And if $n \in \mathbb{Z}^+, f_* \neq 0$, then by the naturality of Hurewicz homomorphism (3.10.1.17), $f_* \neq 0 : H_1(\mathbb{R}P^m) \to H_1(\mathbb{R}P^n)$. Then by universal coefficient theorem, so is $f^* \neq 0 : H^1(\mathbb{R}P^n, \mathbb{F}_2) \to H^1(\mathbb{R}P^m, \mathbb{F}_2)$. But $f^*$ is a ring homomorphism and $H^*(\mathbb{R}P^m)$ is generated by $a = f^*(a') \in H^1(\mathbb{R}P^m)(3.10.2.33)$, so $a^{n+1} = f^*((a')^{n+1}) = 0$, contradiction. \square

Lemma (3.10.4.5). If $m > n \geq 1$, there are no antipodal maps: $f : S^m \to S^n$, i.e. $f(x) = -f(-x)$.

Proof: Any such map induces a map $\mathbb{R}P^m \to \mathbb{R}P^n$, which induces 0 on $\pi_1$, so by covering space theory, there exists a lifting $\mathbb{R}P^m \to S^n$. The composition $S^m \to \mathbb{R}P^m \to S^n$ is the original map, by the theory of covering spaces, as $S^n$ is connected and they agree at least on one point. But then $f$ takes antipodal maps to the same point, contradiction. \square

Thm. (3.10.4.6) [Borsuk-Ulam]. For ant map $f : S^n \to \mathbb{R}^n$, there exists $x \in S^n$ s.t. $f(x) = f(-x)$.

Proof: If $f(x) \neq f(-x)$ for any $x \in S^n$, then we can define a map $S^n \to S^{n-1}$ that maps $x$ to the intersection of the ray $0, f(x) - f(-x)$ with $S^n$. Then this map is antipodal, which contradicts (3.10.4.5). \square

5 Obstruction Theory & General Cohomology Theory

Towers

Prop. (3.10.5.1) [Towers]. There are Whitehead Towers and Postnikov Towers for a CW complex $X$.

$$\cdots \to Z_2 \to Z_1 \to Z_0 \to X \to \cdots \to X_2 \to X_1 \to X_0$$

$Z_n$ annihilate $\pi_{\leq n}(X)$, $X_n$ remains only $\pi_{\leq n}(X)$. The towers can be chosen to be fibrations, with fibers $K(\pi_nX, n)$ by (3.9.6.30).

Prop. (3.10.5.2). There is a Postnikov towers of:

$$B\text{String}(n) \to B\text{Spin}(n) \to B\text{SO}(n) \to BO(n)$$

with corresponding obstructions $w_1(X), w_2(X)$ and $p_1(X)/2$.

Prop. (3.10.5.3) [Obstructions]. If a connected abelian CW complex $X$ ($\pi_1(X)$ abelian and action on higher homotopy trivial) and $(W, A)$ satisfies $H^{n+1}(W, A; \pi_nX) = 0$ for all $n$, then $A \to X$ can extend to a map $M \to X$.

Proof: Cf. [Hatcher P417]. \square

Cor. (3.10.5.4). A map between Abelian CW complexes that induce isomorphisms on homology is a homotopy equivalence.

Proof: Notice that $\pi_1(X)$ acts trivially on $\pi_1(Y, X)$ and use Hurewicz. \square
6 Brown Representability

Prop.(3.10.6.1). For any $Z \in \mathcal{Top}^{pt}$, the functor

$$\langle - , Z \rangle : \mathcal{CW}^{pt} \to \mathcal{Set}^{pt}$$

satisfies:

**Exactness:** If $A \subset X$ is a subcomplex, then there is an exact sequence

$$\langle X/A, Z \rangle \to \langle X, Z \rangle \to \langle A, Z \rangle.$$

**Additivity:** If $X = \bigvee_i X_i \in \mathcal{CW}^{pt}$, then

$$\langle X, Z \rangle \cong \prod_i \langle X_i, Z \rangle.$$

*Proof:* 1 follows from the fact that $A \to X$ is a cofibration(3.9.6.5). 2 is trivial. □

**Spectrum**

Def.(3.10.6.2)[Prespectrums]. A prespectrum is a sequence of pointed spaces $(T_n)_{n \in \mathbb{Z}}$ together with maps $\sigma_n \in \langle \Sigma T_n \to T_{n+1} \rangle \cong \langle T_n, \Omega T_{n+1} \rangle$.

An $\Omega$-Spectrum is an prespectrum $(T_n)_{m \in \mathbb{Z}}$ s.t. $\sigma_n$ are all weak-homotopy equivalences.

Def.(3.10.6.3)[Suspension Prespectrums]. For $X \in \mathcal{Top}^{pt}$, the sequence of pointed spaces $(\Sigma^n(X))_{n \in \mathbb{Z}}$ (where we define $\Sigma^{-1} = \Omega$) is a prespectrum, called the suspension prespectrum of $X$. If $X = S^0$, this is called the sphere spectrum.

Prop.(3.10.6.4)[Prespectrum and Homotopy Theories]. Let $(T_n)_{n \in \mathbb{N}}$ be a prespectrum consisting of pointed CW complexes s.t. $T_n$ is $(n-1)$-connected for any $n \in \mathbb{N}$, then

$$\tilde{E}_p(X) = \lim_{n} \pi_{p+n}(X \wedge T_n)$$

is a reduced homology theory on $\mathcal{CW}^{pt}$.

*Proof:* Cf.[May, P176]. □

Prop.(3.10.6.5)[$\Omega$-Prespectrum and ES-Cohomology theories]. If $K_n$ is an $\Omega$-spectrum, i.e. $K_n \cong \Omega K_{n+1}$ weak equivalence, then the functors $X \mapsto \langle X, K_n \rangle$ define a reduces ES-cohomology theory on $\mathcal{CW}^{pt}$

*Proof:* By(3.10.6.1), these functors satisfy the additivity and exactness. The natural suspension isomorphism is given by

$$\Sigma : \langle X, T_n \rangle \to \langle \Sigma(X), \Sigma T_n \rangle \cong \langle \Sigma(X), \Sigma T_n \rangle,$$

which is an isomorphism by(3.9.5.5). □

Thm.(3.10.6.6)[Brown Representability]. Any reduced ES-cohomology theory on $\mathcal{CW}^{pt}$ is represented by a $\Omega$-prespectrum.

*Proof:* ? □
Eilenberg-Maclane Spaces

Def. (3.10.6.7) [Eilenberg-Maclane Spaces]. For $\Lambda \in Ab$, an Eilenberg-Maclane space is defined to be a pointed CW complex $K(\Lambda, n) \in \mathcal{CW}^pt$ s.t. $\pi_k(K(\Lambda, n)) = \begin{cases} \Lambda, & k = n \\ 0, & \text{otherwise.} \end{cases}$

Prop. (3.10.6.8) [Eilenberg-Maclane Spaces and Homologies]. For $X \in \mathcal{CW}^pt, \Lambda \in Ab$, there are isomorphisms

$$\tilde{H}_p(X; \Lambda) \cong \lim_{\longrightarrow} \pi_{p+n}(X \wedge K(\Lambda, n)).$$

Proof: Cf. [May, P176]. □

Prop. (3.10.6.9) [Eilenberg-Maclane Spaces and Cohomologies]. For $\Lambda \in Ab, X \in \mathcal{CW}^pt, n \in \mathbb{N}, K(\Lambda, n)$ are unique up to weak homotopy, and there are natural isomorphisms

$$\tilde{H}^n(X; \Lambda) \cong \langle X, K(\Lambda, n) \rangle.$$

Proof: Given a $K(\Lambda, n)$, if we define $K(\Lambda, m) = \Sigma^{m-n}(K(\Lambda, n))$, then these are all CW complexes by (3.9.3.13), and it defines an ordinary cohomology theory: The dimension axiom follows from the definition of $K(\Lambda, n)$, and it is a reduced ES-cohomology theory by (3.9.5.5) and (3.10.6.10). Thus the asserted isomorphism follows from (3.10.2.3).

This shows in particular that $K(\Lambda, n)$ are unique up to homotopy by Yoneda lemma. □

Cor. (3.10.6.10) [Uniqueness of Eilenberg-Maclane Spaces]. $K(\Lambda, n)$ is unique up to homotopy, and $\Omega(K(\Lambda, n)) \sim K(\Lambda, n - 1) \in \mathcal{CW}^pt$.

Prop. (3.10.6.11) [Eilenberg-Maclane Spaces Exist]. Take $K(\Lambda, n) = \Gamma(B(\Lambda, n))(3.11.3.7)$, where $\Lambda$ is regarded as a discrete subgroup.

Note $K(G, 1)$ is constructed the same as by (3.12.7.30).

Proof: □

Prop. (3.10.6.12) [Cohomology Operators]. Cohomological operators $\tilde{H}^p(-; \Lambda) \rightarrow \tilde{H}^{p+n}(-; \Lambda)$ are in bijection with elements in $\tilde{H}^{p+n}(K(\Lambda, p); \Lambda')$, by (3.10.6.9) and Yoneda lemma.

Prop. (3.10.6.13) [Examples].

- $K(\mathbb{Z}, 1) = S^1 = U(1)$.
- $K(\mathbb{Z}, 2) = \mathbb{C}P^\infty$.
- $K(\mathbb{Z}/(2), 1) = \mathbb{R}P^\infty$.

Proof: 1 is clear.

2: This is because by (3.11.1.17), $S^\infty \rightarrow \mathbb{C}P^\infty$ is a locally trivial bundle with fiber $S^1$, and $S^\infty$ is contractible by (3.9.3.18) thus by (3.9.6.14), $\pi_2(\mathbb{C}P^\infty) = \mathbb{Z}$ and $\pi_n(\mathbb{C}P^\infty) = 0$ for $n \neq 2$.

3: This is because by (3.11.1.17), $S^\infty \rightarrow \mathbb{C}P^\infty$ is a locally trivial bundle with fiber $\{\pm 1\}$, and $S^\infty$ is contractible by (3.9.3.18) thus by (3.9.6.14), $\pi_2(\mathbb{C}P^\infty) = \mathbb{Z}/2\mathbb{Z}$ and $\pi_n(\mathbb{C}P^\infty) = 0$ for $n \neq 2$. □
Steenrod Powers

Prop.(3.10.6.14)[Steenrod Powers]. There are stable cohomology operators

\[ Sq : H^*(X, F_2) \to H^*(X, F_2) : x \in H^k(X, F_2) \mapsto \sum_{i \in \mathbb{N}} Sq^i(x), \quad Sq^i(x) \in H^{k+i}(X, F_2) \]

called Steenrod Powers that satisfies

- \( Sq(\alpha \cup \beta) = Sq(\alpha) \cup Sq(\beta). \)
- \( Sq^i(\alpha) = \alpha^2 \) if \( i = |\alpha|, \) and 0 if \( i > |\alpha|. \)

For \( p \in P, \) the total Steenrod powers \( P \) is a similar map from \( H^n(X, F_p) \to H^{n+i}(X, F_p) \) that
\[ P^i(\alpha) = \alpha^p \] if \( 2i = |\alpha| \) and 0 if \( 2i > |\alpha|. \)

Proof: Cf.[Hatcher P497]. □

Prop.(3.10.6.15)[Adam Relations]. For \( 0 < i < 2j \in \mathbb{Z}, \)

\[ Sq^i Sq^j = \sum_{0 \leq k \leq \lfloor \frac{j}{2} \rfloor} \binom{j-k-1}{i-2k} Sq^{i+j-k} Sq^k \in \text{End}(H^*(-, F_2)) \]

There are Adam relation calculators in terms of Serre-Cartan basis at https://math.berkeley.edu/~kruckman/adem/.

Proof: □

Cor.(3.10.6.16). The subalgebra of \( \text{End}(H^*(-, F_2)) \) generated by \( \{ Sq^Z \} \) is generated respectively by elements \( Sq^{2k}. \)

and for \( p \in P \) The subalgebra of \( \text{End}(H^*(-, F_p)) \) generated by \( \{ P^Z \} \) is generated by elements \( P^p, \) and \( \beta. \)

Proof: □

Prop.(3.10.6.17)[\( H^*(K(F_2, p), F_2) \). \( H^*(K(F_2, p), F_2) \)] can be calculated, Cf.[May, P185].

Proof: □

7 Stable Homotopy Theory
3.11 Fiber Bundles & K-Theory

Main references are [Ati64], [AGP02] and [M-S74].

Remark (3.11.0.1). Any base space $B$ in this section is assumed to be paracompact. Instead, we may require in the definition of locally trivial bundles s.t. there exists a trivialization that is dominated by a partition of unity on $B$.

1 Fiber Bundles

Def. (3.11.1.1) [Fiber Bundles]. $\pi : E \to X \in \mathcal{CG}$ is called a fiber bundle with fiber $F$ if every fiber $\pi^{-1}(x)$ is homeomorphic to $F$. If any $x \in X$ has a nbhd $U$ together with a homeomorphism $\pi^{-1}(U) \cong U \times F$ over $U$, then it is called a locally trivial bundle. And a numerical locally trivial bundle is a locally trivial bundle $\pi : E \to X$ s.t. there is a numerical covering $\{U_i \to X\}$ s.t. there are homeomorphisms $\pi^{-1}(U_i) \cong U_i \times F$ over $U_i$ for each $i$.

Prop. (3.11.1.2) [Dold]. If $\pi : E \to X \in \mathcal{CG}$ and there is a numerical covering $\{U_i \to X\}$ s.t. $\pi^{-1}(U_i) \to U_i$ are Hurewicz fibrations, then $\pi$ is a Hurewicz fibration.

Proof: Cf. [Tammo tom Dieck, Algebraic Topology] Chap13. \qed

Cor. (3.11.1.3) [Fiber Bundles are Hurewicz Fibrations]. Every numerical locally trivial bundle is a Hurewicz fibration.

Prop. (3.11.1.4) [Pullback Bundle]. Let $\pi : E \to X$ be a fiber bundle with fiber $F$ and $f : Y \to X$ a map, then the pullback space $f^*E \to Y$ (3.6.1.7) is also a fiber bundle over $Y$ with fiber $F$, called the pullback bundle.

Prop. (3.11.1.5). If $E \to B, E' \to B'$ are fiber bundles both with compact Hausdorff fibers/or both with discrete fibers/, and $f : E/B \to E'/B'$ is a bundle map that induces isomorphisms on the fibers, then $E \cong f^*E'$ over $B$.

Proof: \qed

Lemma (3.11.1.6). Suppose $\pi : E \to B \times I$ is a fiber bundle whose restriction to $B \times [0,a]$ and $B \times [a,1]$ are all trivial for some $a \in I$, then $E \to B \times I$ is a trivial bundle.

Proof: Choose trivializations $\varphi_1 : B \times [0,a] \times B \times F \to \pi^{-1}(B \times [0,a])$, and $\varphi_2 : B \times [a,1] \times B \times F \to \pi^{-1}(B \times [a,1])$, then these induces a map

$$ B \times \{a\} \times F \xrightarrow{\varphi_1|} \pi^{-1}(B \times \{a\}) \xrightarrow{\varphi_2^{-1}} B \times \{a\} \times F, $$

of the form $(b,a,v) \mapsto (b,a,g(b)v)$, where $g : B \to \text{Homeo}(F)$ is continuous. Then we get a trivialization

$$ B \times I \times F \to E : \varphi(b,t,v) = \begin{cases} \varphi_1(b,t,v) & t \leq a \\ \varphi_2(b,t,g(b)v) & t \geq a \end{cases}. $$

\qed

Lemma (3.11.1.7). Let $E \to B \times I$ be a fiber bundle, then there exists a covering $\{U_i\}$ of $B$ that $E$ is trivial on each $U_i \times I$.
Prop. (3.11.1.13) [Ehresmann].

Lemma (3.11.1.8). Let \( \pi : E \to B \times I \) be a fiber bundle, where \( B \) is a paracompact space, and \( r : B \times I \to B \times I \) defined by \( r(b,x) = (b,1) \), then there exists a bundle morphism \( f \) over \( r \) that induces an isomorphism \( r^*E \cong E \) over \( B \times I \).

Proof: By (3.11.1.7), we can choose a covering \( \{U_\alpha\} \) of \( B \) that is \( E \) is trivial over each \( U_\alpha \times I \), and let \( \psi_\alpha \) be a partition of unity \( 1 = \sum \psi_i \) that \( \text{Supp}(\psi_i) \subset U_i \) and \( \{\text{Supp}(\psi_i)\} \) is locally finite. We also define \( \mu_\alpha(x) = \frac{\psi_\alpha(x)}{\max(\psi_\beta(x))} \), then \( \mu_\alpha \) are all continuous and subordinate to \( \{U_\alpha\} \), and for each \( x \in B, \max\{\mu_\alpha(x)\} = 1 \).

Let \( \varphi_\alpha : U_i \times I \times F \to \pi^{-1}(U_i \times I) \) be the local trivializations. We define a bundle map \( f_\alpha : E/B \times I \to E/B \times I \) by identity outside \( \pi^{-1}(U_i \times I) \) and \( f_\alpha(\varphi_\alpha(b,t,v)) = \varphi_\alpha(b,\max(\mu_\alpha(x),t),v) \), then \( f_\alpha \) is continuous and induces an isomorphism \( f_\alpha^*E \cong E \) over \( B \times I \). Now choose a well-ordering on \( \alpha \), by local finiteness, for each \( v \in E \), there is a nhhd \( W_v \times I \) of \( \pi(v) \in B \times I \) that \( W_v \cap U_\alpha \neq \emptyset \) for only \( \alpha \) in a finite set \( \{\alpha_1, \ldots, \alpha_m\} \) with \( \alpha_1 < \alpha_2 < \cdots < \alpha_m \). Then we define a bundle map \( f : E \to E \) that \( f|_{\pi^{-1}(W_v \times I)} = f_{\alpha_m} \circ \cdots \circ f_{\alpha_1} \). Then this is well-defined, and it is a bundle over \( r \) that induces an isomorphism \( r^*E \cong E \).

Prop. (3.11.1.9) [Homotopy Invariance of Fiber Bundles]. Let \( E' \to B' \) be fiber bundles. If \( f,g : B \to B' \) are two homotopic maps with \( B \) paracompact, then there is a bundle isomorphism \( f^*E' \cong g^*E' \).

Proof: Let \( F : B \times I \to B' \) be a homotopy from \( f \) to \( g \), and let \( i_v : B \to B \times I : i_v(b,x) = (b,v) \) for \( v = 0,1 \). Let \( r : B \times I \to B \times I \) be the retraction defined by \( r(b,x) = (b,1) \), then by (3.11.1.8), there is an isomorphism of fiber bundles

\[
f^*E' \cong (F \circ i_0)^*E' \cong i_0^*F^*E' \cong i_0^*\circ r^*F^*E' \cong i_1^*F^*E' \cong g^*E'.
\]

Prop. (3.11.1.10) [Cone Bundles]. Let \( E/X \) be a fiber bundle with fiber \( F \), then we can construct a new fiber bundle \( \text{Cone}(E)/X \) with bundle \( C(F) \).

Cor. (3.11.1.11). This is because we can use the transformation characterization to extend maps \( U_i \cap U_j \to \text{Aut}(F) \) to maps \( U_i \cap U_j \to \text{Aut}(C(F)) \).

Prop. (3.11.1.12) [Hopf Fibration]. There is a locally trivial fiber bundle \( S^3 \to S^2 \) with fiber \( S^1 \), called the Hopf fibration.

Proof: Cf. [AGP02] P129.

Prop. (3.11.1.13) [Ehresmann]. Let \( f : E \to B \in \text{Man}_{\text{sm}} \) be a proper submersion, then it is a locally trivial bundle.

Proof: Cf. [Björn Dundas, A Short Course in Differential Topology].

Cor. (3.11.1.14). There is a locally trivial bundle \( S^{2n-1} \to \mathbb{C}P^n \) with fiber \( S^1 \).

Proof:
Cor. (3.11.1.15). There is a locally trivial bundle $\mathbb{R}P^{2n-1} \to \mathbb{C}P^n$ with fiber $S^1$.

Proof: □

Prop. (3.11.1.16) [Classifying Space Bundles]. There is a locally trivial bundle $U(n,K) \to V_n(K^\infty) \to \text{Gra}(n,K^\infty)$ for $K = \mathbb{R}, \mathbb{C}$ or $\mathbb{H}$.

Proof: □

Cor. (3.11.1.17). There is a locally trivial bundle $S^\infty \to \mathbb{C}P^\infty$ with fiber $S^1$.

Prop. (3.11.1.18). There is a locally trivial bundle $S^n \to \mathbb{R}P^n$ with fiber $\{\pm 1\}$.

Proof: □

Prop. (3.11.1.19). There is a locally trivial fiber bundle $S^\infty \to \mathbb{R}P^\infty$ with fiber $\{\pm 1\}$.

Proof: Cf. [AGP02] P335.

Covering Space

Def. (3.11.1.20) [Covering Space]. A covering space is a fiber bundle $E \to X$ with discrete fibers.

Prop. (3.11.1.21). If $X$ and $Y$ are Hausdorff spaces, $f : X \to Y$ is a local homeomorphism, $X$ is compact, and $Y$ is connected, then $f$ a covering map.

Proof: First, $f$ is surjective (using the connectedness), and that for each $y \in Y$, $f^{-1}(y)$ is finite. Because $X$ is compact, there exists a finite open cover of $X$ by $\{U_i\}$ such that $f(U_i)$ is open and $f|_{U_i} : U_i \to f(U_i)$ is a homeomorphism. For $y \in Y$, let $\{x_1, \ldots, x_n\} = f^{-1}(y)$ (the $x_i$ all being different points). Choose pairwise disjoint neighborhoods $U_1, \ldots, U_n$ of $x_1, \ldots, x_n$, respectively (using the Hausdorff property).

By shrinking the $U_i$ further, we may assume that each one is mapped homeomorphically onto some neighborhood $V_i$ of $y$.

Now let $C = X \setminus (U_1 \cup \cdots \cup U_n)$ and set
\[ V = (V_1 \cap \cdots \cap V_n) \setminus f(C) \]

$V$ should be an evenly covered nbhd of $y$. □

Prop. (3.11.1.22). If $\pi : \tilde{B} \to B$ is a local onto homeomorphism with the property of lifting arcs. Let $\tilde{B}$ be arcwise connected and $B$ simply connected, then $\pi$ is a homomorphism.

Proof: only need to prove injective. If $p_1$ and $p_2$ map to the same point, then they can be connected, and the image is a loop thus contractable, contradiction. □

Cor. (3.11.1.23). If $\tilde{B}$ is locally arcwise connected and $B$ is locally simply connected, then $\pi$ is a covering map.

Proof: Choose the connected components of a simply connected nbhd of a point $p$ and use (3.11.1.22). □
Prop. (3.11.1.24) [Homotopy Lifting Property]. Given a covering space \( \pi : \tilde{X} \to X \), and a homotopy \( f_t : Y \to X \), and a map \( f_0 : Y \to \tilde{X} \) lifting \( X \), then there is a unique homotopy \( \tilde{f}_t : Y \to \tilde{X} \) of \( f_0 \) lifting \( f_t \).

**Proof:** Let \( U_\alpha \) be a covering of \( X \) that the We first construct a lift \( \tilde{F} : N \times I \to \tilde{X} \) for \( N \) a nbhd near some point \( y_0 \in Y \). Because \( f \) is continuous, there is a nbhd \( N \) of \( y_0 \) and a partition \( 0 = t_0 < t_1 < \ldots < t_m = 1 \) of \( I \) that each \( N \times [t_i, t_{i+1}] \) is mapped into some \( U_\alpha \). Then we can construct a lifting \( \tilde{F} : N \times I \to \tilde{X} \) by induction using the local homeomorphism property of covering space.

Next we show the uniqueness in the special case that \( Y \) is a point. This can also be done using a partition of \( I \) and induction.

Finally we can construct lifting near every point \( y \in Y \), and also they coincide on the overlap because of the uniqueness we just proved. So these liftings glue together to give a lifting \( \tilde{f}_t : Y \to \tilde{X} \).

□

Cor. (3.11.1.25). The map \( \pi_* : \pi_1(\tilde{X}, \tilde{x}_0) \to \pi_1(X, x_0) \) induced by the covering map is injective. And the image of this map consists of homotopy types of loops that based at \( x_0 \) whose lift starting at \( \tilde{x}_0 \) are also loops.

**Proof:** This is because a homotopy of a the image of a loop to trivial loop in \( \tilde{X} \) can be lifted to a homotopy of the loop itself to trivial loop. And this homotopy also fixes the endpoint, because the lifting of a trivial loop must be a trivial loop.

For the second assertion, one direction is easy, for the other, if a loop is a homotopic to the image of a loop of \( \tilde{X} \), then it is itself the image of a loop of \( \tilde{X} \).

□

Prop. (3.11.1.26) [Degree of a Covering]. Let \( \pi : \tilde{X} \to X \) be a covering map, then the cardinality of \( \pi^{-1}(x) \) is a a locally constant function of \( x \). Thus if \( X \) is constant, this cardinality is fixed for any \( x \in X \), and it is called the degree of the covering.

The number of sheets of a covering with \( \tilde{X} \) path-connected equals the index of \( \pi_*(\pi_1(\tilde{X}, \tilde{x}_0)) \) in \( \pi_1(X, x_0) \).

**Proof:** For a loop \( g \) in \( X \) based at \( x_0 \), let \( \tilde{g} \) be its lift to \( \tilde{X} \) starting at \( \tilde{x}_0 \). Now if \( h \in \pi_*(\pi_1(\tilde{X}, \tilde{x}_0)) \), then the loop \( h \cdot \tilde{g} \) has lift that has the same ending as \( \tilde{g} \). So we get a map from the quotient set \( \pi_1(X, x_0)/\pi_*(\pi_1(\tilde{X}, \tilde{x}_0)) \) to \( p^{-1}(x_0) \) mapping \( \pi_*(\pi_1(\tilde{X}, \tilde{x}_0)) \) to \( \tilde{g}(1) \). This map is injective, and it is surjective because \( \tilde{X} \) is path-connected. Then we are done.

□

Prop. (3.11.1.27) [Unique Lifting Property]. Let \( \pi : (\tilde{X}, \tilde{x}_0) \to (X, x_0) \) be a covering space and \( f : (Y, y_0) \to (X, x_0) \) be a map with \( Y \) path-connected and locally path-connected, then a lift \( \tilde{f} : (Y, y_0) \to (\tilde{X}, \tilde{x}_0) \) exists iff \( f_* (\pi_1(Y, y_0)) \subset \pi_* (\pi_1(\tilde{X}, \tilde{x}_0)) \). And when \( Y \) is connected, this lifting is unique.

In particular, a covering space has unique path lifting property.

**Proof:** One direction is clear, for the other, to construct a lifting, choose a path \( \gamma \) from \( y_0 \) to \( y \), the path \( f \gamma \) has a unique lifting \( \tilde{f} \gamma \) starting from \( \tilde{x}_0 \). Define \( \tilde{f}(y) = \tilde{f} \gamma \). This is a well-defined map: if \( \gamma' \) is another path from \( y_0 \) to \( y \), then \( f \gamma^{-1} f \gamma' \) is a loop that is homotopic to the image of a loop at \( \tilde{x}_0 \). Now we can lift this homotopy, and then \( f \gamma^{-1} f \gamma' \) is also the image of a loop at \( \tilde{x}_0 \), which must be \( \tilde{f} \gamma^{-1} \gamma' \) by uniqueness. So \( \tilde{f} \) is well-defined.

It can be verified that \( \tilde{f} \) is continuous.

The uniqueness is clear, because if there are two lifts, the points that they are equal and the points that they are not are both open in \( Y \).

□
Prop. (3.11.1.28) [Galois Theory of Covers]. Let $X$ be a path-connected and locally path-connected and semilocally simply-connected space (3.9.4.26), then
- there is a connected and simply-connected covering space $\tilde{X}$ of $X$, called a **universal cover** of $X$.
- The fundamental group acts continuously and properly on $\tilde{X}/X$.
- For any subgroup $H$ of $\pi_1(X,x_0)$, there is a connected covering space $\pi : X_H \to X$ that $\pi_* (\pi_1(X_H, \tilde{x}_0)) = H$ for a suitably chosen base point $\tilde{x}_0$. And this covering space is unique up to isomorphism over $(X, x_0)$. Thus by (3.11.1.27), there is an inclusion-preserving bijection between isomorphism classes of covering spaces over $X$ and the the set of conjugacy classes of subgroups of $\pi_1(X, x_0)$.

*Proof:* Cf. [Hat02] P64, P67. \square

Def. (3.11.1.29) [Normal Covering Spaces]. A **normal covering space** is a covering space $\pi : \tilde{X} \to X$ that for any $x \in X$ and two elements $\tilde{x}, \tilde{x}' \in \pi^{-1}(x)$, there is a covering isomorphism of $\tilde{X}/X$ taking $\tilde{x}$ to $\tilde{x}'$.

Prop. (3.11.1.30). Let $\pi : (\tilde{X}, \tilde{x}_0) \to (X, x_0)$ be a path-connected covering space of a path-connected, locally path-connected space $X$, and let $H$ be the subgroup $\pi_*(\pi_1(\tilde{X}, \tilde{x}_0)) \subset \pi_1(X, x_0)$, then
- The covering space is normal iff $H$ is normal in $\pi_1(X, x_0)$.
- The group $G(\tilde{X})$ of covering transformations of $\tilde{X}$ is isomorphic to $N(H)/H$.

*Proof:* 1: Let $\tilde{x}_1, \tilde{x}_2 \in \pi^{-1}(x_0)$ and $\gamma$ a path from $\tilde{x}_1$ to $\tilde{x}_2$ corresponding to an element of $\pi_1(X, x_0)$, then $H$ is normal is equivalent to $\pi_*(\pi_1(\tilde{X}, \tilde{x}_1)) = \pi_*(\pi_1(\tilde{X}, \tilde{x}_2))$. Then the lifting criterion shows there is a covering transformation taking $\tilde{x}_1$ to $\tilde{x}_2$. The converse is also true.

2: From the above argument, we can define a map $N(H) \to G(\tilde{x})$ by mapping a $\gamma \in N(H)$ to a covering transformation mapping $\tilde{x}_0$ to $\tilde{x}_1$. And the kernel of this map is exactly those $\gamma$ lifting to a loop at $\tilde{x}_0$, which are exactly the elements of $H$. \square

Prop. (3.11.1.31) [Covering Space Action]. If $G$ is a discrete group and $G \times Y \to Y$ is a covering space action (3.8.1.14), then the quotient map $Y \to Y/G$ is a normal covering space. And if $Y$ is path-connected, $G$ is the group of covering transformations.

*Proof:* The condition on the action shows it is locally a homeomorphism, thus it is a covering space. And it is a normal covering space because $g_1 g_2^{-1}$ takes any $g_1(x)$ to $g_2(x)$. The group of covering transformations is just $G$, because the covering transformation on a path-connected space is determined by its action on a single point. \square

2 Vector Bundles

Basics

Def. (3.11.2.1) [Vector Bundle]. Let $K = \mathbb{R}$ or $\mathbb{C}$, a **K-vector bundle** of dimension $n$ over a topological space $X$ is a fiber bundle over $X$ with fiber $K^n$ that each trivialization $\varphi_a$ restricts to $K$-linear isomorphisms on the fibers. The category of vector bundles over $X$ is denoted by $\text{Vect}_K(X)$. A **vector bundle homomorphism** $E \to F$ is a map of spaces over $X$ that the maps on the fibered are all $K$-linear.

Then a $K$-vector bundle of dimension $n$ over $X$ is just an associated $\text{GL}(n, K)$-bundle with fiber $K^n$ over $X$. In particular, there is a bijection $\text{Vect}_K^n(X) \cong \mathcal{O}_{\text{GL}(n, K)}(X)$ by (3.11.3.4).
Def. (3.11.2.2) [Trivial Vector Bundles]. For any \( n \in \mathbb{N} \), the trivial vector bundle of rank \( n \) is denoted by \( e^n \).

Prop. (3.11.2.3) [Constructions of Vector Bundles]. Let \( T : (\text{Vect}^f / \mathbb{K})^\otimes_n \rightarrow \text{Vect}^f / \mathbb{K} \) be a functor that is either covariant or contravariant for each of its factors in that \( T : \bigoplus_i \text{Hom}(V_i,W_i) \rightarrow \text{Hom}(T(V_i),T(W_i)) \) is continuous, then we have a functor \( T : \text{Vect}(X)^n \rightarrow \text{Vect}(X) \) that is either covariant or contravariant for each of its factors.


Cor. (3.11.2.4). In this way, given a vector bundles \( E, F \) on \( X \), we can construct
\[
E \oplus F, \quad E \otimes F, \quad \text{Hom}(E,F) \cong E^* \otimes F, \quad E^*, \quad T^n E, \quad \wedge^i E.
\]

Prop. (3.11.2.5) [Existence of Hermitian Metric]. There exists a Hermitian (Riemannian) metric on any bundle \( E \) over a paracompact space \( X \). In this way, \( E^* \cong E(\overline{E}) \).

Proof: Choose a metric on each trivialization open subset and use partition of unity to glue.

Cor. (3.11.2.6). A vector bundle over a paracompact space can have its transform maps \( \in O(n) \) (or \( U(n) \)).

Proof: We can choose the metric on it compatible with the given metric. In this way, the transform map is \( \in O(n) \) (or \( U(n) \)).

Cor. (3.11.2.7) [Semisimplicity of Vect(\( B \))]. Any exact sequence of vector bundles over a paracompact space \( B \) splits.

Proof: Because we can take the orthogonal complement.

Cor. (3.11.2.8). If \( f : X \rightarrow Y \) is a homotopy equivalence, then \( f^* : \text{Vect}(Y) \rightarrow \text{Vect}(X) \) is an isomorphism.

In particular, if \( X \) is contractible, then every bundle over \( X \) is trivial.

Def. (3.11.2.9) [Orientations of Vector Bundles]. Let \( \pi : E \rightarrow X \) be a vector bundle of rank \( n \) over a space \( X \) and \( R \cong \mathbb{Z} \) or \( \mathbb{Z} / 2\mathbb{Z} \), then a orientation of \( E \) with coefficient \( R \) is a functions that assigns a generator \( u_x \) of \( H^n(E_x, 0, R) \cong R \) for any \( x \in X \) s.t. for any \( x \in X \), there is a nbhd \( U \) of \( x \in X \) and an element \( u \in H^n(\pi^{-1}N, \pi^{-1}(N)_0, R) \) s.t. \( u \) pulls back to \( u_x \) via \( (E_x, 0) \subset (\pi^{-1}N, \pi^{-1}(N)_0) \) for any \( x \in U \). In particular, any vector bundle is \( \mathbb{F}_2 \)-orientable.

Prop. (3.11.2.10) [Orientation of Complex Vector Bundles]. For \( E / X \in \text{Vect}_C(X) \), the underlying real bundle has a preferred orientation, which is compatible with direct sums.

In particular, the tangent bundle of a complex manifold gives rise to a unique orientation of the underlying real manifold.

Proof: Let \( a_1, \ldots, a_\ell \) be a complex basis for \( E \), then take the real basis to be \( a_1, ia_1, \ldots, a_\ell, ia_\ell \). This orientation is stable under \( GL(\ell, \mathbb{C}) \) transformation, as \( GL(\ell, \mathbb{C}) \) is connected.

Prop. (3.11.2.11). If \( E \) is a complex vector bundle over \( X \), then \( E \otimes_{\mathbb{R}} \mathbb{C} \cong E \oplus \overline{E} \) as complex vector bundles.

Lemma (3.11.2.12). Suppose \( \pi : E \rightarrow B \times I \) is a fiber bundle whose restriction to \( B \times \{0, a\} \) and \( B \times \{a, 1\} \) are all trivial for some \( a \in I \), then \( E \rightarrow B \times I \) is a trivial bundle.
Proof: The proof is similar to that of (3.11.1.6)

Lemma (3.11.2.13). Let $E \to B \times I$ be a fiber bundle, then there exists a covering $\{U_i\}$ of $B$ that $E$ is trivial on each $U_i \times I$.

Proof: The proof is similar to that of (3.11.1.7)

Lemma (3.11.2.14). Let $\pi : E \to B \times I$ be a fiber bundle, where $B$ is a paracompact space, and $r : B \times I \to B \times I$ defined by $r(b, x) = (b, 1)$, then there exists a bundle morphism $f$ over $r$ that induces an isomorphism $r^*E \cong E$ over $B \times I$.

Proof: The proof is similar to that of (3.11.1.8)

Prop. (3.11.2.15) [Homotopy Invariance of Vector Bundles]. Let $E' \to B'$ be a vector bundle. If $f, g : B \to B'$ are two homotopic maps with $B$ paracompact, then there is a bundle isomorphism $f^*E' \cong g^*E'$.

Proof: The proof is similar to that of (3.11.1.9)

Bundles of Finite Type

Def. (3.11.2.16) [Bundles of Finite Type]. Let $X$ be a paracompact Hausdorff space, then a vector bundle of finite type over $X$ is a vector bundle over $X$ that has a covering by f.m. trivialization maps. The category of $k$-dimensional vector bundles over $X$ of f.t. is denoted by $\text{Vect}_k^f(X)$. Trivially, any vector bundle over a compact space is of f.t..

Prop. (3.11.2.17) [Vector Bundles on the Quotient]. Let $Y$ be a closed subspace of $X$, $E$ a vector bundle over $X$, then a trivialization $\alpha : E|_Y \cong Y \times V$ defines a bundle $E/\alpha$ over $X/Y$. The isomorphism class of $E/\alpha$ only depends on the homotopy type of $\alpha$.

Proof: To show it is a vector bundle, notice the trivialization $\alpha$ extends to a

Prop. (3.11.2.18) [Splitting Principle]. For a vector bundle $E \to X$, there is a space $Y \to X$ that $p^*$ is injective on $H^*(-, \mathbb{Z})$ and $p^*E$ splits as a sum of line bundles. This proposition is useful when proving theorems about characteristic classes.

Proof: It suffice to find a $Y$ that $p^*E$ has a subbundle, then choose its orthogonal part, and use induction. For this, choose $Y = P(E)$, then $Y$ has a tautological bundle, which is a subbundle of $p^*E$, and $Y$ is fibered over $X$ with fiber $\mathbb{P}^n$, and we want to use Leray-Hirsch, so check the fact $H^*(\mathbb{P}^n)$ is free and generated by the first Chern class, by (3.11.4.16) and (5.7.2.1). And Chern class is functorial, so the powers of Chern class of $f^*E$ will generate the cohomology ring of any stalks.

Prop. (3.11.2.19). For any bundle $E$ over a compact Hausdorff space $X$, there is a surjective bundle map $X \otimes \mathbb{R}^n \to E$ for some $m \geq 0$.

Proof: Choose a finite cover of trivialization of $E$, then we can glue these maps together via a partition function.

Cor. (3.11.2.20) [Negation of Bundles]. For any vector bundle $E$ on a compact space $X$, there is a vector bundle $F$ that $E \oplus F$ is a trivial bundle.
Prop. (3.11.2.23) [Constructing Vector Bundles].

Cor. (3.11.2.24). There is a natural isomorphism \( \text{Vect}_n(S(X)) \cong [X, GL(n, \mathbb{C})] \).

Proof: Write \( \Sigma(X) = C^+(X) \coprod C^-(X) \), and \( C^\pm(X) \) are both contractible, thus \( E \) are trivial restricted to them(3.11.2.8). Let \( \alpha^\pm \) be the trivialization isomorphism, then \( \alpha^+ \circ \alpha^- \) is a bundle map of \( X \times \mathbb{R}^n \), which is equivalent to a map \( \alpha : X \to GL(n, \mathbb{C}) \). The homotopy type of \( \alpha \) is determined because \( C^\pm(X) \) are both contractible, and vise versa.

Prop. (3.11.2.25) [Vector Bundles as Modules]. \( \Gamma \) induces an equivalence between the category of vector bundles over \( X \) and the category of finitely projective modules over \( C(X) \).

Proof: Clearly a bundle induces a module over \( C(X) \). And it is a fully faithful functor. Now the image is the subcategory of finite projective modules, because every bundle is a direct summand of a trivial bundle, and a trivial bundle corresponds to a finite free \( C(X) \)-modules.

Thom isomorphism

Prop. (3.11.2.26) [Thom Class]. Let \( R = \mathbb{Z} \) or \( \mathbb{F}_2 \) and an \( R \)-orientable vector bundle \( E \) over base \( B \) of rank \( n \).

Then there exists uniquely **Thom class** \( u_E \in H^n(E, E\backslash B, R) \) that induce the preferred generator \( H^n(E_x, E_x\backslash \{0\}, R)(3.11.2.9) \) on every fiber. Then the relative Leray-Hirsch will give an isomorphism

\[
\varphi_R : H^i(B, R) \cong H^{i+n}(E, E\backslash B, R) : x \mapsto \pi^*(x) \cup u_E.
\]

For \( \mathbb{F}_2 \) coefficient there exists a Thom class, and for orientable bundle there exists a \( \mathbb{Z} \)-Thom class. Notice that fiber bundle over a simply connected base is orientable.

Proof:

Cor. (3.11.2.27) [Naturality].

- Let \( B' \to B \) be a map and \( E/B \) be an \( R \)-orientable vector bundle, which induces a map \( f^* : H^n(E, E_0, R) \to H^n(f^*(E), E'_0, R) \). Then \( f^*u_E \cong u_{f^*(E)} \).
- The Thom class \( u_E \) maps to \( u_{E,2} \) under the change of coefficients \( \mathbb{Z} \to \mathbb{Z}/2\mathbb{Z} \).

Prop. (3.11.2.28). Similarly, for a orientable fiber bundle \( S^{n-1} \to E \to B \), make it a \( D^n \to E' \to B \) bundle, then \( E' \) is homotopy equivalent to \( B \) so there is a Gysin sequence

\[
\cdots \to H^{i-n}(B) \xrightarrow{\gamma^e} H^i(B) \to H^i(E) \to H^{i-n+1}(B) \to \cdots
\]

Where the Euler class \( e \) is chosen to commute with the Thom isomorphism.
Examples of Vector Bundles

Def. (3.11.2.29) [n-Universal \( k \)-Vector Bundle]. Let \( K = \mathbb{R} \) or \( \mathbb{C} \), endow \( \mathbb{K}^n \) with the canonical Hermitian metric, define \( E_k(\mathbb{K}^n) \) be the subspace of \( \text{Gra}(k, \mathbb{K}^n) \times \mathbb{K}^n \) consisting of pairs \((W, v)\) that \( v \in W \). Then this is a vector bundle over the Grassmannian \( \text{Gra}(k, \mathbb{K}^n) \) (11.6.2.12), called the \( n \)-universal \( k \)-vector bundles, or the tautological bundles.

Proof: We construct localization maps: endow \( \mathbb{K}^n \) with the natural metric. For \( W_0 \in G_k(\mathbb{K}^n) \), then the subspace \( U \) of \( G_k(\mathbb{K}^n) \) consisting of \( W \) that \( W \cap W_0^\perp = \emptyset \) is a nbhd of \( W_0 \), and it is naturally homeomorphic to \( \text{Hom}(W_0, W_0^\perp) \). There is an isomorphism

\[
\pi^{-1}(U) \cong U \times W_0 : (f, (f + id)w_0) \mapsto (f, w_0).
\]

Prop. (3.11.2.30) [Universal Vector Bundle]. Because by (3.11.3.20) \( E_k(\mathbb{K}^\infty) / \text{Gra}(k, \mathbb{K}^\infty) \) is the universal bundle, there is a map \( i_k : \text{Gra}(k, \mathbb{K}^\infty) \to \text{Gra}(k + 1, \mathbb{K}^\infty) \) s.t. \( i_k^*(E_{k+1}(\mathbb{K}^\infty)) \) is the bundle \( E_k(\mathbb{K}^\infty) \oplus \mathbb{K} \). Then it can be shown

\[
BU(\mathbb{K}) = \text{colim}_k (\text{Gra}(k, \mathbb{K}^\infty) \xrightarrow{i_k} \text{Gra}(k+1, \mathbb{K}^\infty))
\]

is a CW complex.

Moreover, there are maps \( w_{k,l} : \text{Gra}(k, \mathbb{K}^\infty) \times \text{Gra}(l, \mathbb{K}^\infty) \to \text{Gra}(k + l, \mathbb{K}^\infty) \) that corresponds to the bundle \( E_k(\mathbb{K}^\infty) \times E_l(\mathbb{K}^\infty) \), and these maps induces an H-space structure on \( BU \).

Proof:

Prop. (3.11.2.31) [Tautological Line Bundles]. For \( \text{Gra}(1, \mathbb{R}^{n+1}) \cong \mathbb{R}P^n \), the line bundle \( E_1(\mathbb{R}^{n+1}) \) is denoted by \( \gamma_n \).

Then the tangent bundle \( \tau_n \) of \( \mathbb{R}P^n \) is isomorphic to \( \text{Hom}(\gamma_n^1, \gamma_n^1) \), where \( \gamma_n^1 \) is the orthogonal complement of \( \gamma_n \) in \( e_{\mathbb{R}P^n}^{n+1} \) (with the canonical norm).

Proof: This is because a tangent vector at \( x \in \mathbb{R}P^n \) is equivalent to a homomorphism \([x] \) to \([x]^\perp \).

How to prove this rigorously.

Cor. (3.11.2.32). \( \tau_n \oplus e^1 \cong (\gamma_n^1)^{n+1} \).

Proof: By (3.11.2.31), \( \tau_n \oplus e^1 \cong \text{Hom}(\gamma_n^1, \gamma_n^1) \oplus \text{Hom}(\gamma_n^1, \gamma_n^1) = \text{Hom}(\gamma_n^1, \mathbb{R}^n) = (\gamma_n^1)^{\ast n} \). Then we are done because \( \gamma_n^{1\ast} \) is self-dual because it has a Euclidean metric (3.11.2.5).

Prop. (3.11.2.33) [Pullback the Universal Bundle]. For \( V \in \text{Vect}/\mathbb{K} \), for any continuous map \( \varphi : X \to \text{Gra}(k, V) \), we get a subspace \( E_\varphi = \{(x, v) \in X \times V | v \in \varphi(x)\} \subset X \times V \). This is a vector bundle over \( X \), and it is a subbundle of the trivial bundle \( X \times V \to X \). In fact, \( E_\varphi \cong f^*E_k(V) \) (3.11.2.29).

Cor. (3.11.2.34). Let \( f : X' \to X \) and \( \varphi : X \to Pr(V) \), then \( f^*(E_\varphi) = E_{\varphi \circ f} \).

Prop. (3.11.2.35) [Infinite Universal \( k \)-Vector Bundle]. The \( n \)-universal \( k \)-vector bundles \( E_k(\mathbb{K}^n) \) (3.11.2.29) for various \( n \) gets together to a bundle \( E_k(\mathbb{K}^\infty) \) on \( \text{Gra}(k, \mathbb{K}^\infty) \) that the pullback of \( E_k(\mathbb{K}^\infty) \) via \( i : \text{Gra}(k, \mathbb{K}^n) \to \text{Gra}(k, \mathbb{K}^\infty) \) is \( E_k(\mathbb{K}^n) \).

Def. (3.11.2.36) [Hopf Bundle]. Define a map \( \varphi : C^\mathbb{P}^n \to G_1(\mathbb{C}^{n+1}) \) that \( \varphi([z]) = [z] \), then this defines a vector bundle on \( C^\mathbb{P}^n \) by (3.11.2.33), called the dual of Hopf bundle. The Hopf bundle is defined to be the dual of the dual of Hopf bundle.
3 Principal Bundles

Main reference is [Principal Bundles and Classifying Space].

Def. (3.11.3.1) [Principal Bundles]. For $G \in \text{TopGrp}$, a principal $G$-bundle is a bundle $P$ with $G$-fibers that the transition function is right $G$-map, i.e. left multiplication by some $g_{\alpha\beta}$. A associated bundle of a representation $G \to \text{End}(V)$ is the total space of $P \times V$ module the equivalence $[gg_0, v] = [g, g_0v]$. The corresponding transition function is just the left action by $g_{\alpha\beta}$.

For $B \in \text{Top}$, denote $\mathcal{P}_G(B)$ the isomorphism classes of vector bundles on $B$.

Prop. (3.11.3.2) [Homogeneous Space]. For $G \in \text{LieGrp}$ and $H \leq G$ is a closed subgroup, then the quotient $H \backslash G$ can be given a structure of a $G$-homogeneous space and $G \to H \backslash G$ is a principal $H$-bundle.

Proof: □

Prop. (3.11.3.3). The projection $S^{2n+1} \to \mathbb{C}P^n$ is a principal $S^1$-bundle.

Proof: □

Prop. (3.11.3.4) [Associated Bundles]. If $G \in \text{TopGrp}$ and $G$ acts freely on $F \in \text{Top}$, then an associated $G$-bundle with fiber $F$ is a locally trivial $F$-bundles with a $G$-action. Then the isomorphism classes of associated $G$-bundles with fiber $F$ over $B$ is in bijection with $\mathcal{P}_G(B)$.

Proof: □

Classifying Space

Def. (3.11.3.5) [Classifying Spaces]. For $G \in \text{TopGrp}$, a classifying space of $G$ is a space $B(G) \in \text{Top}$ together with a principal $G$-bundle $E(G) \to B(G)$ s.t. $E(G)$ is contractible.

Notice $\pi_{n+1}(BG) = \pi_n(G)$ by ??.

Thm. (3.11.3.6) [Classifying Spaces and Principal Bundles]. If $G \in \text{TopGrp}$ and $E(G) \to B(G)$ is a classifying space for $G$, then for any $B \in \text{Top}$ that is paracompact, the pullback induces a bijection

$$[B, B(G)] \cong \mathcal{P}_G(B).$$

In particular, the classifying spaces is uniquely defined ique up to homotopy, if it exists.

Proof: ??

Prop. (3.11.3.7) [Classifying Spaces Exist]. For $G \in \text{TopGrp}$, define

$$E_n(G) \in s\text{Top} : E_n(G) = G^{n+1}$$

$$d_i((g_1, \ldots, g_{n+1})) = \begin{cases} (g_2, \ldots, g_{n+1}), & i = 0 \\ (g_1, g_{i-1}, g_i g_{i+1}, g_i g_{i+2}, \ldots, g_{n+1}), & 1 \leq i \leq n \end{cases}$$

$$s_i((g_1, \ldots, g_n)) = (g_1, \ldots, g_i, e, g_{i+1}, \ldots, g_n), \quad 0 \leq i \leq n$$

And

$$B_n(G) \in s\text{Top} : B_n(G) = G^n$$
Then there is a map
\[ \text{pr} : E_*(G) \to B_*(G) \in s\text{Top} : (g_1, \ldots, g_{n+1}) \in E_n(G) \mapsto (g_1, \ldots, g_n) \in B_n(G). \]
Denote \( E(G) = |E_*(G)|, B(G) = |B_*(G)|, \) then \( \text{pr} \) induces a map \( \text{pr} : E(G) \to B(G) \). \( B(G) \) is called the **classifying space** of \( G \).

**Cor. (3.11.3.8).** Any group \( G \) is a fundamental group of a topological space.

**Prop. (3.11.3.9).** Situation as in (3.11.3.7), there is a right action of \( G \) on \( E_*(G) \) on the last coordinates, which induces an action of \( G \) on \( E(G) \), and \( B(G) \cong E(G)/G \). Then if \((G, e)\) is well-pointed, \( E(G) \to B(G) \) is a locally trivial fiber bundle with fiber \( G \), and \( E(G) \) is contractible. In particular, \( G \cong \Omega(BG) \), by (3.9.6.20).

**Proof:** \( \square \). Cf.[Milnor, Construction of Universal Fiber Bundles, I, II].

**Cor. (3.11.3.10).** For \( G, G' \in \text{Top}_{s}\text{r} \),
\[ E(G \times G') \cong E(G) \times E(G'), \quad B(G \times G') \cong B(G) \times B(G'). \]

**Cor. (3.11.3.11).** If \( G \) is commutative, then \( G \times G \to G \) is a homomorphism that makes \( B(G) \) a commutative topological group. Then we can define for any \( n \in \mathbb{N} \),
\[ B(G, n) = B^0(G). \]

**Prop. (3.11.3.12).** \( [X, BG] \cong G \)-bundles on \( X \). And \( BG \) is Abelian if \( G \) is Abelian. Thus the classifying space \( BG \) is unique up to homotopy equivalence because they all represent the functor from the CW homotopy category to the set of \( G \)-bundles on it.

**Proof:** Cf.[Principal Bundles and Classifying Space P13]. \( \square \)

**Prop. (3.11.3.13)[Examples of Classifying Spaces].**
- \( B(\mathbb{Z}/n\mathbb{Z}) \cong S^\infty / (\mathbb{Z}/n) = (\mathbb{C}^\infty \backslash \{0\}) / (\mathbb{R}^+ \times \mu_n)(3.9.3.17) \). In particular, \( B(\mathbb{Z}/2) \cong \mathbb{R}P^\infty (3.9.3.19) \).
- \( BSU(2, \mathbb{R}) = \mathbb{H}P^\infty \).
- \( B(\mathbb{T}^g) \times \mathbb{T}^1 \) because \( \mathbb{R} \to \mathbb{T}^1 \) is a universal cover, this can be seen observing only \( \mathbb{R} \) has to satisfy the sum of inner angle is \( \pi \).
- \( BO(n), BU(n), BSp(n) \) are respectively the infinite Grassmannians \( \text{Gra}(n, \mathbb{R}^\infty), \text{Gra}(n, \mathbb{C}^\infty), \text{Gra}(n, \mathbb{H}^\infty) \), because there is a locally trivial fiber bundle (3.11.1.16) \( U(n, K) \to V_n(K^\infty) \to \text{Gra}(n, K^\infty) \), and \( V_n(K^\infty) \) is contractible (3.9.3.18). In particular, \( B(\mathbb{Z}/2) = \mathbb{R}P^\infty \) and \( BS^1 = \mathbb{C}P^\infty \).

**Proof:** \( \square \)
Def. (3.11.3.14) [Admissible Subgroups]. A subgroup of a topological group $G$ is called **admissible** if $G \to G/H$ is a principal $H$-bundle. In particular, this is the case for $G \in \text{LieGrp}$ and $H \leq G$ closed, by (3.11.3.2).

Prop. (3.11.3.15). If $H$ is an admissible subgroup of $G$, then there is a homotopy fiber sequence $G/H \to BH \to BG$.

*Proof:* Cf. [Principal Bundles and Classifying Space P22].

Cor. (3.11.3.16). There are homotopy equivalences $\Omega BK \cong K$ and $B\Omega K \cong K$.

Prop. (3.11.3.17). If $H$ is an admissible normal subgroup of $G$, then there is a homotopy fiber sequence $BH \to BG \to B(G/H)$.

*Proof:* 

Cor. (3.11.3.18).
- there are fiber bundles $S^0 \to BSO(n) \to BO(n)$ and similarly for $BSU(n)$ and $BSp(n)$.
- there are fiber bundles $S^n \to BO(n) \to BO(n + 1)$.
- there are fiber bundles $U(n)/T^n \to (\mathbb{C}P^\infty)^n \to BU(n)$, where $U(n)/T^n$ is the variety of complete flags in $\mathbb{C}^n$.
- for a discrete group $H \subset G$, $BH \to BG$ is a covering map.
- there are fiber bundles $BSO(n) \to BO(n) \to \mathbb{RP}^\infty$ and similarly for $\mathbb{C}$ and $\mathbb{H}$.
- there are fiber bundles $\mathbb{RP}^\infty \to B\text{Spin}(n) \to BSO(n)$.

*Proof:* These are all classifying spaces of Lie groups.

Prop. (3.11.3.19) [Classifying Line Bundles]. Note that $K(\mathbb{Z}, 2) = \mathbb{CP}^\infty = B(K(\mathbb{Z}, 1)) = BU(1)$ (3.11.3.13), thus we have a bijection $H^2(X, \mathbb{Z}) \cong [X, K(\mathbb{Z}, 2)] \cong \text{Vect}_\mathbb{C}^1(X)$. Similarly, we have a bijection $H^1(X, \mathbb{Z}/2\mathbb{Z}) \cong \text{Vect}_\mathbb{R}^1(X)$.

**Classifying Spaces**

Prop. (3.11.3.20) [Universal Real Bundle]. Let $X$ be paracompact, then there is a natural bijection

$$ [X, \text{Gra}(k, K^\infty)] \to \text{Vect}_\mathbb{R}^1(X) : f \mapsto f^*E_k(K^\infty).$$

*Proof:* Because $E$ is of f.t., we can find a f.d. vector space $W$ with a metric and a vector bundle epimorphism $\varphi : X \times W \to E$ via partition of unity. Then we can take the map $\varphi : X \to G_k(W) : x \mapsto \ker(\varphi_x)^\perp$. Then $f^*E_k(K^\infty) \cong E$ via restriction of $\varphi$. The last assertion follows from the definition of $E_k(K^\infty)$ (3.11.2.35) and (3.11.2.15). Cf. [AGP02] P284.

Cor. (3.11.3.21). By (3.10.6.13), there are isomorphisms

$$ \text{Vect}_\mathbb{R}^1(X) \cong [X, \text{Gra}(1, K^\infty)] = [X, K(\mathbb{Z}/(2), 1)] = H^1(X, \mathbb{F}_2). $$

$$ \text{Vect}_\mathbb{C}^1(X) \cong [X, \text{Gra}(1, \mathbb{C}^\infty)] = [X, K(\mathbb{Z}, 2)] = H^2(X, \mathbb{Z}). $$
Cohomology of Classifying Spaces

Prop. (3.11.3.22). $H_*(BG, \mathbb{Z}) \cong H_*(\Lambda, \mathbb{Z})$ and $H^*(BG, \mathbb{Z}) \cong H^*(G, \mathbb{Z})$.

Proof: Because $EG$ is weakly contractible, $S_*(EG)$ is a free $\mathbb{Z}[G]$-module resolution of $\mathbb{Z}$ and $S_*(EG)_G$ is identified with $S_*(BG)$. The rest is easy. □

Def. (3.11.3.23) [Whitney Sums].

Prop. (3.11.3.24). The diagonal map $(\mathbb{R}P^\infty)^n \to O(n)$ induces a map

$$\omega : (\mathbb{R}P^\infty)^n \cong (BO(1))^n \to BO(n).$$

The conjugation by permutation matrices preserves $O(1)^n$, thus induces a covariant action on this map. The action on $BO(n)$ is identity?, and the action on $(BO(1))^n$ is by permutation.

Then it induces a map

$$H^*(BO(n)) \to H^*((BO(1))^n)^{\Delta_n} \cong F_2[\sigma_1, \sigma_2, \ldots, \sigma_n]$$

where $\sigma_i$ are the elementary symmetric functions. This is injective and thus surjective when tensoring any field, thus it is a bijection?.

Denote the inverse image of $\sigma_i$ by $w_i$, then

$$H^*(BO(n)) \cong F_2[w_1, \ldots, w_n], \quad |w_i| = i$$

and these elements satisfy

- $c_0 = 1$.
- $i_1^*(c_1)$ is the canonical generator of $H^2(BU(1))$.
- $i_n^*(w_i) = c_i$.
- $p^*(w_i) = \sum_{j=0}^i w_j \otimes w_{i-j}$.

Proof: Cf. [Cohomology of Classifying Space Toda P82]. □

Prop. (3.11.3.25) \[H^*(BSO(n), F_2), \text{pr : } BSO(n) \to BO(n) \text{ is the universal covering with fiber} \]

$$\mathbb{Z}/(2), \text{ and}$$

$$H^*(BSO(n), F_2) \cong F_2[pr^* \omega_2, \ldots, pr^* \omega_n].$$

Proof: □

Prop. (3.11.3.26). The diagonal map $U(1)^n \to U(n)$ induces a map

$$\omega : (\mathbb{C}P^\infty)^n \cong (BU(1))^n \to BU(n).$$

The conjugation by permutation matrices preserves $U(1)^n$, thus induces a covariant action on this map. The action on $BU(n)$ is identity?, and the action on $(BU(1))^n$ is by permutation.

Then it induces a map

$$H^*(BU(n)) \to H^*((BU(1))^n)^{\Delta_n} \cong \mathbb{Z}[\sigma_1, \sigma_2, \ldots, \sigma_n]$$
where $\sigma_i$ are the elementary symmetric functions. This is injective and thus surjective when tensoring any field, thus it is a bijection.

Denote the inverse image of $\sigma_i$ by $c_i$, then

$$H^*(BU(n)) \cong \mathbb{Z}[c_1, \ldots, c_n], \quad |c_i| = 2i$$

and these elements satisfy

- $c_0 = 1$.
- $i_1^*(c_1)$ is the canonical generator of $H^2(BU(1))$.
- $i_n^*(c_i) = c_i$.
- $p^*(c_i) = \sum_{j=0}^i c_j \otimes c_{i-j}$.

**Proof:** Cf. [Cohomology of Classifying Space Toda P81].

**Prop. (3.11.3.27).**

$$H^*(BO(2n), \mathbb{Z}[\frac{1}{2}]) \cong H^*(BO(2n+1), \mathbb{Z}[\frac{1}{2}]) \cong H^*(BSO(2n+1), \mathbb{Z}[\frac{1}{2}]) = \mathbb{Z}[\frac{1}{2}][p_1, p_2, \ldots, p_n], \quad |p_i| = 4i$$

Cf. [Cohomology of Classifying Space Toda P81].

**Prop. (3.11.3.28)[Complexifications].** As $BSO(n)$ is the set of oriented real $n$-planes in $\mathbb{R}^\infty$, $BU(n)$ is the set of complex $n$-planes in $\mathbb{C}^\infty$, regarding a complex $n$-plane as an oriented real $2n$-plane induces a map

$$r : BU(n) \to BSO(2n).$$

And complexification of a real plane induces a map

$$e : BO(n) \to BU(n).$$

Then

$$p_k = (-1)^k e^*(c_{2k}) \in H^{4k}(BO(n)), \quad e^*(c_k) = w_k^2 \in H^{2k}(BO(n), F_2), \quad p_k = w_{2k}^2 \in H^{4k}(BO(n), F_2)$$

$$r^*(w_{2k}) = c_k \in H^{2k}(BU(n), F_2), \quad r^*(e) = c_n \in H^{2n}(BU(n)).$$

Cf. [Cohomology of Classifying Space Toda P81].

4 Characteristic Classes

References are [Cohomology of Classifying Space, Toda], [May99] and [M-S74].

**Def. (3.11.4.1) [Characteristic Classes].** For an ES-cohomology theory $E^*$, $p \in \mathbb{Z}, n \in \mathbb{N}$, a characteristic class functor of degree $p$ for $n$-dimensional K-bundles is a natural assignment $c : \text{Vect}_k^n(X) \to E^p(X)$ for any $X \in \text{Top}$ paracompact that is functorial w.r.t. pullbacks.

By (3.11.3.20), there is a bijection between characteristic class functors of degree $p$ with elements in $E^p(BO(n))$. 
Stiefel-Whitney Classes

**Def. (3.11.4.2) [Stiefel-Whitney Classes].** A Stiefel-Whitney class functor $w$ for real bundles is a total characteristic class functor for real bundles for the ordinary cohomology theory with $F_2$ coefficients $H^*(-, F_2)$ that satisfies:

- $w(E) = 1 + w_1(E) + \ldots + w_n(E) \in H^*(X, F_2)$, $|w_i| = i, n = \text{rank}(E)$.
- $f^*(w(E)) = w(f^*(E))$.
- $w(E \oplus F) = w(E)w(F)$.
- On the tautological bundle $\gamma_1^1$ over $RP^1$, $w(\gamma_1^1) = 1 + w_1(\gamma_1^1)$ and $w_1(\gamma_1^1)$ is the unique non-trivial element in $H^1(RP^1, F_2)$.

**Prop. (3.11.4.3) [Existence and Uniqueness of Stiefel-Whitney Classes].** There exists uniquely a Stiefel-Whitney class functor, and they can be defined using the Thom isomorphism

$$\varphi_E : H^i(B; F_2) \cong H^{i+n}(E, E \backslash B; F_2) \quad (3.11.2.26)$$

as

$$w(E) = \varphi^{-1}_E Sq(\varphi_E(1)) \in H^*(B; F_2) = \varphi^{-1} Sq(u_E).$$

**Proof:** Cf.[May, P191] and [Milnor, P92].

**Prop. (3.11.4.4).** For $B \in \text{Top}$ paracompact, $E, E' \in \text{Vect}_R(B)$, then

- If $E$ is trivial, $w(E) = 1$.
- If $E \oplus E'$ is trivial, then

$$w(E') = w(E)^{-1} = 1 + w_1 + (w_1^2 + w_2) + (w_1^3 + w_3) + (w_1^4 + w_1^2w_2 + w_2^2 + w_4) + \ldots.$$  

- Let $\gamma_1^n$ be the tautological line bundle over $RP^n \quad (3.11.2.31)$, then $w(\gamma_1^n) = 1 + a$.
- Let $\xi, \eta$ be vector bundles on $M, N$, then

$$w(\xi \times \eta) = \pi_1^\ast w(\xi) \cup \pi_2^\ast w(\eta) = w(\xi) \times w(\eta)$$

in $H^*(M \times N, F_2)$.

**Proof:** 1: A trivial bundle is the pullback of a bundle over pt, thus $w(f^*(E)) = w^*(e(E)) = 1$.

2: This is trivial.

3: This is because $E_1(R)/RP^1 \to E_1(R^n)/RP^n$ is a bundle map, thus $w_1(E_1(R^n))$ pulls back to $w_1(E_1(R)) \neq 0$, thus $w_1(E_1(R^n)) = a$.

4: This follows from the definition that $\xi \times \eta = \pi_1^\ast \xi \oplus \pi_2^\ast \eta$ and Kunneth formula(3.10.2.13).

**Cor. (3.11.4.5) [Tangent and Normal Bundles].** Let $M$ be a submanifold of a smooth manifold $N$, let $T_M, T_N$ be the tangent bundles and $\nu$ the normal bundle, then

$$w(N_{M/N}) = w(T_N)w(T_M)^{-1}$$

**Proof:** This follows form the smooth nbhd theorem ?.

\[\square\]
Prop. (3.11.4.6) [Wu Formula]. For $E \in \text{Vect}_B$,

$$\text{Sq}^i(w_j) = \sum_{t=0}^{i} \binom{j+t-i-1}{t} w_{i-t} w_{i+t}$$

Proof: Use splitting principle.

Def. (3.11.4.7) [Characteristic Classes of Smooth Manifolds]. For $M \in \text{Mani}_{\text{sm}}$, denote $w(M) = w(TM)$.

Prop. (3.11.4.8) [Wu Formula]. For $M \in \text{Mani}_{\text{sm, cpt}}$, define the Wu class $\nu(M) = \sum v_i \in H^*(M, \mathbb{F}_2)$ s.t.

$$\langle \nu(M) \cup x, [M]_2 \rangle = \langle \text{Sq}(x), [M]_2 \rangle$$

for any $x \in H^*(M, \mathbb{F}_2)$. In particular, $\nu_k(M)_k \cup x = \text{Sq}^k(x)$ for any $x \in H^{d-k}(M, \mathbb{F}_2)$. Notice such a class exists by Poincaré duality.

Then the Stiefel-Whitney class of $M$ is given by the Wu class:

$$w(M) = \text{Sq}(\nu(M)) \tag{3.10.6.14}$$

Proof: Cf. [Milnor, P132].

Cor. (3.11.4.9) [Homotopy Invariance of Stiefel-Whitney Classes of Manifolds]. The Stiefel-Whitney classes only depends on the homotopy type of $M$, and pullbacks of Stiefel-Whitney classes along smooth maps between smooth manifolds only depends on the homotopy type of the map.

Def. (3.11.4.10) [Stiefel-Whitney Numbers]. Let $M$ be a closed smooth manifold of dimension $n$, then for each tuple $(i_1, \ldots, i_k)$ with $i_1 + \ldots + i_k = n$, define the Stiefel-Whitney number

$$w_{i_1, \ldots, i_k}(M) = (w_{i_1}(TM) \cup \ldots \cup w_{i_k}(TM), [M]) \in \mathbb{Z}/2\mathbb{Z}.$$

Euler Classes

Def. (3.11.4.11) [Euler Classes]. Axioms for Euler classes for orientable real bundles $E/B$:

- $e(e^1) = 0$.
- For any map $f : B' \to B$, $f^*(e(E)) = e(f^*(E))$.
- $e(E \oplus F) = e(E)e(F)$.
- For the opposite orientation $-E$, $e(-E) = -e(E)$.

Prop. (3.11.4.12) [Existence of Euler Classes]. For any oriented $E/B \in \text{Vect}_B$, let $e(E)$ be defined as the image of the Thom class (3.11.2.26) under the maps

$$\varphi_E^{-1} : H^n(E, E_0, \mathbb{Z}) \to H^n(E, \mathbb{Z}) \cong H^n(B, \mathbb{Z}).$$

or equivalently, $e(E) = \varphi^{-1}(u_E \cup u_E)$ where $u_E$ is the Thom class and $\varphi$ is the Thom isomorphism (3.11.2.26). Then it is the desired Euler class.
Proof: ?
1: If $E$ has a non-zero section $s : B \to E_0$, then $B \xrightarrow{s} E_0 \subset E \to B$ is identity, thus

$$H^n(B) \xrightarrow{\pi^*} H^n(E) \to H^n(E_0) \xrightarrow{s^*} H^n(B)$$

is the identity. But $H^n(B) \xrightarrow{\pi^*} H^n(E) \to H^n(E_0)$ equals the restriction of $u_E$ to $E_0$, which is 0.
2: This $e(E)$ is compatible with base change by (3.11.2.27) and the definition.
3: For products, Cf.[Milnor, P100].
4: If the orientation is reversed, then $u_{-E} = -u_E$. \hfill \Box

Cor. (3.11.4.13).
- For a trivial line bundle, $e(E) = 0$.
- For an odd dimensional vector space $E/B$, $2e(E) = 0$.

Proof: 1: A trivial bundle is the pullback of a bundle over pt, thus $e(f^*(E)) = f^*(e(E))$ is trivial.
2: This is because their is an orientation preserving isomorphism $(-1) : E/B \cong (-E)/B$ that is isomorphism on the base, so $e(-E) = e(E)$. \hfill \Box

Cor. (3.11.4.14)[Euler classes and Whitney Classes]. For a vector bundle $E/B$ of rank $n$, the natural map $H^n(B, \mathbb{Z}) \to H^n(B, \mathbb{Z}/2\mathbb{Z})$ maps the Euler class $e(E)$ to the top Whitney class $w_n(E)$.

Proof: $e(E) = \varphi^{-1}(u_E \times u_E)$, which maps to $\varphi_2^{-1}(u_{E,2} \cup u_{E,2}) = \varphi_2^{-1}(Sq^n(u_{E,2})) = w_n(E)$ by (3.11.2.27). \hfill \Box

Prop. (3.11.4.15)[Euler Class and Euler Characteristic]. For $M \in \text{Man}_{\text{cpt}, \text{sm}, \text{orntd}}$, then

$$\langle e(T_M), [M] \rangle = \chi(M).$$

Proof: ? \hfill \Box

Chern Classes

Def. (3.11.4.16)[Chern Classes], Axioms for Chern classes for complex bundles:
- $c(E) = 1 + c_1(E) + \ldots + c_n(E) \in H^*(X, \mathbb{Z})$, \quad $|c_i| = 2i, n = \deg(E)$.
- $f^*(c(E)) = c(f^*(E))$.
- $c(E \oplus F) = c(E)c(F)$.
- For the tautological bundle $\eta$ over $\mathbb{CP}^\infty$, $c_1(\eta)$ corresponds to the element $\text{id} \in [\mathbb{CP}^\infty, \mathbb{CP}^\infty] \cong H^2(\mathbb{CP}^\infty)$.

Prop. (3.11.4.17). There exists uniquely a natural transformation $c : \text{Vect}_C(X) \to H^*(X, \mathbb{Z})$ satisfying these axioms. (For this, it suffice to calculate the cohomology ring of $BGL_n(\mathbb{C})$, Cf.[Cohomology of Classifying Space Toda]).

Cor. (3.11.4.18). For a trivial bundle $E = \mathbb{C}$, $c_i(E) = 0$ for $i > 0$, because $E$ is a pullback from a bundle on pt.

In particular, for any complex vector bundle $E$, $c(E \oplus \mathbb{C}) = c(E)$.
Prop. (3.11.4.19) [First Chern Class Map]. A complex line bundle can be seen as an element of $H^1(X, \mathbb{C}^\ast)$, by (5.3.2.14), by the exact sequence

$$0 \to \mathbb{Z} \to \mathbb{C} \xrightarrow{\exp(2\pi i - )} \mathbb{C}^\ast \to 0$$

($\mathbb{C}$ is sheaf of smooth functions from $X$ to $\mathbb{C}$) which gives a map $H^1(X, \mathbb{C}^\ast) \to H^2(X, \mathbb{Z})$, called the first Chern class map. It is called so because it gives the first Chern class of this complex line bundle. It is also an isomorphism because $\mathbb{C}$ is fine sheaf so acyclic.

Proof: Only have to prove they are equal in $H^2(X, \mathbb{C})$. We choose a totally convex covering $U_i$ of $X$ by (11.2.3.21), then it is a fine cover, so by (5.3.2.15) the Čech cohomology and sheaf cohomology equal.

Use the Chern-Weil map definition of the Chern class, a connection on a line bundle satisfies $\nabla e_\alpha = \omega_\alpha e_\alpha$, and if $e_\beta = e_\alpha g_{\alpha \beta}$, then $\omega_\beta = g_{\alpha \beta}^{-1} \omega_\alpha g_{\alpha \beta} + g_{\alpha \beta}^{-1} \omega_{\alpha \beta} = \omega_\alpha + d(\log g_{\alpha \beta})$. So $\Omega_\alpha = d\omega_\alpha$ locally, and the first Chern class is giving by $\Omega_\alpha$ in $H^2(X, \mathbb{C})$.

Then we need to understand the deRham isomorphism. For the exact sequence $0 \to \mathbb{C} \to \mathcal{A}^0 \to \mathcal{A}^1 \to \ldots$, it has a splitting: $0 \to \mathbb{C} \to \mathcal{K}^1 \to 0$ and $0 \to \mathcal{K}^1 \to 0 \to \mathcal{A}^1 \to \mathcal{K}^2 \to 0$, this gives

$$0 \to H^1(X, \mathcal{K}^1) \xrightarrow{\delta} H^2(X, \mathbb{C}) \to 0, \quad \mathcal{A}^1(X) \to \mathcal{K}^2(X) \xrightarrow{\delta} H^1(X, \mathcal{K}^1) \to 0.$$

because $\mathcal{A}^k$ are fine sheaves. The composite of them is just the de Rham isomorphism (Here we are identifying $H^2(X, \mathbb{C})$ to $H^2(X, \mathbb{C})$ by (5.3.5.9)). Tracking the lifting, we notice $\Omega$ is mapped to the cocycle $\{\log g_{\alpha \beta} + \log g_{\beta \gamma} - \log g_{\alpha \gamma}\}$, which is exactly the image of the first Chern class map. $\square$

Cor. (3.11.4.20). Complex line bundles are characterized by the first Chern class up to smooth isomorphism, because $H^1(X, \mathbb{C}^\ast) \to H^2(X, \mathbb{Z})$ is an isomorphism.

Pontryagin Classes

Def. (3.11.4.21) [Pontryagin Classes]. The Pontryagin classes are defined as $p_k(E) = (-1)^k c_{2k}(E_C) \in H^{4k}(X, \mathbb{Z})$.

Def. (3.11.4.22) [Pontryagin Number]. Let $M$ be a closed manifold of dimension $4n$, then for each tuple $I = (i_1, \ldots, i_k)$ with $i_1 + \ldots + i_k = n$, define the Pontryagin numbers

$$p_I(M) = (p_{i_1}(TM) \cup \ldots \cup p_{i_k}(TM), [M]) \in \mathbb{Z}.$$

Prop. (3.11.4.23) [Pontryagin Number of Product Manifolds]. Let $M, N$ be closed submanifolds of dimension $4m, 4n$ resp., then for any tuple $I = (i_1, \ldots, i_k)$ with $i_1 + \ldots + i_k = m + n$,

$$p_I(M \times N) = \sum_{I_1, I_2 | I_1 + I_2 = I} p_{I_1}(M)p_{I_2}(N)$$

where the summation is over all partitions $I_1, I_2$ of $m, n$ resp..

Proof: Cf. [Milnor, P193]. $\square$

Combinatorial Pontryagin Classes

Calculations and Applications

Prop. (3.11.4.24). \( w(\mathbb{R}P^n) = (1 + a)^{n+1} \). In particular, \( w(\mathbb{R}P^n) = 1 \) iff \( n = 2^k - 1 \) for some \( k \).

Proof: This follows from (3.11.2.32).

\[ \square \]

Cor. (3.11.4.25). Let \( n = 2^k - 1 - r \), where \( r \leq 2^{k-1} - 1 \), then \( \mathbb{R}P^n \) can be immersed into \( \mathbb{R}^{n+d} \) iff \( d \geq r \).

Proof: By (3.11.4.5), the normal bundle \( \nu \) satisfies \( w(\nu) = (1+a)^r \), and \( r < n \), thus \( d = \text{rank}(\nu) \geq r \).

\[ \square \]

Cor. (3.11.4.26). If \( n + 1 = 2^r m \), then there doesn’t exist \( 2^r \)-linearly independent vector fields on \( \mathbb{R}P^n \).

Proof: This is because if their is, then \( w(\mathbb{R}P^n) \) has degree \( \leq n - 2^r = 2^r(m - 1) - 1 \), but in fact it equals \((1 + a^2)^m\) has leading term \( a^{2^r(m-1)} \).

\[ \square \]

Remark (3.11.4.27). By considering irreducibility, we can prove stronger results, like \( \tau_{\mathbb{R}P^4} \) doesn’t contain a subbundle of rank 2.

Prop. (3.11.4.28)[Non-Vanishing Vectors]. \( \mathbb{R}P^n \) admits a non-vanishing vector field iff \( n \) is odd.

Proof: If \( n = 2k + 1 \), consider the non-vanishing vector field on \( S^{2k+1} : (x_1, \ldots, x_{2k+2}) \mapsto (x_2, -x_1, x_4, -x_3, \ldots, x_{2k+2}, -x_{2k+1}) \). Then This descends to a non-vanishing vector field on \( \mathbb{R}P^{2k+1} \). Conversely, if \( n = 2k \), by (3.11.4.26), there doesn’t exist a non-vanishing vector field on \( \mathbb{R}P^{2k} \).

\[ \square \]

5 K-Theory

Def. (3.11.5.1) [Topological K-Groups]. For \( X \in \text{Top}_{\text{cpt}} \), the K-group \( K(X) \) is defined to be \( K_0(\text{Vect}(X))(3.3.1.25) \), which is a ring under sum and tensor. Two vector bundles \( E, F \) are called stably equivalent if \( [E] = [F] \).

There is a degree map \( \deg K(X) \to \mathbb{Z} \), and the kernel is denoted by \( \tilde{K}(X) \). There is a canonical splitting \( K(X) \cong \tilde{K}(X) \oplus \mathbb{Z} \).

Prop. (3.11.5.2). A continuous map \( f : X \to Y \) induces a group morphism \( f^* : K(Y) \to K(X) \).

By (3.11.1.9), this map only depends on \( f \in [X, Y] \).

Prop. (3.11.5.3). By (3.11.2.20), over a compact Hausdorff space, \( E, F \) is stably equivalent iff \( E \oplus \mathbb{R}^n \cong F \oplus \mathbb{R}^n \) for some \( n \).

Thm. (3.11.5.4) [Periodicity Theorem]. Let \( L \) be a line bundle over \( X \), then as a \( K(X) \)-algebra, \( K(P(L \oplus 1)) \) is generated by \([H]\), and is subject to the single relation \( ([H] - [1])([L][H] - [1]) = 0 \).

Proof: Cf.[K theory, Atiyah, P46].

\[ \square \]

Cor. (3.11.5.5). \( K(S^2) \) is generated by \([H]\) as a \( K(\text{pt}) \)-module, and is subject to the single relation \( ([H] - [1])^2 = 0 \).

Cor. (3.11.5.6). There is an isomorphism \( \mu : K(X) \otimes K(S^2) \to K(X \times S^2) \), where \( \mu(a \otimes b) = (\pi_1^*a)/(\pi_2^*b) \).
Def. (3.11.5.7) [Setup for Proof of Periodicity Theorem]. Given a line bundle $E$ over $X$, we can associate a projective bundle $P(E)$ that $P(E)_x = P(E_x)$. Now denote $P^0$ the subspace of $P(E)$ consisting of all vectors of length $\leq 1$ and $P_\infty$ the subspace consisting of all vectors of length $\geq 1$ together with the infinity section. There are projections $\pi_0 : P_0 \to X$ and $\pi_\infty : P_\infty \to X$, which are homotopy equivalences.

Now by (3.11.2.8),

6 Adam Operators

7 Cobordism

Def. (3.11.7.1) [Bordism Groups]. If $X$ is a topological space, define the bordism group $\Omega_n(X)$ to be the set of pairs $(M, f)$ where $M$ is a closed smooth manifold of dimension $n$ and $f : M \to X$ is a continuous map, under the equivalence relation that $(M_0, f_0) \sim (M_1, f_1)$ iff there is an $n + 1$ manifold $N$ and a map $F : N \to X$ that $\partial F = f_1 \amalg f_2$. This is a vector space over $F_2$.

Let $\Omega = \Omega_0(pt)$, then for any $m, n$, there is a map $\Omega_m \times \Omega_n \to \Omega_{m+n} : (M, N) \mapsto M \times N$, so $\Omega_*$ is a graded commutative ring.

Prop. (3.11.7.2) [Thom]. If $N \in \text{Mani}_{s^m,\text{cpt}}^{n+1}$ and $\partial(N) = M$, then all the Stiefel-Whitney numbers of $M$ vanish.

Conversely, if $M \in \text{Mani}_{s^m,\text{cpt}}^{n}$ with all Stiefel-Whitney numbers $0$, then it is the boundary of a compact smooth manifold with boundary.

**Proof:** Let $[N] \in H_{n+1}(N, M)$ be the fundamental homology class of the pair, then $\partial([N]) = [M]$. Let $\tau N, M$ be the tangent bundle of $N, M$, then $\tau N|_M = \tau M \oplus R^1$, because there is an outward pointing normal bundle. Thus the Stiefel-Whitney classes of $M$ comes from restriction of that of $N$. Now the composite $H^n(N) \to H^n(M) \xrightarrow{\delta} H^n(N, M)$ is $0$, so $\delta(w_{i_1}, \ldots, w_k(M)) = 0$. Thus

$$\langle w_{i_1}, \ldots, w_k(M), [M] \rangle = \langle \delta(w_{i_1}, \ldots, w_k(M)), [N] \rangle = 0.$$

Conversely, Cf. [Stong, Notes on Cobordism Theory].

Prop. (3.11.7.3). For $m \in \mathbb{Z}_+$, $RP^{2m-1}$ is a boundary and $RP^{2m}$ is not a boundary.

**Proof:** Consider the fiber bundle $S^1 \to RP^{2n-1} \to CP^n$, its cone bundle is $D^1 \to M^n \to CP^{2n-1}$, which has boundary $RP^{2n-1}$.

$RP^{2m}$ is not a boundary by (3.11.7.2) and the fact its top Stiefel-Whitney class is non-zero.

Thm. (3.11.7.4) [Thom].

$$\Omega_* = F_2[t_2, t_4, t_5, \ldots]$$

is a graded polynomial algebra where there’s one generator $t_n \in \Omega_n$ for each $n \not= 2^k - 1$.

Also $\Omega_*(X) = H_*(X, \Omega_*) \cong H_*(X, F_2) \otimes_{F_2} \Omega_*$. 

**Proof:**

Cor. (3.11.7.5). A map $f : X \to Y$ induces a map $f_* : \Omega_n(X) \to \Omega_n(Y)$. This map only depends on the homotopy type of $f$. 

Oriented Cobordism

Def. (3.11.7.6) [Oriented Bordism Groups]. When $X$ is an orientable manifold, define the oriented bordism group $\Omega_n^s(X)$ to be the set of pairs $(M, f)$ where $M$ is an oriented smooth manifold of dimension $n$ and $f : M \to X$ is a continuous map preserving orientation, under the equivalence relation that $(M_0, f_0) \sim (M_1, f_1)$ iff there is an $n+1$ manifold $N$ and a map $F : N \to X$ that $\partial F = (−f_1) ∪ f_2$.

Let $\Omega_n^s = \Omega_n^s(pt)$, then for any $m, n$, there is a map $\Omega_m^s \times \Omega_n^s \to \Omega_{m+n}^s : (M, N) \mapsto M \times N$, and $M \times N \cong (−1)^{mn}N \times M$, so $\Omega_n^s$ is a graded anti-commutative ring.

Prop. (3.11.7.7). The relation of (oriented) bordism is truly an equivalence class. It suffices to show transitivity, and this is because we can piece together two manifold with boundaries by collar neighborhood theorem (11.1.1.2).

Prop. (3.11.7.8). If $N \in \text{Man}_{n+1}^\text{o, sm,cpt,ornt,∂}$ and $\partial(N) = M$, then all the Pontryagin numbers of $M$ vanish.

Proof: Let $[N] \in H_{n+1}(N, M)$ be the fundamental homology class of the pair, then $\partial([N]) = [M]$. Let $\tau_N, M$ be the tangent bundle of $N, M$, then $\tau_{N|M} = \tau_M \oplus \mathbb{R}^1$, because there is an outward pointing normal bundle. Thus the Stiefel-Whitney classes of $M$ comes from restriction of that of $N$. Now the composite $H^n(N) \to H^n(M) \overset{\delta}{\to} H^n(N, M)$ is 0, so $\delta(w_{i_1, \ldots, i_k}(M)) = 0$. thus

$$\langle w_{i_1, \ldots, i_k}(M), [M]\rangle = \langle \delta(w_{i_1, \ldots, i_k}(M)), [N]\rangle = 0.$$  

□

Prop. (3.11.7.9) [Mayer-Vitores]. Let $X = U \cup V$ where $U, V$ are open subsets of $X$.

Thm. (3.11.7.10) [Thom].

$$\Omega_*^s \otimes \mathbb{Q} \cong \mathbb{Q}[u_1, \ldots, u_n, \ldots],$$

where $u_i \in \Omega_{4i}^s$ and is represented by $[\mathbb{CP}^{2i}]$. Moreover,

- $\Omega_0^s = \mathbb{Z}$.
- $\Omega_1^s = 0$.
- $\Omega_2^s = 0$.
- $\Omega_3^s = 0$.
- $\Omega_4^s = \mathbb{Z}$, generated by $\mathbb{CP}^2$.
- $\Omega_5^s = \mathbb{Z}/2\mathbb{Z}$, generated by $Y^5$.
- $\Omega_6^s = 0$.
- $\Omega_7^s = 0$.
- $\Omega_8^s = \mathbb{Z} \oplus \mathbb{Z}$, generated by $\mathbb{CP}^4$ and $\mathbb{CP}^2 \times \mathbb{CP}^2$.
- $\Omega_9^s = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$, generated by $Y^9$ and $Y^5 \times \mathbb{CP}^2$.
- $\Omega_{10}^s = \mathbb{Z}/2\mathbb{Z}$, generated by $Y^5 \times Y^5$.
- $\Omega_{11}^s = \mathbb{Z}/2\mathbb{Z}$, generated by $Y^{11}$.
- $\Omega_n^s \neq 0$ for $n \geq 8$. 

Proof: Cf. [Milnor, P203].

By (3.11.7.8), for any partition $I$ of $k$, there is a map $\Omega_{4k} \to \mathbb{Z}: M \mapsto p_I(M)$. These maps can be used to show that the products $\{\mathbb{CP}^{2i_1} \times \mathbb{CP}^{2i_r} | \sum i_r = k\}$ are linearly independent in $\Omega_{4k}$ by (3.11.4.23).

\[ \square \]

Prop. (3.11.7.11) [Index and Oriented Cobordism]. If $k \in \mathbb{N}, W \in \text{Mani}_{cntd,orntd,cpct}^{4k+1}$, then the index $I(M) = 0$.

Proof: This follows from the fact the image of $H^{2k}(W) \overset{i^*}{\rightarrow} H^{2k}(M)$ is a half-dimensional subspace (3.10.3.18) that the intersection product is trivial:
\[
\langle i^*\alpha \cup i^*\beta, \partial[W] \rangle = \langle \alpha \cup \beta, i^*\partial[W] \rangle = 0.
\]

Then it is by linear algebra that the signature of this pairing is 0. \[ \square \]

Def. (3.11.7.12) [Stably Framed Manifold]. A stably framed manifold is a smooth manifold $M$ of dimension $n$ together with an isomorphism $TM \oplus \mathbb{R}^N \cong \mathbb{R}^{N+n}$ for some $N$.

Def. (3.11.7.13) [Framed Bordism Groups]. Because $T(\partial N) \oplus \mathbb{R} \cong TN|_{\partial N}$, we have the notion of a stably framed bordism $\Omega^fr_n(X)$. Denote $\Omega^fr_n = \Omega^fr_n(pt)$.

Prop. (3.11.7.14). $S^3 \cong SU(2)$ is naturally framed, and this generates $\Omega^fr_3 \cong \mathbb{Z}/24$.

Thm. (3.11.7.15) [Pontryagin]. $\Omega^fr_n \cong \pi_{n+N}(S^N)$.

Applications

Prop. (3.11.8.1). A simply connected manifold is orientable. (Use the orientable double cover).
3.12 Simplicial Homotopy Theory

Main references are [Jardine Simplicial Homotopy Theory], [Lur09].

1 Simplicial Objects

Def.(3.12.1.1)[Simplex Category]. The simplex category $\Delta$ consists of simplicial objects $[n]$ for each $n \geq 0$ and there maps are order-preserving maps.

$\Delta$ has a subcategory $\Delta_+$ consisting of the same objects but the morphisms are all surjective order-preserving maps.

For $C \in \text{Top}$, a simplicial object in $C$ is a functor $\Delta^{\text{op}} \to C$. A cosimplicial object in $C$ is a simplicial object in $C^{\text{op}}$. The category of simplicial objects in $C$ is denoted by $sC$.

Def.(3.12.1.2). $\Delta^n$ is the simplicial set $\Delta^n([m]) = \text{Hom}([m],[n])$.

Def.(3.12.1.3)[Augmentation]. If $X$ is a simplicial object in a category, then an augmentation of $X$ is a morphism $d : A \to X$ that $dd_0 = dd_1$. In case $C$ is $\text{Mod}_R$, this is equivalent to a morphism $\pi_0(X) \to A$.

Def.(3.12.1.4)[s-Free Simplicial Objects]. $X \in sC$ is called s-free if the underlying category $\Delta_+^{\text{op}} \to C$ is $\Delta_+^{\text{op}}$-free (3.1.2.16).

Equivalently, an s-free object is a simplicial object $X$ that there are objects $Z_n \in C$ that $X_n = \coprod_{\varphi : [n] \to [k]} \varphi^*Z_k$. Moreover, a simplicial morphism of simplicial objects are called s-free if the underlying diagram $X_+ \to Y_+$ is of the form $X_+ \to X_+ \coprod Y_0$ where $Y_0$ is s-free.

Prop.(3.12.1.5)[sC is a Simplicial Category]. Let $sC$ be the category of simplicial $C$-objects, then it can be made into a simplicial category which is also tensored and cotensored (3.1.5.6) over $\text{Set}_\Delta$.

Proof: We define first a action of $\text{Set}_\Delta$ on $sC$:

$$\otimes : \text{Set}_\Delta \times sC \to sC : (K,X) \mapsto (K \otimes X)_n = \coprod_{K_n} X_n,$$

with the simplicial maps determined by that of $K$ and $X$.

Also there is a action of $\text{Set}_\Delta^{\text{op}}$ on $sC$:

$$(-) : \text{Set}_\Delta^{\text{op}} \times sC \to sC : (K \otimes X)_n = \prod_{K_n} X_n$$

with the simplicial maps determined by that of $K$ and $X$.

Then there is an adjointness

$$\text{Hom}_{sC}(K \otimes X,Y) \cong \text{Hom}_{sC}(X,Y^K)$$

for any simplicial set $K$.

Next we define $\text{Map}_{sC}(X,Y) \subset \text{Set}_\Delta$ as $(\text{Map}_{sC}(X,Y))_n = \text{Hom}_{sC}(X \otimes \Delta^n,Y)$, then there are functorial isomorphisms

$$\text{Map}_{sC}(K \otimes X,Y) \cong \text{Map}_{sC}(X,Y^K) \cong \text{Map}_{\text{Set}_\Delta}(K,\text{Map}_{sC}(X,Y))$$

(easy to check). So we are done.
Remark (3.12.1.6) [Realization Functor]. For $\mathcal{C} \in \text{Cat}$ that has countable colimits, there is a simplicial realization functor

$$| - | : s\mathcal{C} \to \mathcal{C} : X \mapsto \lim_{\Delta_+^\text{op}} X_n.$$ 

2 Topological Categories

Def. (3.12.2.1) [Topological Categories]. A topological category is a category that is enriched over the category $\mathcal{S}$ of compactly generated and Hausdorff spaces. The category of topological categories is denoted by $\text{Cat}_{\text{Top}}$.

Two topological categories is called strongly equivalent if they are equivalent as enriched categories.

Def. (3.12.2.2) [Homotopy Category of Spaces]. Given a topological category $\mathcal{C}$, the homotopy category $h\mathcal{C}$ of $\mathcal{C}$ is defined to be the category transferred from $\mathcal{C}$ (3.1.5.3) by the right-lax monoidal functor $\pi_0$ (3.1.4.13).

Def. (3.12.2.3) [Homotopy Category of Spaces]. Let $\mathcal{C}$ be the category of CW complexes that the morphisms are given the compact-open topology, then its homotopy category $\mathcal{H}$ is called the homotopy category of spaces.

3 Simplicial Sets

Simplicial Set

Remark (3.12.3.1). The fact that any simplicial set $X$ is a colimit of $\Delta^n$ (3.1.2.13) is important in proving properties of constructions of simplicial set.

Def. (3.12.3.2) [Objects, Morphisms and Equivalences]. Given a simplicial set $S$, its objects are just maps $\Delta^0 \to S$, and its morphisms are maps $\Delta^1 \to S$.

Def. (3.12.3.3) [Nerves]. The nerve of a category $\mathcal{C}$ is a simplicial set with $(N(\mathcal{C}))_n = \text{Hom}([n], \mathcal{C})$, i.e. composable arrows of morphisms of length $n$. It is a fully faithful functor from the category of small categories to the category of simplicial sets.

Prop. (3.12.3.4) [Natural Transformation and Homotopy]. A natural transformation will induce homotopic nerve map. thus a pair of adjoint functors will induce a simplicial homotopy between their nerve.

Prop. (3.12.3.5). The nerve construction is a fully faithful functor $\text{Cat} \to s\text{Set}$.

Prop. (3.12.3.6) [Characterization fo Nerves]. For any simplicial set $K$, there is a small category $\mathcal{C}$ that $K \cong N(\mathcal{C})$ iff for each diagram

$$\Delta^n \to K$$

there exists uniquely a dotted arrow.

Proof: [HTT, P9].
Def. (3.12.3.7) [Set $\Delta$ and $\mathcal{C}G$]. There is a functor $v : \Delta \to \mathbb{Top} : [n] \mapsto \Delta^n$?, which induces a map $s \text{Set} \to s \mathbb{Top}$.

The (topological) **geometrization** is the functor

$$s \text{Set} \to \mathbb{Top} : X \mapsto |X| = |v(X)|.$$

The **singular complex functor** maps a topological space $Y$ to a simplicial set

$$(\text{Sing}(Y))_n = \text{Map}(\Delta_n, Y).$$

The geometrization functor is left adjoint to the singular functor as functors between the categories $\mathcal{C}G$ and $\text{Set}_\Delta$ (use colimit definition of $X$). This is just the Kan extension in (3.1.2.14).

Moreover, the geometrization as a functor from $\text{Set}_\Delta \to \mathcal{C}G$ preserves finite limits. Cf. [Jardine P9].

The three kinds of geometrization of a bisimplicial set is the same: geometrization the diagonal simplicial set, the twice geometrization of left(resp. right) simplicial set.

**Proof:**

Def. (3.12.3.8) [Weak Homotopy Equivalence]. A morphism of simplicial sets $S \to T$ is called a **weak homotopy equivalence** if the induced map $|S| \to |T|$ is a weak homotopy equivalence.

Prop. (3.12.3.9) [Quillen]. The geometrization functor and the singular complex functor defines a Quillen equivalence:

$$|−| : \text{Set}_\Delta \rightleftarrows \mathcal{C}G : S(−)$$

where the RHS is Serre-Quillen model category (3.9.6.28).

The functor $|−| \circ S(−)$ is denoted by $\Gamma : \mathcal{C}G \to \mathcal{C}G$.

**Proof:** Cf. [May, P125].

Cor. (3.12.3.10). The localized category of $\mathcal{C}G$ and $\text{Set}_\Delta$ at weak homotopy equivalence classes are the same, and it is just the homotopy category of spaces $\mathcal{H}$, by (3.7.2.7).

**Constructing Simplicial Sets**

Def. (3.12.3.11) [Joins]. Let $S, S'$ be simplicial sets, then the **join** of $S, S'$ is defined to be the simplicial set that for all any finite ordered set $J$,

$$(S \star S')(J) = \bigcup_{J = I \coprod I'} S(I) \times S(I').$$

where $I, I'$ satisfies $i < i'$ for any $i \in I, i' \in I'$. And the glueing is natural. Join clearly commutes with colimits.

Prop. (3.12.3.12) [Monoidal Structure of $\text{Set}_\Delta$]. The join operation makes the category of sets a monoidal category.

Def. (3.12.3.13) [Cones]. For a simplicial set $K$, the **left/right cone** of $K$ are defined to be the join $K^\diamond = \Delta^0 \star K$ and $K^\blacksquare = K \star \Delta^0$.

For a map $f : X \to S$, the **left/right cone** of $f$ are defined to be $S \coprod_X X^\diamond$ and $S \coprod_X X^\blacksquare$. 
Def. (3.12.3.14) [Overcategories]. Let \( p : K \to S \) be a morphism of simplicial sets, then there is a simplicial set \( S_{/p} \) that
\[
\text{Hom}(Y, S_{/p}) \cong \text{Hom}_p(Y \times K, S).
\]
Where \( \text{Hom}_p \) indicates that we only consider morphisms that \( f|_K = p \). And dually we can define the undercategories.

Proof: We just define \((S_{/p})_n = \text{Hom}_p(\Delta^n \times K, S)\), then the condition holds for \( \Delta^n \), and use the fact every simplicial set is a colimit of \( \Delta^n \)s (3.12.3.1), and both sides commutes with colimits. □

Prop. (3.12.3.15) [Generating Simplicial Sets]. Let \( \mathcal{U} \) be a collection of simplicial sets that:
- \( \mathcal{U} \) is stable under isomorphisms,
- \( \mathcal{U} \) is stable under disjoint union,
- \( \Delta^n \subset \mathcal{U} \) for any \( n \),
- If there is a pushout diagram \( X \xrightarrow{f} X' \xleftarrow{g} Y \xrightarrow{h} Y' \) and \( X, X', Y \in \mathcal{U} \) and \( f \) is a monomorphism, then \( Y' \in \mathcal{U} \),
- suppose we are given a sequence of monomorphisms between objects in \( \mathcal{U} \) indexed over \( \mathbb{N} \), then the colimit belongs to \( \mathcal{U} \).

Proof: Use induction on the dimension of \( S \), and notice \( S \) is glued together using their simplexes. □

Fibrations and Anodynes

Def. (3.12.3.16) [Fibrations]. A morphism of simplicial sets is called a
- Kan fibration iff it has right lifting property w.r.t all \( \Lambda^i_k \to \Delta^n \).
- left fibration iff it has right lifting property w.r.t. all inclusions \( \Lambda^i_k \subset \Delta^n, 0 \leq i < n \).
- right fibration iff it has right lifting property w.r.t all inclusions \( \Lambda^i_k \subset \Delta^n, 0 < i \leq n \).
- inner fibration iff it has right lifting property w.r.t all inclusions \( \Lambda^i_k \subset \Delta^n, 0 < i < n \).

A morphism of simplicial set is called a
- anodyne iff it has left lifting property w.r.t. all Kan fibrations.
- left anodyne iff it has left lifting property w.r.t. all left fibrations.
- right anodyne iff it has left lifting property w.r.t. all right fibrations.
- inner anodyne iff it has left lifting property w.r.t all inner fibrations.

So a morphism between topological spaces \( X \to Y \) is a Serre fibration iff \( S(X) \to S(Y) \) is a Kan fibration (3.12.3.7).

Def. (3.12.3.17) [Trivial Fibration]. A morphism \( X \to S \) of simplicial sets that has right lifting property w.r.t. all inclusions \( \partial \Delta^n \to \Delta^n \) is called a trivial fibration.

A cofibration is a morphism that has left lifting property w.r.t all trivial fibrations. By (3.1.6.10) a cofibration of simplicial sets is just an inclusion.
Lemma (3.12.3.18) [Join and Anodynes]. If $f : A_0 \subset A$ and $g : B_0 \subset B$ are inclusions of simplicial sets, then
\[ h : (A_0 \ast B) \coprod_{A_0 \ast B_0} (A \ast B_0) \subset A \ast B \]
is an \( \ast \)-inner anodyne if either $f$ is right anodyne or $g$ is left anodyne, then
• inner anodyne if either $f$ is right anodyne or $g$ is left anodyne.

Proof: 1: By symmetry we assume $f$ is right anodyne. Notice the class of all morphisms $f$ that the conclusion holds is weakly saturated because $\ast$ commutes with colimits, so it suffice to check for $f : \Lambda^n_k \subset \Delta^n$. Then similarly it suffices to check for $g : \partial \Delta^m \subset \Delta^m$, but then the inclusion is just $\Lambda^{m+n+1}_j \subset \Delta^{m+n+1}$, which is left anodyne.

Prop. (3.12.3.19) [Anodynes].
• The saturated class generated by either of the following three classes of monomorphisms are both left anodynes:
  1. $\Lambda^n_k \subset \Delta^n$, $0 \leq k < n$.
  2. $(\Delta^m \times \{0\}) \coprod (\partial \Delta^m \times \Delta^1) \subset \Delta^m \times \Delta^1$.
  3. $(S' \times \{0\}) \coprod (S \times \Delta^1) \subset S' \times \Delta^1$, where $S \subset S'$.

Similar conclusion holds for right anodynes and together implies the similar conclusion for anodynes.

Proof: 2 and 3 are equivalence because any inclusion comes from attaching cells (3.12.3.3).
Now inclusions in 2 are compositions of pushouts of inclusions $\Lambda^{n+1}_k \subset \Delta^{n+1}$, where $0 \leq k \leq n$, thus it is generated by 1. Conversely, $\Lambda^n_k \subset \Delta^n$ is a retract of $(\Delta^n \times \{0\}) \coprod (\Lambda^n_k \times \Delta^1) \subset \Delta^n \times \Delta^1$:
Cf. [HTT, P64].

Cor. (3.12.3.20) [Products and Anodynes]. Let $A \subset A'$ be an inner anodyne and $B \subset B'$, then so does the induced map
\[ (A \times B') \coprod_{A \times B} (A' \times B) \to A' \times B'. \]

Proof: For left anodyne, the proof is similar to that of (3.12.3.18), just check for classes 3 of (3.12.3.19), and use the fact
\[ (S' \times \Delta^1) \times B \coprod (S' \times \{0\}) \coprod (S \times \Delta^1) \times B' \to (S' \times \Delta^1) \times B' \]
is just
\[ (S' \times B \coprod S \times B') \times \Delta^1 \coprod (S' \times B') \times \{0\} \to (S' \times B') \times \Delta^1. \]
which is left(inner) anodyne. And similarly for inner anodynes.
3.12. SIMPLICIAL HOMOTOPY THEORY

**Left Fibration**

**Remark (3.12.3.21)**[Left and Right Fibrations Dual]. The theory of left fibrations is dual to the theory of right fibrations, thus we don’t study right fibrations.

**Prop. (3.12.3.22)**[Left Fibration and CoFibered in Groupoids]. Let $F : \mathcal{C} \to \mathcal{D}$ be a functor, then $\mathcal{C}$ is a category cofibered in groupoids over $\mathcal{D}$, iff the induced functor $N(F) : N(\mathcal{C}) \to N(\mathcal{D})$ is a left fibration of simplicial sets.

**Proof:** By (3.12.3.6), $N(F)$ is an inner fibration, thus it suffices to check for $\Lambda^n_0 \to \Delta^n$. For $n = 1$, this is the definition of cofibered category (3.1.7.10), and $n = 2$ is just the surjectivity of the map defining CoCartesian arrows (3.1.7.7), and $n = 3$ is equivalent to the injectivity of the map defining Cocartesian arrows. And for $n > 3$, then extension is automatic for nerves. □

**Remark (3.12.3.23)**[Right Fibrations and Fibered Categories]. The (left)right fibration is the $\infty$-categorial analogue of (co)fibered categories in usual category theory.

**Remark (3.12.3.24).** Given a left fibration $X \to S$ is more or less similar to given a functor from the homotopy category $hS$ to the $\infty$-category $\mathcal{H}$ of spaces.

**Proof:** Cf.[HTT, P58]. □

**Prop. (3.12.3.25)**[Over(Under)categories and Fibrations]. Given a digram of simplicial sets:

$$A \subset B \xrightarrow{q} X \xrightarrow{p} S.$$  

Let $r = q \circ p$, $p_0 = p|_A$, $r_0 = r|_A$, and $q$ is an inner fibration, then

- the induced map $X_{p/} \to X_{p_0/} \times_{S_{r_0/}} S_{r/}$ is a left fibration. And dual argument holds for overcategories.
- If $q$ is a left fibration or $A \subset B$ is right anodyne, then $X_{p/} \to X_{p_0/} \times_{S_{r_0/}} S_{r/}$ is a trivial fibration.
- If $q$ is moreover a left fibration, then the induced map $X_{r/} \to X_{p_0} \times_{S_{r_0}} S/r$ is a left fibration.

**Proof:** These just follow from (3.12.3.18). □

**Prop. (3.12.3.26)**[Homotopy Extension Lifting Property]. Let $p : X \to S$ be a map of simplicial sets and $i : A \subset B$, consider the map

$$q : X^B \to X^A \times_{S^A} S^B.$$  

- If $p$ is a left fibration, then $q$ is a left fibration.
- If $p$ is a left fibration and $i$ is a left anodyne, then $q$ is a trivial fibration.
- If $i : \{0\} \subset \Delta^1$, then $p$ is a left fibration iff $q$ is a trivial fibration.
- If $p$ is an inner fibration, then $q$ is an inner fibration.
- If $p$ is an inner fibration and $i$ is an inner anodyne, then $q$ is a trivial fibration.

**Proof:** First notice that a right lifting of $q$ w.r.t a map $Z \to Z'$ is equivalent to a right lifting of $p$ w.r.t the map $Z \times B \coprod Z' \times A \to Z' \times B$. Then the conclusions follow from (3.12.3.20) and (3.12.3.19). □
Prop. (3.12.3.27) [Homotopy Section and Left Fibration]. Let $X \to S$ be a map of simplicial sets and $s : S \to X$ be section of $p$, and let $h \in \text{Hom}_S(X \times \Delta^1, X)$ that $h|_{X \times \{0\}} = s \circ p$ and $h|_{X \times \{1\}} = \text{id}$, then $s$ is a left anodyne.

Proof: Cf.[HTT, P65]. □

Prop. (3.12.3.28) [Left Fibration and Functor to Spaces]. Let $X \to S$ be a left fibration, then the fibers are all Kan complexes by (3.13.2.5), and for any edge $f : s \to s' \in S$, we can solve the lifting diagram

\[
\begin{array}{ccc}
\{0\} \times X_s & \to & X \\
\downarrow & & \downarrow \\
\Delta^1 \times X_s & \to & \Delta^1 \xrightarrow{f} S
\end{array}
\]

because the left hand side is left anodyne by (3.12.3.20), thus getting a morphism $f_! : X_s \to X_{s'}$.

Then this determines a functor from $hS$ to $\mathcal{H}$ the homotopy category of spaces.

Proof: First notice $f_!$ is uniquely defined up to homotopy: given to dotted arrow solving the diagram, we can use the lifting property w.r.t. the map

\[
\Delta^1 \times \partial \Delta^1 \times X_s \coprod_{\{0\} \times \partial \Delta^1 \times X_s} \{0\} \times \Delta^1 \times X_s \to \Delta^1 \times \Delta^1 \times X_s
\]

which is a left anodyne by (3.12.3.20), to get a homotopy between them.

Next if $\eta \in \text{Hom}_H(K, X_s), \eta' \in \text{Hom}_H(K, X_{s'})$, then $\eta' = f_! \circ \eta$ iff there is a map $q : K \times \Delta^1 \to X$ that $q \circ p$ is given by the mapping $X_s \times \Delta^1 \to \Delta^1 \xrightarrow{f_!} S$, and $p|_{K \times \{0\}}, p|_{K \times \{1\}}$ have homotopy types $\eta, \eta'$ resp..

Then for any $g \circ f \cong h \in S$, which is depicted by a 2-complex, we can use the left anodyne $X_u \times \{0\} \subset X_u \times \Delta^2$ to get a morphism $p : X_u \times \Delta^2 \to X$, then $p|_{X_u \times \{1\}} \cong f_!, p|_{X_u \times \{2\}} \cong h_!$, and the map $p|_{X_u \times \Delta(1,2)}$ witnesses the fact $g_! \circ f_! \cong h_!$. □

Kan Fibrations

Remark (3.12.3.29) [Kan Complexes and Groupoids]. Kan complexes are $\infty$-categorical analogy of groupoids, by (3.13.2.5).

Lemma (3.12.3.30). If a left fibration $p : S \to T$ is a weak homotopy equivalence of Kan complexes, then it is a surjection on vertices.

Proof: Because it is homotopy equivalence, for any $t \in T$, there is a morphism $p(s) \to t$ for some $s \in S$(Kan complex used), thus it lifts to a morphism in $S$, so surjective on vertices. □

Lemma (3.12.3.31) [Fibrations of Kan Complexes]. If $S \to T$ is a left fibration and $T$ is a Kan complex, then $p$ is a Kan fibration.

Proof: Firstly $S$ is a Kan complex. Let $A \subset B$ be anodyne morphisms, we need to show $p : S^B \to S^A \times_{T^A} T^B$ is surjective on vertices. Since $S, T$ are complexes, $S^B \to S^A$ and $T^B \to T^A$ are trivial fibrations by (3.12.3.26). Cf.[HTT, P66].

Notice this is an immediate consequence of (3.12.3.36), because the homotopy category of a Kan complex is a groupoid, by (3.13.2.5), so $f_!$ must be isomorphisms. □
Prop. (3.12.3.32) [Examples of Kan Complexes].
- The singular complex of topological space is a Kan complex.
- The nerve of a topological space is a Kan complex.
- The nerve of a category is a Kan complex iff the category is a groupoid, by (3.12.3.22).
- Simplicial $R$-module are Kan complexes, by (8.1.1.1).

Prop. (3.12.3.33). The bar resolution $BG$ is a Kan fibration for every group $G$.

Proof: □

Prop. (3.12.3.34). A principal $G$ fibration, i.e. $X \to X/G$ where $X$ is a simplicial object of $G$-sets that $G$ acts freely on $X_n$, is a Kan fibration.

Lemma (3.12.3.35). Let $p : S \to T$ be a left fibration that all the fibers are contractible, then $p$ is a trivial Kan fibration.

Proof: By duality, it suffices to prove for right fibrations. Because fiber is nonempty, it has right lifting property w.r.t $\emptyset \subset \Delta^0$, and for $n > 0$, let $\partial \Delta^n \to S$ be any map, then to show the lifting property, we may take fiber product and assume $T = \Delta^n$, thus $S$ is an $\infty$-category. Cf. [HTT, P66]. □

Prop. (3.12.3.36) [Characterization of Kan Fibrations]. Let $p : S \to T$ be a left fibration of simplicial sets, then $p$ is a Kan extension iff the morphism $f!$ defined in (3.12.3.28) is an isomorphism in $\mathcal{H}$ for any morphism $f \in T$.

Proof: Cf. [HTT, P66]. □

4 Simplicial Categories & Model Categories

Def. (3.12.4.1) [Simplicial Category]. The category $\mathcal{Cat}_\Delta$ of simplicial categories consists of categories enriched over the Cartesian monoidal category $\mathbf{Set}_\Delta$ of simplicial sets.

Def. (3.12.4.2) [Homotopy Category]. There are singular complex functor and geometrization functor that induce isomorphism of $h(\mathbf{Set}_\Delta) \cong h(\mathcal{G})$ by (3.12.3.10), thus the theory of simplicial categories and topological categories are the same.

Simplicial Nerves

Def. (3.12.4.3) [Thickened Finite Ordered Sets]. Let $J$ be a finite ordered set, define a simplicial category $\mathcal{C}[\Delta^J]$ as follows:
- The objects are elements of $J$.
- For $i, j \in J$, $\text{Mor}(i, j) = N(P_{i,j})$, where $P_{i,j}$ is the partially ordered set of subsets $I \subset J$ that $i, j \in I$.
- The morphism is induced by the inclusion of partially ordered sets $P_{i,j} \times P_{j,k} \subset P_{i,k}$.

Prop. (3.12.4.4) [$\mathcal{C}$].
- There is a unique functor $\mathcal{C}[\Delta^n] \to \Delta^n$, and it is an equivalence of simplicial categories, because each morphism space in $\mathcal{C}[\Delta^n]$ is a cube.
• The mapping $J \mapsto \mathcal{C}[\Delta^J]$ is a functor from $\Delta$ to $\mathcal{C}at_\Delta$. In other words, $\mathcal{C}$ defines a cosimplicial object in $\mathcal{C}at_\Delta$.

• $\mathcal{C}$ extends naturally to a colimit-preserving morphism $\mathcal{S}et_\Delta \to \mathcal{C}at_\Delta$, by (3.12.3.1).

**Def. (3.12.4.5) [Simplicial Nerve].** For a simplicial category $\mathcal{C}$, we define the simplicial nerve to be the simplicial set that

$$(N(\mathcal{C}))_n = \text{Hom}_{\mathcal{C}at_\Delta}(\mathcal{C}[\Delta^n], \mathcal{C}).$$

If $\mathcal{C}$ is a topological category, then define the topological nerve to be the simplicial nerve of $\text{Sing}(\mathcal{C})$.

By the definition and the adjointness of (3.12.3.7), the nerve functor $N$ is right adjoint to the functor $[\mathcal{C}[-]]$ or $\mathcal{C}[-].$

**Remark (3.12.4.6).** It should be checked that to give a 2-complex in $N(\mathcal{C})$ is equivalent to giving morphisms $f, g, h \in \mathcal{C}$ and a path from $g \circ f$ to $h$.

**Prop. (3.12.4.7) [Nerve and Simplicial Nerve].** If we forget the enriched structure on $hS$, then the usual nerve $N$ and $h$ determines a adjoint between $\mathcal{S}et_\Delta$ and $\mathcal{C}at_\Delta$.

*Proof:* Notice that the usual nerve is a special case of simplicial nerve by the inclusion $\mathcal{C}at \subset \mathcal{C}at_\Delta$. And also the inclusion $\mathcal{S}et \subset \mathcal{S}et_\Delta$ is left adjoint to the functor $\pi_0$. □

**Prop. (3.12.4.8) [Kan Fibrations Nerve Inner Fibrations].** Let $F : \mathcal{C} \to \mathcal{D}$ be a a map of simplicial categories that for any $C, C' \in \mathcal{C}$, $\text{Map}(C, C') \to \text{Map}(F(C), F(C'))$ is a Kan fibration, then the induced map of simplicial sets $N(\mathcal{C}) \to N(\mathcal{D})$ is an inner fibration.

*Proof:* This is because a lifting of $N(\mathcal{C}) \to N(\mathcal{D})$ w.r.t. $\lambda^p_j \subset \Delta^n$ is equivalent to a lifting of $\mathcal{C} \to \mathcal{D}$ w.r.t. $\mathcal{C}[\Delta^p_j] \subset \mathcal{C}[\Delta^n]$. But this lifting is equivalent to a lifting of $\text{Map}(F(0), F(n)) \to \text{Map}(F'(0), F'(n))$ w.r.t. the anodyne map $\text{Map}_{\mathcal{C}[\Delta^p_j]} \subset \text{Map}_{\mathcal{C}[\Delta^n]}$, which is a cube removing the interior and a face. □

**Cor. (3.12.4.9).** The topological nerve of a topological category $\mathcal{C}$ is an $\infty$-category, as the singular complex of a topological space is always a Kan complex, by (3.12.3.32).

**Def. (3.12.4.10) [Homotopy Category].** For a simplicial set $S$, the homotopy category $hS$ is defined to be the homotopy category (3.12.4.2) of the simplicial category $\mathcal{C}[S]$. A map of simplicial sets is called a categorical equivalence if their homotopy categories are equivalent as $\mathcal{S}$-enriched categories.

**Remark (3.12.4.11).** It is immediate that $S \cong T$ categorically iff $\mathcal{C}[S] \cong \mathcal{C}[T]$ iff $|\mathcal{C}[-]| \cong |\mathcal{T}|$.

**Lemma (3.12.4.12).** Let $\mathcal{C}$ be a topological category, then the counit map $|\mathcal{C}(N(\mathcal{C}))| \cong \mathcal{C}(3.12.4.5)$ is an equivalence of topological categories.

*Proof:* By the Quillen equivalence between $\mathcal{S}et_\Delta$ and $\mathcal{C}at_\Delta(3.12.3.9)$, as by (3.7.7.11) and (3.12.3.32), $\text{Sing}(\mathcal{C})$ is a fibrant simplicial category. □

**Lemma (3.12.4.13).** Let $\mathcal{C}$ be fibrant simplicial category, then the counit map $u : \text{Map}_{\mathcal{C}[N(\mathcal{C})]}(x, y) \to \text{Map}_{\mathcal{C}}(x, y)$ is a weak homotopy equivalence of simplicial sets.

*Proof:* Cf. [HTT, P72]. □
Prop. (3.12.4.14) [Topological Category and \(\infty\)-Category Equivalent]. The adjoints functors \(N\) and \(|\cdot|\) define an equivalence of the category of topological categories and \(\infty\)-categories modulo equivalence.

**Proof:** It suffices to show the units and counits are equivalences:

\[
|\mathcal{C}[N(\mathcal{E})]| \cong \mathcal{E}, \quad S \mapsto N(|\mathcal{C}[S]|).
\]

The first is (3.12.4.12), and the second follows from the first by remark (3.12.4.11). \(\Box\)

Prop. (3.12.4.15). For simplicial sets \(S, S'\), the natural map \(\mathcal{C}[S \times S'] \to \mathcal{C}[S] \times \mathcal{C}[S']\) is an equivalence of simplicial categories.

**Proof:** If \(S, S'\) are nerves of fibrant simplicial categories \(\mathcal{C}, \mathcal{C}'\), then we have a diagram \(\mathcal{C}[S \times S'] \to \mathcal{C}[S] \times \mathcal{C}[S'] \to \mathcal{C} \times \mathcal{C}'\). Then by the two out of three axiom, the assertion follows from the fact that for any fibrant simplicial category \(\mathcal{D}\), \(\mathcal{C}[N(\mathcal{D})] \to \mathcal{D}\) is an equivalence (3.12.4.12).

Now for general \(S, S'\), we can find a categorical equivalences \(\mathcal{C} \to \mathcal{C}[N(\mathcal{C}[S])] = T\), and then \(S \times S' \to T \times T'\) is also categorical equivalence by (3.12.4.15), and we are done, by (3.12.5.16). \(\Box\)

### Simplicial Model Categories

Def. (3.12.4.16) [Simplicial Model Category]. A simplicial model category is a \(\text{Set}_{\Delta}\)-enriched model category (3.7.6.3).

Prop. (3.12.4.17) [Simplicial Model Category Criterion]. Let \(\mathcal{C}\) be a simplicial category that is equipped with a model structure that every object of \(\mathcal{C}\) is cofibrant and the collection of weak equivalences in stable under filtered colimits, then \(\mathcal{C}\) is a simplicial model category iff the following conditions holds:

- \(\mathcal{C}\) is both tensored and cotensored over \(\text{Set}_{\Delta}\).
- Given a cofibration of simplicial sets \(i : K \to L\) and a cofibration \(C \to D \in \mathcal{C}\), the induced map \((C \otimes L) \coprod_{C \otimes K} D \otimes K \to D \otimes L\) is a cofibration in \(\mathcal{C}\).
- The natural map \(C \otimes \Delta^n \to C \otimes \Delta^0 \cong C\) is a weak equivalence in \(\mathcal{C}\).

**Proof:** Cf. [HTT, P850]. \(\Box\)

Prop. (3.12.4.18). Let \(\mathcal{C}\) be a simplicial model category and \(X\) cofibrant and \(Y\) fibrant, then \(K = \text{Map}(X, Y)\) is a Kan complex, and there is a canonical bijection \(\pi_0 K \cong \text{Hom}_{\text{Ho}(\mathcal{C})}(X, Y)\).

**Proof:** Use (3.7.6.4). \(\Box\)

Prop. (3.12.4.19).

5 Covariant Model Structure

Prop. (3.12.5.1) [Covariant Model Structure]. Let \(S\) be a simplicial set, then we call a map \(X \to Y \in (\text{Set}_{\Delta})_S\)

- **covariant cofibration** if it is a monomorphism.
- **covariant equivalence** if the induced map \(X^\circ \coprod_X S \to Y^\circ \coprod_Y S\) is a categorical equivalence (3.12.4.10).
Then these define a left proper combinatorial model structure on \((\mathbf{Set}_\Delta)/S\).

**Proof:** Cf.[HTT, P69]. □

**Lemma (3.12.5.2).** Every left anodyne map in \((\mathbf{Set}_\Delta)/S\) is a covariant equivalence.

**Proof:** Cf.[HTT, P69]. □

**Prop. (3.12.5.3)[Covariant Model Structure].** \((\mathbf{Set}_\Delta)/S\) is a simplicial model category with the contravariant model structure and the simplicial structure where

\[
\text{Map}(X,Y) = Y^X \times_{S^X} \{\varphi\} \in \mathbf{Set}_\Delta
\]

where \(\varphi : X \to S\) is the structure map.

**Proof:** We use (3.12.4.17), it suffices to check that \(X \times \Delta^n \to X \times \Delta^0\) is a covariant equivalence. But it has a section, which is a left anodyne by (3.12.3.20), thus it is a covariant equivalence by (3.12.5.2). □

**Cor. (3.12.5.4)[Contravariant Model Structure].** Let \(S\) be a simplicial set, then the covariant model is usually not self-dual, and we can define a **contravariant model structure** as follows:

- A **contravariant cofibration** is a monomorphism of simplicial sets.
- \(f\) is a **contravariant equivalence** in \((\mathbf{Set})/S\) iff \(f^{op}\) is a covariant equivalence in \((\mathbf{Set})/S^{op}\).
- \(f\) is a **contravariant fibration** in \((\mathbf{Set})/S\) iff \(f^{op}\) is a covariant fibration in \((\mathbf{Set})/S^{op}\).

**Prop. (3.12.5.5)[Base Change].** Let \(S \to S'\) be a map of simplicial sets, then the forgetful functor and base change functor \(j_!, j^*\) defines a Quillen adjunction of covariant models:

\[
j_! : (\mathbf{Set}_\Delta)/S \rightleftarrows (\mathbf{Set}_\Delta)/S' : j^*
\]

**Proof:** it is clearly a pair of adjoints, and \(j_!\) preserves cofibrations. \(j_!\) also preserves covariant equivalences: Cf.[HTT, P71]? Thus it is a Quillen adjunction. □

**Lemma (3.12.5.6).** Let \(S' \subset S\) be simplicial sets, let \(p : X \to S\) be a map and \(q : Y \to S\) be a right fibration. Let \(X' = X \times_S S', Y' = Y \times_S S'\), then the restriction map

\[
\varphi : \text{Map}(\mathbf{Set}_\Delta)/S(X,Y) \to \text{Map}(\mathbf{Set}_\Delta)/S'(X',Y')
\]

is a Kan fibration.

**Proof:** Firstly it is a right fibration because it has right lifting property w.r.t. right anodyne inclusion \(A \to B\): this is because \((A \times X') \sqcup (A \times X) \subset B \times X\) is also a right anodyne (3.12.3.20). Next we apply this to the inclusion \(\emptyset \subset S'\) to see that \(\text{Map}(\mathbf{Set}_\Delta)/S'(X',Y')\) is a Kan complex (3.13.2.5), and then \(\varphi\) is a Kan fibration by (3.12.3.31). □

**Lemma (3.12.5.7).** Let \(p : X \to S\) be an object of \((\mathbf{Set}_\Delta)/S\), then \(p\) is a right fibration iff it is a covariant fibrant object in \((\mathbf{Set}_\Delta)/S\).

**Proof:** Cf.[HTT, P85]. □
Def. (3.12.5.8) [Pointwise Equivalence]. Let \( X \to Y \) be a map in \( RFib(S) \), then \( f \) is called a \textbf{pointwise equivalence} iff the induced map \( X_s \to Y_s \) is a homotopy equivalence of Kan complexes (3.13.2.5) for any \( s \in S \).

Lemma (3.12.5.9). Let \( f : X \to Y \) be a morphism in \( RFib(S) \), then the following are equivalent:

- \( f \) is a pointwise equivalence.
- \( f \) is an equivalence in the simplicial category \((\text{Set})/S\).
- For any \( A \in (\text{Set})/S \), \( f \) induces a homotopy equivalence of Kan complexes:
  \[
  \text{Map}_{(\text{Set}_\Delta)/S}(A,X) \to \text{Map}_{(\text{Set}_\Delta)/S}(A,Y).
  \]

Proof: Cf. [HTT, P82]. \( \square \)

Prop. (3.12.5.10) [Equivalences]. In the situation of (3.12.5.8), \( f \) is a pointwise equivalence iff it is a contravariant equivalence iff it is a categorical equivalence.

Proof: Cf. [HTT, 2.2.3.13, 3.3.1.5]? \( \square \)

Prop. (3.12.5.11) [Cotravariant Fibration as Right Fibration]. Let \( f : X \to Y \) be a map in \( RFib(S) \), then \( f \) is a contravariant fibration in \((\text{Set}_\Delta)/S\) iff it is a right fibration.

Proof: Cf. [HTT, P86]. \( \square \)

### Straightening and Unstraightening

Def. (3.12.5.12) [Straightening and Unstraightening]. Fix a simplicial set \( S \), a simplicial category \( \mathcal{C} \) and a functor \( \mathcal{C}[S] \to \mathcal{C}^{op} \). Given an object \( X \in (\text{Set}_\Delta)/S \), let \( v \) be the cone point of \( X^\circ \). Then the simplicial category \( \mathcal{M} = \mathcal{C}[X^\circ] \coprod \mathcal{C}[X] \mathcal{C}^{op} \) can be viewed as a correspondence between \( \mathcal{C}^{op} \) and \( \Delta^0 \), thus giving a simplicial functor

\[
\text{St}_\varphi : \mathcal{C} \to \text{Set}_\Delta : C \mapsto \text{Map}_\mathcal{M}(C,v).
\]

Then \( \text{St}_\varphi \) is called the \textbf{straightening functor} associated to \( \varphi \). And we denote by \( \text{St}_S \) the functor \( \text{St}_\varphi \) where \( \varphi : \text{id}_{\mathcal{C}[S]} \).

By the adjoint functor theorem (3.1.1.35), \( \text{St}_\varphi \) has a left adjoint called \textbf{unstraightening functor} \( \text{Un}_\varphi \)?.

Prop. (3.12.5.13). Let \( S \) be a simplicial set, \( \mathcal{C} \) a simplicial category and \( \varphi : \mathcal{C}[S] \to \mathcal{C}^{op} \) a simplicial functor, then the straightening and unstraightening functor determines a Quillen adjunction

\[
\text{St}_\varphi : (\text{Set}_\Delta)/S \rightleftarrows \text{Set}_\Delta^{\mathcal{C}} : \text{Un}_\varphi
\]

determines a Quillen adjunction, where the LHS has the contravariant model structure and the RHS has the projective model structure. And if \( \varphi \) is an equivalence of simplicial categories, then \((\text{St}_\varphi, \text{Un}_\varphi)\) is a Quillen equivalence.

Proof: \( \square \)
Unstraightening of Right Fibrations

Prop. (3.12.5.14). For every simplicial set $S$, the unstraightening $Un_S$ induces an equivalence of simplicial categories

$$(\text{Set}^{\mathcal{C}[S]}_{\Delta})^{\circ} \rightarrow \text{RFib}(S).$$

(3.7.6.5), where the RHS is the category of fibrations $X \rightarrow S$.

Proof: Cf.[HTT, P83].

Joyal Model Structure

Lemma (3.12.5.15) [Inner Anodyne is Categorical Equivalence]. Every inner anodyne map $A \rightarrow B$ of simplicial sets is a categorical equivalence.

Proof: The class of morphisms $f$ that $\mathbb{C}(f)$ is a trivial cofibration is weakly saturated (because $\mathbb{C}$ is a left adjoint of $\mathbb{C}(S)$), then it suffices to check for $\Lambda^n_j \subset \Delta^n$. Then $\mathbb{C}[\Lambda^n_j] \subset \mathbb{C}[\Delta^n]$ is a pushout of $[i]_K \subset [1]_{(\Delta^1)^{n-1}}$, where $K$ is obtained form $(\Delta^1)^{n-1}$ by moving a face and the interior. Thus it is a trivial cofibration (3.7.7.4). □

Prop. (3.12.5.16) [Joyal Model Structure]. There is a left proper combinatorial model structure called Joyal model structure on $\text{Set}_{\Delta}$, with:

- Cofibrations: monomorphisms.
- Weak equivalences: categorical equivalences defined in (3.12.4.10).
- Fibrations: categorical fibrations which has the right lifting property w.r.t. trivial cofibrations.

And the adjoint functors $(\mathbb{C}, N)$ determines a Quillen equivalence between $\text{Set}_{\Delta}$ and $\mathbb{C}at_{\Delta}$.

Proof: Cf.[HTT, P89],?

Firstly we show $\mathbb{C}$ preserves cofibrations. It suffices to show that $\mathbb{C}[\partial \Delta^n] \subset \mathbb{C}[\Delta^n]$ is a cofibration (3.7.7.4). But notice this two simplicial category only differ at $\text{Hom}_{\mathbb{C}[\partial \Delta^n]}(0, n)$ is the boundary of the simplicial cube $(\Delta^1)^{n-1} \cong \text{Hom}_{\mathbb{C}[\Delta^n]}(0, n)$, thus the inclusion is a pushout of the inclusion $[1]_{(\Delta^1)^{n-1}} \subset [1]_{(\Delta^1)^{n-1}}$, which is a cofibration by (3.7.7.3).

Left properness is clear (3.7.0.9). $\mathbb{C}$ preserves weak equivalences by (3.12.4.10) and (3.7.7.4), so $(\mathbb{C}, N)$ is a Quillen adjunction. To show it is a Quillen equivalence: It suffices to check for each simplicial set $S$ and fibrant simplicial category $\mathbb{C}$, a map $u : S \rightarrow N(\mathbb{C})$ is a categorical equivalence iff the adjoint map $v : \mathbb{C}[S] \rightarrow \mathbb{C}$ is an equivalence of simplicial categories. But $v$ factors as

$$\mathbb{C}[S] \xrightarrow{[u]} \mathbb{C}[N(\mathbb{C})] \xrightarrow{w} \mathbb{C}$$

and the counit map $w$ is an equivalence by (3.12.4.13). □

Cor. (3.12.5.17). if $f : A \rightarrow B$ is a categorical equivalence of simplicial sets and $K$ is a simplicial set, then $A \times K \rightarrow B \times K$ is also a categorical equivalence.

Proof: Choose a factorization $B \rightarrow Q$, which is an inner anodyne and $Q$ is an $\infty$-category, by small object argument (3.1.6.8), then $B \times K \rightarrow Q \times K$ is also an inner anodyne map (3.12.3.20), hence a categorical equivalence (3.12.5.15), so we can assume $B$ is an $\infty$-category. Similarly we can reduce to the case $A, K$ are also $\infty$-categories.

For the rest, Cf.[HTT, P92]. □
Prop. (3.12.5.18) [∞-Category Fibrant in Joyal Model]. A simplicial set $C$ is fibrant in the Joyal model structure iff it is an $\infty$-category.

Proof: Fibrant objects are $\infty$-categories, by (3.12.5.15). For the converse, fix an $\infty$-category and an inclusion $A \subset B$, given a map $A \to \mathcal{C}$, the inclusion $\mathcal{C} \subset C \coprod_A B$ is also a categorical equivalence because Joyal model structure is left proper (3.12.5.16), thus $\mathcal{C}$ is a retract of $C \coprod_A B$ by (3.12.5.19), which gives an extension $B \to \mathcal{C}$.

Lemma (3.12.5.19). Let $\mathcal{C} \subset \mathcal{D}$ be an inclusion of simplicial sets that is also a categorical equivalence, and $\mathcal{C}$ is also an $\infty$-category, then $\mathcal{C}$ is a retract of $\mathcal{D}$.

Proof: Include $\mathcal{D}$ into an $\infty$-category by small object argument and (3.12.5.15), we may assume $\mathcal{D}$ is also an $\infty$-category, then we finish by applying (3.12.5.20) for $A = \mathcal{C}$ and $B = \mathcal{D}$.

6 Cartesian Fibrations

Remark (3.12.6.1). The theory of Cartesian fibrations is an analogue of the theory of fibered categories.

Def. (3.12.6.2) [p-Cartesian]. Let $p : X \to S$ be an inner fibration and $f$ is an edge of $X$, then $f$ is called a $p$-Cartesian if the induced map

$$X/f \to X/y \times_{s(y)} S_{p(f)}$$

is a trivial Kan fibration.

Remark (3.12.6.3). For an ordinary category $\mathcal{C}$ and a map $p : N(\mathcal{C}) \to \Delta^1$, then a morphism $f \in \mathcal{C}$ is $p$-Cartesian iff it is Cartesian in the usual sense.

Prop. (3.12.6.4) [Characterization of Cartesian Fibrations]. Let $p : \mathcal{C} \to \mathcal{D}$ be an inner fibration of $\infty$-categories, then an edge $f : Y \to Z \in \mathcal{C}$ is $p$-Cartesian iff for every object $X \in \mathcal{C}$, there is a Cartesian diagram

$$\begin{array}{ccc}
\text{Map}(X,Y) & \longrightarrow & \text{Map}(X,Z) \\
\downarrow & & \downarrow \\
\text{Map}(p(X),p(Y)) & \longrightarrow & \text{Map}(p(X),p(Z))
\end{array}$$

Proof: Cf. [HTT, P131].

Cartesian Fibrations

Def. (3.12.6.5) [Cartesian Fibration]. A Cartesian fibration is an inner anodyne map $p : X \to S$ that for any edge $f : x \to y \in S$ and a vertex $\tilde{y}$ mapping to $y$, there is a $p$-Cartesian edge $\tilde{f}$ with $p(\tilde{f}) = f$. The dual of a Cartesian fibration is called a coCartesian fibration.

Prop. (3.12.6.6). The class of Cartesian fibrations is stable under compositions and base change.

Prop. (3.12.6.7) [Cartesian Fibration and Right Fibration]. Let $p : X \to S$ be an inner fibration, then the following are equivalent:

- $p$ is a Cartesian fibration and the every edge of $X$ is $p$-Cartesian.
- $p$ is a right fibration.
- $p$ is a Cartesian fibration and every fiber $X_s$ is a Kan complex.

Proof: Cf.[HTT, P122].

**Def.(3.12.6.8)[Locally Cartesian Fibration].** A map $X \to S$ of simplicial sets is called a **locally Cartesian fibration** if it is an inner fibration and for every edge $\Delta^1 \to S$, the pullback $X \times_S \Delta^1 \to \Delta^1$ is a Cartesian fibration.

**Prop.(3.12.6.9)[Cartesian and Locally Cartesian].** Let $p : X \to S$ be a locally Cartesian fibration, then the following are equivalent:
- $p$ is a Cartesian fibration.
- Given a composition $fg \simeq h$ in the homotopy category, if $f, g$ are both locally $p$-Cartesian, then $h$ is also locally $p$-Cartesian.
- Every locally $p$-Cartesian edge in $X$ is $p$-Cartesian.

Proof: Cf.[HTT, P124].

**Prop.(3.12.6.10).** Given maps of $\infty$-categories: $C \xrightarrow{p} D \xrightarrow{q} E$, if $q, q \circ p$ are both locally Cartesian fibrations and $p$ maps locally $(q \circ p)$-Cartesian maps to locally $q$-Cartesian maps and for any $Z \in E$, $p$ induces a categorial equivalence $C_Z \to D_Z$, then $p$ is a categorical equivalence.

Proof: Cf.[HTT, P132].

**Prop.(3.12.6.11).** Categorical equivalences between $\infty$-categories are stable under base change of Cartesian fibrations of $\infty$-categories.

Proof: Cf.[HTT, P132].

# 7 Cyclic Homology Theory (欧阳恩林)

**Combinatorial Category**

**Def.(3.12.7.1).** The **Segal category** $\text{Fin}_*$ is the category of pointed finite sets. A morphism is called **inert** iff $|f^{-1}([i])| = 1$ for all $i \neq *$. It is called **active** iff $f^{-1}([*]) = \{*\}$.

A morphism can be uniquely factorized as a composition $gh$, where $h$ is inert and $g$ is active.

**Prop.(3.12.7.2).** There is a morphism $\text{Cut} : \Delta^{op} \to \text{Fin}_*$ where we interpret $[n] \in \text{Fin}_*$ as the set of cut in $[n]$, and

$$\text{Cut}(\alpha)(i) = \begin{cases} j & \text{if there are } j \text{ s.t. } \alpha(j - 1) < i \leq \alpha(j) \\ 0 & \text{otherwise} \end{cases}$$

**Prop.(3.12.7.3).** The category of functors from the $E_\infty = \text{Fin}_*$ to $\text{Cat}$ that

$$X([n]) \xrightarrow{\prod_{i=2}^n X(\rho)} \prod_{i=1}^n X([1]) \quad n \geq 0$$

and $X([0])$ is the final object, is equivalent to the category of symmetric unital monoidal categories with base category $(X([1]))$. (Because the commutativity of morphisms encodes the fact that the tensor action is symmetric).
Similarly, the category of functors from the $\Delta^{op}$ to $\text{Cat}$ that

$$X([n]) \xrightarrow{\prod_{i=2}^{n} X([\rho_i])} \prod_{i=1}^{n} X([1]) \quad n \geq 0$$

is equivalent to the category of symmetric unital monoidal categories ($X([1])$). And it is symmetric iff it factors through Cut:$\Delta^{op} \rightarrow \text{Fin}_*$.  

**Def. (3.12.7.4).** The *Connes cyclic category* $\Delta_C$ is a category containing $\Delta$ that $\text{Aut}_{\Delta_C}([n])$ is $C_{n+1}$. And every morphism $[n] \rightarrow [m]$ in $\Delta_C$ can be uniquely written as the form $\varphi g$, where $\varphi \in \text{Hom}_\Delta([n],[m])$ and $g \in \text{Aut}_{\Delta_C}([n])$.

$\Delta^{op}$ is isomorphic to $\Delta_C$ Cf.[杨樱循环同调 P31], thus $\Delta$ and $\Delta^{op}$ are all subcategories of $\Delta_C$.

**Def. (3.12.7.5).** The category $\Delta_S$ is the category that $\text{Aut}_{\Delta_S}([n]) \cong \mathbb{S}^n$ and every morphism $[n] \rightarrow [m]$ in $\Delta_S$ can be uniquely written as the form $\varphi g$, where $\varphi \in \text{Hom}_\Delta([n],[m])$ and $g \in \text{Aut}_{\Delta_S}([n])$.

**Def. (3.12.7.6).** For a category $C$, a *cyclic object* in $C$ is a functor $\Delta^{op}_C \rightarrow C$.

For example, the functor that maps $[n]$ to $C_{n+1}$ and the functor maps to the pull back of the order of the cyclic, is a cyclic object.

**Hochschild Homology (Jeremy Hahn)**

**Def. (3.12.7.7) [Hochschild Homology Group].** Let $R$ be a commutative ring and $A$ a flat $R$-algebra, $A^{\text{env}} = A \otimes_R A^{\text{op}}$. Then an $A^{\text{env}}$-module is equivalent to an $(A,A)$-bimodule.

If $M$ is an $(A,A)$-bimodule, then we define the *Hochschild homology group* $HH_n(A/R,M) = \text{Tor}^{A^{\text{env}}}_n(M,A)$. And also we denote $HH_n(A/R) = HH_n(A/R,M)$.

$H_n(A,M)$ is a $Z(A)$ module by the action of $Z(A)$ on $M$ and $HH_n$ defines a functor $\text{Alg}_R \rightarrow \text{Mod}_R$.

**Def. (3.12.7.8) [Hochschild Complex].** Let $R$ be a commutative ring and $A$ a flat $R$-algebra, we define $A^{\text{env}} == A \otimes^L_R A^{\text{op}}$, and $HH(A/R) = A \otimes^L_{A^{\text{env}}} A \in D(A)$.

**Def. (3.12.7.9) [Flat Case].** For a flat $R$-algebra $A$ and a $(A,A)$-bimodule $M$, there is a simplicial module $C(A,M)$ called the *Hochschild complex* of $A$ with coefficient in $M$, with $M_n = M \otimes A^n$ that

$$d_i(m,a_1,\ldots,a_n) = \begin{cases} (m_0a_1,a_2,\ldots,a_n) & i = 0 \\ (a_n m_0,a_1,\ldots,a_{n-1}) & i = n \\ (m_0,a_1,\ldots,a_ia_{i+1},\ldots,a_n) & \text{otherwise} \end{cases}$$

$$s_j(m,a_1,\ldots,a_n) = (m,a_1,\ldots,a_{j-1},1,a_{j+1},\ldots,a_n)$$

The homology group of the Moore complex associated to the Hochschild complex is just $HH_n(A,M)$. The Moore complex is of the form

$$\ldots \rightarrow M \otimes A \otimes A \otimes A \xrightarrow{\partial_3} M \otimes A \otimes A \xrightarrow{\partial_2} M \otimes A \xrightarrow{\partial_1} M \xrightarrow{\partial_0} 0 \rightarrow 0 \rightarrow \ldots$$

where

$$\partial_1(m \otimes a) = ma - am, \quad \partial_2(m \otimes a_1 \otimes a_2) = ma_1 \otimes a_2 - m \otimes a_1 a - 2 + a_2 m \otimes a_1$$

$$\partial_3(m \otimes a_1 \otimes a_2 \otimes a_3) = ma - 1 \otimes a_2 \otimes a_3 - m \otimes a_1 a_2 \otimes a_3 + m \otimes a_1 \otimes a_2 a_3 - a_3 m \otimes a_1 \otimes a_2.$$
Proof: □

Example (3.12.7.10).

- \( HH_n(R, R) = R \) if \( n = 0 \) and 0 otherwise.
- \( HH_0(A/R, A/R) = A^{ab} \).
- If \( A \) is commutative, \( HH_1(A, A) \cong \Omega^1_{A/R} \) giving by \( a \otimes x \mapsto adx \) by (4.4.3.4).
- For a symmetric \((A, A)\)-module \( M \), thus we have \( H_1(A, M) = M \otimes_A A^{ab} \) and \( H_1(A, M) = M \otimes_A \Omega^1_{A/R} \). And if \( M \) is flat, \( H_n(A, M) = M \otimes_A H_n(A, A) \).
- \( HH_n(R[X]/R) = \begin{cases} R[X] & n = 0 \\ \Omega^1_{R[X]/R} & n = 1 \\ 0 & \text{otherwise} \end{cases} \).

Example (3.12.7.11) \([HH(F_p/\mathbb{Z})]\). Because \( F_p \otimes_{\mathbb{Z}} F_p = (\mathbb{F}_p^0 \to \mathbb{F}_p) \).

\[
HH_*(\mathbb{F}_p, \mathbb{Z}) \cong \mathbb{F}_p[X_1, X_2, \ldots]/(X_iX_j = \binom{i+j}{i}X_{i+j})
\]

where \( \deg(X_i) = 2i, \partial X_i = 0 \).

Prop. (3.12.7.12). Suppose \( A, B \) are \( R \)-algebras, then

\[
HH(A \otimes^L_R B/R) = HH(A/R) \otimes^L_R HH(B/R).
\]

Cor. (3.12.7.13). \( HH(R[X_1, \ldots, X_n]/R) = \Omega^*_R[X_1, \ldots, X_n]/R \).

Prop. (3.12.7.14). If \( A \) is a commutative \( R \)-algebra, then \( HH(A/R) \) is naturally a commutative dga. In particular, \( HH_*(A/R) \) is a graded ring.

Prop. (3.12.7.15) [Spectral Sequence]. For a commutative ring \( A \) and a symmetric \( A \)-bimodule \( M \), there is a spectral sequence

\[
E^2_{pq} = \operatorname{Tor}_p^R(H_p(A, A), M) \Rightarrow H_{p+q}(A, M).
\]

Hochschild Homology

Prop. (3.12.7.16) [Hochschild-Kostant-Rosenberg]. The isomorphism \( \Omega^1_{A/R} \cong HH_1(A) \) extends to a graded ring map

\[
\Psi : \Omega^*_{A/k} \to H_*(A, A)
\]

. If \( A/R \) be smooth algebra and \( R \) Noetherian, then \( \Psi \) is an isomorphism of graded algebra. Cf.[Weibel P322], [阳恩林循环同调 P133].

Def. (3.12.7.17) [Tsigan’s Double Complex]. For a cyclic objec \( M \) in an Abelian category, let \( t^* \) be the cyclic morphism and \( \partial_n = \sum_{i=0}^{n}(-1)^i d_i \), \( \partial'_n = \sum_{i=0}^{n-1}(-1)^i d_i \), \( N_n = \sum_{k=0}^{n}((-1)^n t^n) \), then
there is a double complex $CC(M)$:

\[
\begin{array}{ccc}
\partial & \downarrow & \partial \\
M_1 & \leftarrow & M_1 \\
\downarrow & N \uparrow & \downarrow \\
M_0 & \leftarrow & M_0 \\
\end{array}
\]

That the column are 2-cyclic. Cf. [Weibel P337]. The first column is called the Hochschild complex of $M$: $C^h(M)$, the second column is called acyclic complex of $M (3.12.7.18) C^a(M)$. And we can even augment a cokernel column on the left, which is the complex of $M$ modulo the cyclic action, called the Conne complex $C^\lambda(M)$.

We define the Cyclic Homotopy Group $HC_n(M) = H_n(TotCC(M))$ and when $M$ is the cyclic module $C(A)(3.12.7.9)$, denote $CC(C(A)) = CC(A)$, $HC_n(A) = HC_n(C(A))$.

**Lemma (3.12.7.18).** The second column is exact and $h = t_{n+1}s_n$ is a null-homotopy. Cf. [Weibel P337].

**Lemma (3.12.7.19).** Notice the rows are in fact a group homology $\text{Hom}(\mathbb{Z}/(n + 1)\mathbb{Z}, M_n)$, thus when $Q \in R$, we have the rows are acyclic because the group homology is killed by $|G|??$, thus $HC_s(M) \cong H_s^\lambda(M)$ are isomorphisms by spectral sequence.

**Prop. (3.12.7.20)[Conne SBI Sequence].** For a cyclic module $M$, there is a long exact sequence

\[
\cdots \to HH_n(M) \overset{L}{\to} HC_n(M) \overset{S}{\to} HC_{n-2}(M) \overset{B}{\to} HH_{n-1}(M) \to \cdots
\]

**Proof:** shift the diagram 2 column right, then there is an exact sequence of double complexes and notice the second column is exact (3.12.7.18), thus we have the kernel is quasi-isomorphic to $C^b(M)$.

So the sequence follows. \( \Box \)

**Cor. (3.12.7.21).** $HC_0(A) = HH_0(A) = A^{ab}$.

When $A$ is commutative, $HC_1(A) = \text{Coker}(HC_0(A) \overset{B}{\to} HH_1(A)) = \Omega^1_{A/R}/dA$ as a $R$ module, because we can verify that $B(a) = a \otimes 1 - 1 \otimes A$.

**Cor. (3.12.7.22).** For a morphism of two cyclic objects, $HH_*(M) \cong HH_*(M')$ iff $HC_*(M) \cong HC_*(M')$. (Use five lemma).

**Def. (3.12.7.23).** A mixed complex $(M, b, B)$ is a complex with $b : M_n \to M_{n-1}$ and $B : M_n \to M_{n+1}$ that makes $M$ into a double chain complex. And there is a Conne double complex associated with this mixed complex. And similarly there is a same SBI sequence associated to the following diagram:

\[
\begin{array}{ccc}
\downarrow & \downarrow & \downarrow \\
M_2 & \leftrightarrow & M_1 \\
\downarrow & B \downarrow & \downarrow \\
M_0 & \leftrightarrow & M_0 \\
\downarrow & \downarrow & \downarrow \\
C_1 & \leftrightarrow & C_0 \\
\downarrow & B \downarrow & \downarrow \\
C_0
\end{array}
\]
From a cyclic object $M$, we notice that the $2k$-th column is acyclic (3.12.7.18), thus there is a snake-like connection homomorphism $B$ that makes $M$ into a mixed complex $BM$. Cf.[Weibel P344]. And the Conne double complex will compute the same cyclic homology with previous defined cyclic homology, Cf.[Weibel P345].

Notice for this $B$, $B_n$ on homology is exactly the composition $BI$.

**Prop.(3.12.7.24).** Let $R$ be a unital commutative ring and $A$ is a commutative $R$-algebra and $M$ is a $A$-module, then there is a natural morphism

$$ M \otimes_A \Omega^n_{A/R} \xrightarrow{\varepsilon_n} H_n(A, M) \xrightarrow{\pi_n} M \otimes_A \Omega^n_{A/R}, $$

such that $\pi_n \circ \varepsilon_n = n!$.

We first define a map $\varepsilon_n : M \otimes \wedge^n A \to H_n(A, M)$ that

$$ \varepsilon_n(m, a_1, \ldots, a_n) = \sum \sgn(\sigma)(m, a_{\sigma^{-1}(1)}, \ldots, a_{\sigma^{-1}(n)}) $$

then define $\varepsilon_n(m \otimes xd a_1 \wedge \cdots \wedge da_n) = \varepsilon_n(mx, a_1, \ldots, a_n)$. And we verify that this map is well-defined and maps into $Z_n(C(A, M), \text{Cf.[}}$[Weibel P344]). And the Conne double complex will compute the same cyclic homology with previous defined $A$-module, then there is a natural morphism

$$ (m, a_1, \ldots, a_n) \mapsto \sum_{i=0}^n (-1)^i \big(1, a_i, \ldots, a_n, m, a_1, \ldots, a_{i-1} \big) - \sum_{i=0}^n (-1)^i \big(a_i, 1, a_{i+1}, \ldots, a_n, m, a_1, \ldots, a_{i-1} \big). $$

Cf.[阳恩林循环同调 P128].

**Prop.(3.12.7.25).** When $A$ is a unital $R$-algebra, there is a commutative diagram

$$ \begin{array}{ccc}
\Omega^n_{A/R} & \xrightarrow{(n+1)d} & \Omega^{n+1}_{A/R} \\
\pi_n & \xrightarrow{d} & \pi_{n+1} \\
HH_n(A) & \xrightarrow{\varepsilon_n} & HH_{n+1}(A)
\end{array} $$

**Proof:** We notice $B = (1 - (-1)^n) sN :$

$$(m, a_1, \ldots, a_n) \mapsto \sum_{i=0}^n (-1)^i \big(1, a_i, \ldots, a_n, m, a_1, \ldots, a_{i-1} \big) - \sum_{i=0}^n (-1)^i \big(a_i, 1, a_{i+1}, \ldots, a_n, m, a_1, \ldots, a_{i-1} \big).$$

Cf.[阳恩林循环同调 P128].

**Cor.(3.12.7.26).** For a commutative unital $R$-algebra $A$, there is a functorial $\varepsilon_n : \Omega^n_{A/R}/d\Omega^{n-1}_{A/R} \rightarrow HC_n(A)$ making the following diagram commutative:

$$ \begin{array}{cccccc}
0 & \xrightarrow{\varepsilon_{n-1}} & \Omega^{n-1}_{A/R} & \xrightarrow{d} & \Omega^n_{A/R} & \xrightarrow{\varepsilon_n} & \Omega^n/d\Omega^{n-1} & \xrightarrow{0} & \Omega^{n-2}/d\Omega^{n-3} & \cdots \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow \\
HC_{n-1} & \xrightarrow{B} & HH_n & \xrightarrow{l} & HC_n & \xrightarrow{s} & HC_{n-2} & \xrightarrow{B} & \cdots
\end{array} $$

which is induced by the cokernel. Cf.[阳恩林循环同调 P130]. When $Q \in R$, $\varepsilon_n$ is a split injection.

**Prop.(3.12.7.27).** When $Q \in R$, $\frac{1}{n!} \pi_n$ induces a morphism of mixed complexes $(BA, \partial, B) \rightarrow (\Omega^*_{A/R}, 0, d)$ by (3.12.7.24), thus there is a natural map

$$ HC_n(A) \rightarrow \Omega^n_{A/R}/d\Omega^{n-1}_{A/R} \bigoplus_{i>0} H^{n-2i}_d(A). $$
Prop. (3.12.7.28) [Morita Invariance]. \( Tr : HH_*(M_r(A), M_r(M)) \cong HH_*(A, M) \) by the trace and inclusion functors. Cf. [Morita Invariance]. In particular, there is an isomorphism \( HH_*(M_r(A)) \cong HH_*(A) \), thus also \( HC_*(M_r(A)) \cong HC_*(A) \) by (3.12.7.20).

Prop. (3.12.7.29) [Karoubi]. \( BG \) is a cyclic group, and then the cyclic homology group \( HC_n(G, A) \cong \bigoplus_{k \geq 0} H_{n-2k}(G, A) \). Cf. [Weibel P339].

Simplicial Homotopy

Prop. (3.12.7.30). For a Kan fibration \( X \), there can be defined a homotopy groups \( \pi_n \) that they agree with \( \pi_i(|X|) \) thus also \( \pi_i(S|X|) \), Cf. [Weibel P263]. Thus we see that \(|BG|\) is truly the Eilenberg-MacLane spaces \( BG \).
3.13 Higher Topos Theory

1 Introduction

Remark (3.13.1.1). This subsection is a place that contains all the heuristic ideas leading to $\infty$-category. It should be deleted after the completion of this section.

Axiom (3.13.1.2) [Grothendieck’s Homotopy Hypothesis]. Spaces and $\infty$-groupoids should be the same.

Axiom (3.13.1.3). Kan complexes and $\infty$-groupoids should be the same.

2 $\infty$-Categories

Def. (3.13.2.1) [$\infty$-Category]. An $\infty$-category is a simplicial set that has lifting property w.r.t all $\Lambda^n_i \to \Delta^n$, where $0 < i < n$.

Prop. (3.13.2.2) [Characterization of $\infty$-Categories]. $\mathcal{C}$ is an $\infty$-category iff the restriction map

$$\text{Map}(\Delta^2, \mathcal{C}) \to \text{Map}(\Lambda^2_1, \mathcal{C})$$

is a trivial Kan fibration.

Proof: This follows immediately from (3.12.3.19). □

Def. (3.13.2.3) [Equivalences]. Two morphisms to an $\infty$-category are called homotopic if they define the same morphism in the homotopy category (3.12.4.10). An equivalence is a morphism that defined an isomorphism in the homotopy category.

Def. (3.13.2.4) [$\infty$-Groupoid]. An $\infty$-groupoid is an $\infty$-category that $h\mathcal{C}$ is a groupoid (3.12.4.10).

Prop. (3.13.2.5) [$\infty$-Groupoids and Kan Complex]. Let $\mathcal{C}$ be a simplicial set, then the following are equivalent:

- $\mathcal{C}$ is an $\infty$-groupoid.
- $\mathcal{C} \to \Delta^0$ is a left fibration.
- $\mathcal{C} \to \Delta^0$ is a right fibration.
- $\mathcal{C}$ is a Kan complex.

Proof: 1, 2 are equivalent by (3.13.10), and dually 1, 3 are equivalent, and $4 = 2 + 3$. □

Prop. (3.13.2.6) [Join]. The join of two $\infty$-categories is also an $\infty$-category.

Proof: Given a morphism $p : \Lambda^n_i \to S \star S'$, if the image is in $S$ or $S'$, then it can be extended to $\Delta^n$ by hypothesis. Then we may assume that it maps $\{0, \ldots, j\}$ into $S$ and $\{j + 1, \ldots, n\}$ into $S'$, then we restricts $p$ to get a morphism $\Delta^{[0 \ldots j]} \to S, \Delta^{[j + 1 \ldots n]} \to S'$, which determines a map $\Delta^n \to S \star S'$ extending $p$. □

Prop. (3.13.2.7) [Homotopic Maps]. If $X$ is an $\infty$-category, then so does $X^B$ for any simplicial set $B$, by (3.12.3.26).

And we can call two maps in $\text{Map}(B, X)$ homotopic if they are homotopic as vertices in $X^B$ (3.13.2.3).
Lemma (3.13.2.8). Let $p : C \to D$ be a left fibration of $\infty$-categories and $f : X \to Y$ be a morphism that $p(f)$ is an equivalence in $D$, then $f$ is an equivalence in $D$. Compare with (3.1.7.8).

Proof: Let $\overline{g}$ be a homotopy inverse to $f$, then there is a 2-complex

$$
\begin{array}{ccc}
p(f) & \rightarrow & p(Y) \\
p(X) & \searrow & p(X) \\
\downarrow & & \downarrow \\
\bigcirc & \Downarrow & \bigcirc
\end{array}
$$

and by left fibration property lifts to a 2-complex

$$
\begin{array}{ccc}
f & \rightarrow & Y \\
g & \searrow & \bigcirc \\
\bigcirc & \Downarrow & \bigcirc \\
X & \rightarrow & X
\end{array}
$$

So $f$ admits a left homotopy inverse, and by the same reason, $g$ admits a left homotopy inverse, thus $g$ has a left homotopy inverse, and it can be chosen to be $f$. □

Lemma (3.13.2.9) [Equivalence Lifts via Left Fibrations]. Let $p : C \to D$ be a left fibration of $\infty$-categories, if $Y \in D$ and $x \in C$ and $f : X \to p(Y)$ is an equivalence, then $f$ can be lifted to a morphism in $C$. (Which is also an equivalence by (3.13.2.8)).

Proof: □

Prop. (3.13.2.10) [Equivalence and Left Extension]. Let $C$ be an $\infty$-category and $\varphi$ an edge, then $\varphi$ is an equivalence iff for any $n \geq 2$ and every map $\Lambda^n_0 \to C$ that $f_0|\Delta^{0,1} = \varphi$, there exists an extension of $f_0$ to $\Delta^n$.

Proof: If $\varphi$ is an equivalence, then consider the diagram

$$
\begin{array}{ccc}
\{0\} & \rightarrow & C/\Delta^{n-2} \\
\downarrow & & \downarrow \varphi' \\
\Delta^1 & \rightarrow & C/\partial \Delta^{n-2}
\end{array}
$$

Because $C/\partial \Delta^{n-2} \to C$ is right fibration (3.12.3.25), and by the dual of (3.13.2.8), $\varphi'$ is an equivalence, thus by the dual of (3.13.2.9) the dotted arrow exists.

Conversely, if the condition holds, then we can use a diagram $\Lambda^n_0 \to C$ to find a morphism $\psi$ that $\psi \circ \varphi \cong \text{id}$, and we can also use a diagram $\Lambda^3_0 \to C$ to witness the fact $\varphi \circ \psi \cong \text{id}$, so $\varphi$ is an equivalence. □

Cor. (3.13.2.11). An equivalence in $\text{Map}(K, C)$ is equivalent to a map $K \times \Delta^1 \to C$ that $\{x\} \times \Delta$ are all mapped to equivalences in $C$.

Proof: Cf. [HTT, P106]. □

Def. (3.13.2.12) [Space of Morphisms]. For vertices $x, y$ in a simplicial set $S$, we want to defines a representative for $\text{Map}_h S(x, y)$ other than $\text{Map}_S S(x, y)$. We define the space of right morphisms

$$
\text{Hom}_S^R(x, y) = S/y \times_S \{x\}.
$$
The definition is not symmetric, instead, we define the **space of left morphisms** \( \text{Hom}_L^S(x,y) = \left( \text{Hom}_R^{\text{op}}(x,y) \right)^{op} \).

Also we define \( \text{Hom}_S(x,y) = \{x\} \times_S S^\Delta^1 \times_S \{y\} \), then there are natural inclusions:

\[
\text{Hom}_R^S(x,y) \twoheadrightarrow \text{Hom}_S(x,y) \hookrightarrow \text{Hom}_L^S(x,y).
\]

**Prop. (3.13.2.13).** If \( C \) is an \( \infty \)-category and \( x, y \in C \), then \( \text{Hom}_C^R(x,y) \) is a Kan complex.

**Proof:** This is obvious, because the right lifting diagram w.r.t. \( \Lambda^n_j \subset \Delta^n, 0 < j < n \) is equivalent to an extension \( \Lambda^n_j \times \Delta^0 \subset \Delta^{n+1} \) that satisfies \( \bar{u}|_{\Delta^0} = x \). It can be solved by a two-step extension where the first is by identity extension and then extend using inner fibration property. \( \square \)

**Prop. (3.13.2.14) [Space of Morphisms Homotopic].** When \( S \) is an \( \infty \)-category, the inclusions defined in (3.13.2.12) are homotopy equivalences.

**Proof:** Cf. [HTT, 4.2.1.8]. \( \square \)

**Prop. (3.13.2.15).** Let \( p : C \to D \) be an inner fibration of \( \infty \)-categories, then the the induced maps on the spaces of right morphisms are Kan fibrations.

**Proof:** Since \( p \) is an inner fibration, the induced map \( \tilde{\varphi} : C/Y \to D/p(Y) \times_D C \) is a right fibration by (3.12.3.25), and the morphism on \( \text{Hom}_C^R(X,Y) \) is obtained from \( \tilde{\varphi} \) by restricting to fiber over \( X \), thus also a right fibration. And by (3.13.2.13) and (3.12.3.31). \( \square \)

**Prop. (3.13.2.16) [Mapping Space].** Let \( C, D \) be \( \infty \)-categories and \( K, K' \) simplicial sets, then

- \( \text{Map}(K,C) \) is also an \( \infty \)-category.
- If \( f : C \to D \) is a categorical equivalence, then the induced map \( \text{Map}(K,C) \to \text{Map}(K,D) \) is also a categorical equivalence.
- If \( g : K \to K' \) is a categorical equivalence, then the induced map \( \text{Map}(K',C) \to \text{Map}(K,C) \) is also a categorical equivalence.

**Proof:** 1 follows from (3.12.3.20). 2, 3 follows from [HTT, P94]. \( \square \)

**Prop. (3.13.2.17).** Let \( C \) be an \( \infty \)-category and \( p : K \to C \) be an morphism, then the projection \( C_{p/} \to C \) is a left fibration. In particular, \( C_{p/} \) is itself an \( \infty \)-category.

**Proof:** We use the proposition (3.12.3.25) in case \( S = \Delta^0, A = \emptyset, X = C \). \( \square \)

**Lemma (3.13.2.18).** Let \( C \to D \) be a fully faithful map of \( \infty \)-categories and a diagram \( K \to C \), the map of Kan complexes (3.12.2.17)

\[
C_{p/} \times_C \{x\} \to D_{pj/} \times_D \{p(x)\}
\]

is a homotopy equivalence.

**Proof:** Cf. [HTT, P134]. \( \square \)

**Prop. (3.13.2.19) [Invariance of Undercategories].** Let \( p : C \to D \) be a weak equivalence of \( \infty \)-categories and let \( j : K \to C \) be a map, then the induced map \( C_{j/} \to D_{pj/} \) is a categorical equivalence.
Proof: There is a factorization \( C_j/ \xrightarrow{f} \mathcal{D}_{pj}/ \times \mathcal{C} \xrightarrow{g} \mathcal{D}_{pj}/. \) (3.13.2.18)(3.13.2.17) shows \( C_j/ \) and \( \mathcal{D}_{pj}/ \times \mathcal{C} \) are fiberwise equivalent left fibrations over \( \mathcal{C} \), thus by (3.12.6.7) and (3.12.6.10), \( f \) is a categorical equivalence. Also, \( g \) is a categorical equivalence by (3.12.6.11). So we are done. \( \square \)

**Prop. (3.13.2.20)** [Lifting of Homotopies]. Let \( p : \mathcal{C} \rightarrow \mathcal{D} \) be a categorical equivalence of \( \infty \)-categories and \( A \subset B \) be an inclusion of simplicial sets. Let \( f_0 : A \rightarrow \mathcal{C}, g : B \rightarrow \mathcal{D} \) be any maps that \( h_0 : A \times \Delta^1 \rightarrow \mathcal{D} \) be an equivalence between \( g|_A \) and \( p \circ f_0 \), then there exists a map \( B \rightarrow \mathcal{C} \) and an equivalence \( h : B \times \Delta^1 \rightarrow \mathcal{D} \) between \( g \) and \( p \circ f \) that \( h_0 = h|_{A \times \Delta^1} \).

**Proof:** Working with simplexes, it suffices to prove for \( A = \partial \Delta^n \subset B = \Delta^n \). The case \( n = 0 \) is true because categorical equivalence is essentially surjective. For \( n > 0 \), we need to construct \( h \) from \( h|_{\Delta^n \times \{0\}} \prod \partial \Delta^n \times \Delta^1 \), and this is a composition of pushout of \( \Lambda_{n+1}^k \subset \Delta^{n+1} \). For \( k \neq 0 \), the extension is clear because \( \mathcal{D} \) is \( \infty \)-category, and for \( k = 0 \), we need to use [HTT, P136]. \( \square \)

**Def. (3.13.2.21)** [Correspondence]. Let \( \mathcal{C}, \mathcal{D} \) be \( \infty \)-categories, an correspondence between \( \mathcal{C}, \mathcal{D} \) is defined to be an \( \infty \)-category \( \mathcal{M} \) and a map \( \mathcal{M} \rightarrow \Delta^1 \mathcal{C} \cong \mathcal{M}_0 \) and \( \mathcal{D} \cong \mathcal{M}_1 \).

**Prop. (3.13.2.22)** [Equivalent Definition of Adjoint]. Cf.[HTT, P5.2.2.8].

**Prop. (3.13.2.23).** Left adjoints preserves all colimits and right adjoints preserves all limits.

**Def. (3.13.2.24)** [Localization Category]. A full subcategory \( \mathcal{C}_0 \) of \( \mathcal{C} \) is called a localization of \( \mathcal{C} \) if the inclusion has a left adjoint.

**\( n \)-Categories**

**Def. (3.13.2.25)** [\( n \)-Categories]. Let \( \mathcal{C} \) be a simplicial set and \( n \geq -1 \), then \( \mathcal{C} \) is called an \( n \)-category if it is an \( \infty \)-category and:

- Given any maps \( f, f' : \Delta^n \rightarrow \mathcal{C} \) that are homotopic (3.13.2.7) relative to \( \partial \Delta^n \), then \( f = f' \).
- For any \( m > n \) and maps \( f, f' : \Delta^m \rightarrow \mathcal{C} \) that coincide on \( \partial \Delta^n \), then \( f = f' \).

Also \( \mathcal{C} \) is called an \((-2)\)-category iff it is isomorphic to \( \Delta^0 \).

The definition of an \( n \)-category is equivalent to the following: if \( f, f' : K \rightarrow \mathcal{C} \) satisfies \( f|_{sk^nK} \) is homotopic to \( f'|_{sk^nK} \) relative to \( sk^{n-1}K \), then \( f = f' \).

**Prop. (3.13.2.26).** A \((-1)\)-category is seen to be isomorphic to \( \emptyset \) or \( \Delta^0 \). A 0-category is equivalent to the nerve of a partially ordered set.

**Prop. (3.13.2.27).** If \( \mathcal{C} \) is an \( n \)-category and \( m > n + 1 \), then the restriction map \( \text{Hom}(\Delta^m, \mathcal{C}) \rightarrow \text{Hom}(\partial \Delta^m, \mathcal{C}) \) is bijective. (use \( \infty \)-category property to extend).

**Prop. (3.13.2.28)** [Usual Category as 1-Category]. For a simplicial set \( S \), the following are equivalent:

- \( u : S \rightarrow N(hS)(3.12.4.7) \) is an isomorphism of simplicial sets.
- There is a small category \( \mathcal{C} \) that \( S \cong N(\mathcal{C}) \).
- \( S \) is a 1-category.
Proof: It suffices to show $3 \to 1$: we induct on the dimension: $n = 0$ is trivial and $n = 1$ follows from the definition of 1-category (3.13.2.25). For $n > 1$, the injectivity of $u$ follows from induction hypothesis and (3.13.2.25), and for surjectivity, for a map $\Delta^n \to N(hS)$, choose $0 < i < n$ and let lift $\Lambda^i_n$ to $S$, then use the fact $S$ is an $\infty$-category to lift to $\Delta^n$, and now it coincide on $N(hS)$ because it is a nerve of a category.

Prop. (3.13.2.29). If $\mathcal{C}$ is an $n$-category, then for any simplicial set $X$, $\mathcal{C}^X$ is also an $n$-category.

Proof: This is because $sk^p(K \times X) \subset sk^p(K) \times X$ for any simplicial set $K$ and integer $p$, and use (3.13.2.25).

Prop. (3.13.2.30). Let $n \geq 1$ and $\mathcal{C}$ an $\infty$-category, then $\mathcal{C}$ is an $n$-category iff it satisfies the unique lifting property w.r.t. the inclusion $\Lambda_i^m \subset \Delta^m$, where $0 < i < m$.

Proof: Cf. [HTT, P109].

Def. (3.13.2.31) $[n$-Truncated Kan Complex]. Let $X$ be a Kan complex and $k \geq -1$, then a Kan complex is called $k$-truncated if for every $i > k$ and every point $x \in X$, we have $\pi_i(X, x) \cong *$. And it is called $(\sim 2)$-truncated if it is contractible.

Prop. (3.13.2.32). A $(-1)$-truncated Kan complex is either empty or contractible. A 0-contractible Kan complex is a Kan complex that $X \to \pi_0(X)$ is a homotopy equivalence.

Proof: ?

Prop. (3.13.2.33) $[Equivalent to an n$-Category]. Let $\mathcal{C}$ be an $\infty$-category and $n \geq -1$, then the following conditions are equivalent:

- There is a minimal model $\mathcal{C}' \subset \mathcal{C}$ that is $n$-truncated.
- $\mathcal{C}$ is categorically equivalent to an $n$-truncated category.
- For any $X, Y \in \mathcal{C}$, the mapping space $\text{Map}(X, Y)$ is $(n-1)$-truncated.

Proof: Cf. [HTT, P112].

Cor. (3.13.2.34). A Kan complex is categorically equivalent to an $n$-category iff it is $n$-truncated.

Proof: Cf. [HTT, P113].

Cor. (3.13.2.35). Let $\mathcal{C}$ be an $\infty$-category and $K$ a simplicial set, if $\text{Map}(C, D)$ is $n$-truncated for any objects $C, D \in \mathcal{C}$, then the $\infty$-category $\mathcal{C}^K$ has the same property.

Proof: Cf. [HTT, P114].

3 $\infty$-Category of $\infty$-Categories

4 Limits and Colimits

5 Presentable and Accessible $\infty$-Categories

Def. (3.13.5.1) $[Presentable \ infty$-Category]. An $\infty$-category is called presentable if it is accessible and admits small limits.

Prop. (3.13.5.2). A presentable $\infty$-category also admits all small limits, Cf. [HTT, P5.5.2.4].
Prop. (3.13.5.3). An $\infty$-category is presentable iff it is an accessible localization of an $\infty$-category of presheaves, Cf.[HTT, P5.5.1.1].

Prop. (3.13.5.4) [Adjoint Functor Theorem]. Let $F : C \to D$ be a functor between presentable $\infty$-categories, then

- $F$ admits a right adjoint iff it preserves small colimits.
- $F$ admits a left adjoint iff it preserves small limits and $\kappa$-filtered colimits for some regular cardinal $\kappa$.

Proof: [HTT. 5.5.2.9].

6 $\infty$-Algebras

7 Topological Cyclic Homology(Scholze)
3.14 Stable $\infty$-Categories

1 Stable $\infty$-Categories

Main References are [HTT, Chap8].

Def. (3.14.1.1) [Stable $\infty$-Category]. Stable $\infty$-category is a "linearized $\infty$-category" for doing geometry. A Stable $\infty$-category is an $\infty$-category that
- There exists a zero element.
- Every morphism $g$ in $\mathcal{C}$ admits a fiber and cofiber over the zero object.
- A triangle in $\mathcal{C}$ is a fiber sequence iff it is a cofiber sequence.

Def. (3.14.1.2) [Suspensions and Loops].

Prop. (3.14.1.3). The suspension and loop are functors from $\mathcal{C} \to \mathcal{C}$ that are mutually inverse equivalences.

Proof: Cf.[HTT, 4.3.1.5]. □

Prop. (3.14.1.4) [Stable $\infty$-Categories and Triangulated Categories]. The distinguished triangles in $h\mathcal{C}$ endow $h\mathcal{C}$ with the classical structure of triangulated category.

Prop. (3.14.1.5) [HA.1.1.3.4]. A stable $\infty$-category admits all finite limits and colimits. And pullback squares and pushout squares coincide.

Prop. (3.14.1.6). Let $\mathcal{C}$ be a pointed $\infty$-category, then the following are equivalent:
- $\mathcal{C}$ is stable.
- $\mathcal{C}$ admits finite colimits, and the suspension functor $\Sigma : \mathcal{C} \to \mathcal{C}$ is an equivalence.

Proof: Cf.[HA, 1.4.2.27]. □

Def. (3.14.1.7) [Exact Functors]. A functor $F : \mathcal{C} \to \mathcal{D}$ between stable $\infty$-categories is called exact if the following equivalent definitions hold:
- $F$ preserves fiber sequences.
- $F$ is left exact.
- $F$ is right exact.

Prop. (3.14.1.8). Let $\mathcal{C}at^\mathbb{E}_{\infty} \subset \mathcal{C}at_{\infty}$ be the subcategory of all stable $\infty$-categories and exact functors, then it admits all small limits and small filtered colimits, and they are preserved by the inclusion.

Proof: Cf.[HA1.1.4.4., 1.1.4.6.] □

Def. (3.14.1.9) [T-Structure]. A $T$-structure on a stable $\infty$-category $\mathcal{C}$ is a pair of full subcategories $\mathcal{C}_{\geq 0}, \mathcal{C}_{\leq 0}$ that

Prop. (3.14.1.10). For any $n \in \mathbb{Z}$, $\mathcal{C}_{\leq n} \subset \mathcal{C}$ is a localization, thus admits a left adjoint $\tau_{\leq n}$, called the truncation functor. Dually for $\tau_{\geq n}$.

Proof: Cf.[HA, P1.2.1.5]. □

Def. (3.14.1.11) [Heart]. The heart $\mathcal{C}^{\flat} \subset \mathcal{C}$ is defined to be the full subcategory of $\mathcal{C}_{\leq 0} \cap \mathcal{C}_{\geq 0} \subset \mathcal{C}$.

2 Monoidal $\infty$-Categories
4 | Commutative Algebras

4.1 Commutative Algebra I

Main References are [A-M69], [Mat80], [Sta]Chap10, [Commutative Algebra with a View Towards Algebraic Geometry] and [Wei94]Chap4.

Commutative rings are studied in this subsection.

Notations(4.1.0.1).

• All rings and algebras in this section is assumed to be commutative.

1 Basics

Def.(4.1.1.1) [Ideals]. For \( R \in \mathbb{C}\text{Ring} \), an ideal of \( R \) is a subgroup \( I \leq R \) that is a left ideal. The category of ideals of \( R \) is denoted by \( \text{Ideal}(R) \).

Prop.(4.1.1.2) [Quotients]. For \( R \in \mathbb{C}\text{Ring}, I \in \text{Ideal}(R) \), there is a quotient ring \( R/I \in \mathbb{C}\text{Ring}_R \) with the universal property: any \( f : R \to R' \in \mathbb{C}\text{Ring} \) that vanishes on \( I \) factors through \( R/I \).

Proof:

Prop.(4.1.1.3). The quotient map induces an order-preserving bijection of ideals of \( A/I \) and ideals of \( A \) containing \( I \).

Prop.(4.1.1.4) [Prime Avoidance]. Let \( R \in \mathbb{C}\text{Ring}, I \in \text{Ideal}(R) \), and \( p_i \) are f.m. prime ideals that \( I \not\subseteq p_i \) for any \( i \), then \( I \not\subseteq \cup p_i \).

Proof: Use induction on the number of primes \( n \). For \( n = 1 \) this is trivial. For \( n > 2 \), let \( z_i \in I \setminus \cup_{j \neq i} P_j \). Now consider \( z = z_1 \cdot z_{n-1} + z_n \). If \( z \in P_i \) for some \( i \leq n \), then \( z_{n-1} \in P_i \), contradiction. If \( z \in P_n \), then some \( z_i, i < n \) is in \( P_n \) because \( P_n \) is a prime ideal, contradiction. □

Prop.(4.1.1.5) [Existence of a Maximal Ideal]. Any non-zero commutative ring has a maximal ideal.

Proof: Use Zorn’s lemma, the union of a chain of ideals is an ideal. □

Cor.(4.1.1.6). Any non-trivial ideal is contained in a maximal ideal.

Proof: If \( I \subset A \) is a non-trivial ideal, then \( A/I \) is a non-zero ring, thus \( A/I \) has a maximal ideal, which corresponds to a maximal ideal of \( A \) containing \( I \).

Prop.(4.1.1.7). If \( r(I) \) and \( r(J) \) are coprime, then \( I, J \) are coprime.
Proof: As \( a + b = 1 \), and \( a^m \in I, b^n \in J, 1 = (a + b)^{m+n} \in I + J \). \( \square \)

**Def. (4.1.1.8)** [Local Ring]. A local ring is a commutative ring \( R \) that has only one maximal ideal. Equivalently, there is a prime ideal \( \mathfrak{m} \) that any element in \( R \setminus \mathfrak{m} \) is invertible.

**Proof:** If \( \mathfrak{m} \) is the maximal ideal, then for any \( x \in R \), if \( (x) \) is not all of \( R \), then \( x \) is contained in a maximal ideal by (4.1.1.5), which can only be \( \mathfrak{m} \). Conversely, if there is a prime ideal \( \mathfrak{m} \) that any element in \( R \setminus \mathfrak{m} \) is invertible, then clearly every non-trivial ideal is included in \( \mathfrak{m} \). \( \square \)

**Prop. (4.1.1.9).** Any quotient of a local ring is also a local ring.

**Def. (4.1.1.10)** [Local Ring Map]. A map between two local rings are called local ring map if it maps non-invertible elements to non-invertible elements, equivalently, \( f^{-1}(\mathfrak{m}_S) = \mathfrak{m}_R \).

**Def. (4.1.1.11)** [Ideal of Definition]. In a Noetherian local ring \( (R, \mathfrak{m}) \), an ideal \( I \subset R \) is called an ideal of definition if \( \sqrt{I} = \mathfrak{m} \).

**Prop. (4.1.1.12)** [Ideals of Products and Filters]. If \( F_i, i \in I \) is a collection of fields, then the prime ideals in the ring \( \prod F_i \) is in bijection with the ultrafilters on \( I \), where the ultrafilter \( \mathcal{F} \) corresponds to the ideal \( p_{\mathcal{F}} = \{ (a_i) \mid \text{the set of coordinates that } a_i = 0 \text{ is in } \mathcal{F} \} \). And in the same way, ideals of \( \prod F_i \) corresponds to the filters on \( I \).

**Proof:** Clearly \( p_{\mathcal{F}} \) is an ideal, and if \( \mathcal{F} \) is an ultrafilter, let \( Z(a) \) be the coordinates that \( a \) is zero on, and notice \( Z(ab) = Z(a) \cup Z(b) \), then \( \mathfrak{ab} \in \mathcal{P} \) iff \( a \in \mathfrak{p} \) or \( b \in \mathfrak{p} \), by (1.1.8.7), so it is a prime ideal. Conversely, notice that any two \( a, b \) with \( Z(a) = Z(b) \) differs by a unit, so \( \mathcal{F}_p = \{ Z(a) \mid z \in p \} \) is easily checked to be a filter. And if \( p \) is a prime, then for any \( A \subset I \), let \( a, b \in \prod F_i \) be that \( Z(a) = A, Z(b) = I - A \), then \( \mathfrak{ab} = 0 \in p \), so \( a \in \mathfrak{p} \) or \( b \in \mathfrak{p} \). \( \square \)

**Def. (4.1.1.13)** [Torsion-Free Modules]. Let \( S \subset A \) be a set in a commutative ring, then an \( A \)-module \( M \) is called \( S \)-torsion-free if for any \( \{ x \in M | Sx = 0 \} = 0 \).

**Prop. (4.1.1.14)** [Maximal Torsion-Free Quotient]. Let \( S \subset A \) be a set, the functor from the category of torsion-free \( A \)-modules to the category of \( A \)-modules has a left adjoint, called the maximal \( S \)-torsion-free quotient.

**Proof:** A quotient of \( M \) is determined by the kernel. It suffices to prove if \( M/N_1, M/N_2 \) are both \( S \)-torsion-free, then \( M/N_1 \cap N_2 \) is also \( S \)-torsion-free: This is easy. \( \square \)

**Prop. (4.1.1.15).** Let \( A \) be a ring and \( B \) a finite \( A \)-algebra. if \( A \to B \) is epimorphism in the category of rings, then \( A \to B \) is surjective.

**Proof:** Notice that \( h^B \to h^A \) is injective iff \( h^B \times_{h^A} h^B \cong h^B \), or equivalently, \( B \times_A B \to B \) is an isomorphism. Now we can localize \( A \) at maximal ideals, thus we can assume \( A \) is local, with maximal ideal \( \mathfrak{m} \) and residue field \( k \). And then use Nakayama lemma, it suffices to show that \( k \to B/\mathfrak{m} = C \) is surjective. But \( C \times_k C \cong C \), so \( \dim_k C = 1 \) or 0, which means \( k \to C \) is surjective. \( \square \)

**Def. (4.1.1.16)** [Locally Nilpotent]. A locally nilpotent ideal is an ideal consisting of nilpotent elements.

**Prop. (4.1.1.17).** If \( I \) is a locally nilpotent ideal of \( A \), then \( 1 + I \to 1 + I : x \mapsto x^n \) is an isomorphism.

**Proof:** The converse is given by \( x \mapsto (1 + x)^{1/n} = 1 + (\frac{1}{1^n})x + (\frac{1}{2^n})x^2 + \ldots \). \( \square \)

**Cor. (4.1.1.18).** If \( I \) is a locally nilpotent ideal of \( A \), then a unit in \( A \) is an \( n \)-th power if it is an \( n \)-th power in \( A/I \).

**Proof:** If \( a \equiv b^n \mod I \), then \( b \) is also a unit, and \( ab^{-n} = c^n \) for some \( n \) by (4.1.1.17), thus \( a \) is a \( n \)-th power. \( \square \)
Tensor Product, Limits and Colimits

Remark (4.1.1.19) [Tensor Product]. Tensor product is defined in (2.2.4.13). Notice that in case the rings are all commutative, there are no need to distinguish between left and right modules.

Def. (4.1.1.20) [Tensor Algebras]. For a module $M$ over a commutative ring $R$, we define the

- **tensor algebra** operator from $\text{Mod}_R$ to graded algebras over $R$ that is left adjoint to the forgetful functor. It can be defined as follows:
  $$T(M) = \bigoplus_{n \geq 0} \otimes^n M$$
  as the module, and the algebra structure determined by the canonical map $\otimes^m M \times \otimes^n M \to \otimes^{m+n} M$.

- **exterior product** $\wedge^k M$ as the module with the universal property that $\text{Hom}_B(\wedge^k M, N)$ is the set of all morphisms $M^n \to N$ that vanishes on all elements that have two equal coordinates.

- **exterior algebra** operator $\wedge$ from $\text{Mod}_R$ to the category of strict graded commutative algebras over $R$ that is left adjoint to the forgetful functor. It can be defined as follows:
  $$\wedge(M) = T(M)/(x \otimes x),$$
  where $x \in M$, or equivalently $\wedge(M) = \bigoplus_{k \geq 0} \wedge^k(M)$.

- **symmetric algebra** operator $S$ from $\text{Mod}_R$ to $\text{C} \text{Ring}_R$ that is left adjoint to the forgetful functor. It can be defined as follows: $\wedge(M) = T(M)/(x \otimes y - y \otimes x)$ where $x, y \in M$.

Cor. (4.1.1.21). The construction of $T(M), \wedge M$ and $\text{Sym}(M)$ commutes with all colimits, because they are all left adjoints.

Prop. (4.1.1.22) [Tensor Product and Quotient]. Let $R$ be a commutative ring and $I, J$ be ideals of $R$, then $R\llcorner I \otimes_R R\llcorner J \cong R\llcorner (I + J)$.

Proof: This follows from the universal property of quotient and tensoring.

Prop. (4.1.1.23). There is a pullback square

$$
\begin{array}{ccc}
R/I \cap J & \longrightarrow & R/I \\
\downarrow & & \downarrow \\
R/J & \longrightarrow & R/(I + J)
\end{array}
$$

Proof: The pullback is just the elements in $R/I \times R/J$ that map to the same element in $R/(I + J)$. If $(x + I, y + J)$ maps to the same element $z + I + J$, then $x = y + i + j$, so $x - i = y + j$, and the pullback lies in the image of $\Delta : R \hookrightarrow R/I \times R/J$. Now the kernel is just $I \cap J$.

Prop. (4.1.1.24) [Filtered Colimits of Modules are Exact]. Let $\mathcal{I}$ be an index category that each connected components of $\mathcal{I}$ is filtered, then taking colimits over $\mathcal{I}$ is exact in the category $\text{Mod}_R$ of modules over a ring $R$.

Proof: It is clearly right exact. To check left exactness, Cf. [Sta]04B0.?

Cor. (4.1.1.25) [Filtered Colimits of Abelian Groups are Exact]. Filtered colimits are exact in $\text{Ab}$.

Prop. (4.1.1.26). Let $k$ be a field and $A, B$ be $k$-algebras and let $b \subset A \otimes_k B$ be an ideal. Then among the ideals $a \subset A$ that $b \subset a \otimes_k B$, there exists a smallest one.

Proof: Choose a $k$-basis of $B$, then the smallest ideal $a$ is just the ideal generated by all the $A$-coefficients of elements of $b$. 

□
**Localization**

**Def. (4.1.1.27) [Localization as Filtered Colimit].** Let \( A \) be a commutative ring and \( S \) be a multiplicatively closed subset of \( A \) containing 1 and not containing 0, the localization \( S^{-1}A \) is defined to be a ring over \( A \) that any ring map \( A \to B \) that maps elements of \( S \) to units factors through \( S^{-1}A \).

\( S^{-1}A \) can be constructed as

\[
\lim_{s \in S} A
\]

where the ordering is defined to be \( s < t \) if \( t = sr \) for some \( r \in S \), and if \( t = sr \), there is a map from \( A_s \) to \( A_t \) defined by multiplying by \( r \). This is easily seen to be a filtered colimit. There is easily seen to be the localization.

**Prop. (4.1.1.28) [Localization is exact].** \( S^{-1} \) is an exact functor from \( \text{Mod}_R \) to \( \text{Mod}_R \). Because it is a filtered colimit (3.3.2.27)(4.1.1.24).

**Cor. (4.1.1.29).** \((R/I)_P \cong R_P/I_RP\), in particular, \( k(R/P) \cong R_P/P_RP\).

**Def. (4.1.1.30) [Total Ring of Fractions].** For any ring \( R \), the set of non-zerodivisors in \( R \) is a multiplicatively closed set \( S \), and the localization \( \text{Frac}(R) = S^{-1}R \) is called the **total ring of fractions** of \( R \).

**Prop. (4.1.1.31) [Localization Along an Ideal].** Let \( I \) be an ideal of \( A \), then the localization of \( A \) along \( I \) is the ring \( \tilde{A} \) that \( \text{Spec} \tilde{A} \) is the localization of \( \text{Spec} A \) along \( V(I) \) as defined in(3.8.4.20)(because \( \text{Spec} A \) is spectral, by(3.8.4.13)).

Equivalently, it can be defined as \( \tilde{A} = S^{-1}A \), where \( S = A \setminus (\cup_{p \in V(I)} p) \). (It can be checked that \( S \) is multiplicatively closed).

Notice then \( I \subset \text{rad} \tilde{A} \).

For \( f \in A \), we call the localization of \( A \) along \( f \) the **\( f \)-localization** of \( A \). In fact, it is the universal \( A \)-algebra that \( f \in \text{rad} \tilde{A} \).

**Prop. (4.1.1.32).** Let \( R \) be a commutative ring, \( f_1, \ldots, f_n \in R \), and \( M \) an \( R \)-module, then \( M \to \bigoplus_i M_{f_i} \) is injective iff \( M \to \bigoplus_i M : m \mapsto (mf_1, \ldots, mf_n) \) is injective.

**Proof:** Cf.[Sta]0565. \(\square\)

**Prop. (4.1.1.33).** For any ring \( A \), \( A \to \prod A_m \) is injective, where \( m \) are maximal ideals of \( A \).

For a domain \( A \), \( A = \bigcap A_m \) inside the fraction field of \( A \), where \( m \) are maximal ideals of \( A \).

**Proof:** if \( g \in \text{Frac}(A) \) is in the RHS, then \( I = \{ x \in A | xg \in A \} \) is an ideal of \( A \) not contained in any maximal ideal, thus \( I = 1(4.1.1.6) \), and thus \( g \in A \). \(\square\)

**Lemma (4.1.1.34).** Let \( R \) be a ring and \( \mathfrak{p} \) be a prime, then there exists an \( f \in R, f \notin \mathfrak{p} \) that \( R_f \subset R_{\mathfrak{p}} \), if any of the following holds:

- \( R \) is a domain.
- \( R \) is Noetherian.
- \( R \) is reduced and has f.m. irreducible components.

**Proof:** Cf.[Sta]0BX1. \(\square\)
Def. (4.1.1.35) [Identifying Local Rings]. A ring map \( A \to B \) is said to identify local rings if for every prime \( q \subset B \), the map \( A_{\varphi^{-1}(q)} \to B_q \) is an isomorphism.

Prop. (4.1.1.36). The property of identifying local rings is stable under base change and composition. (This is immediate from (4.1.1.37)).

Prop. (4.1.1.37) [Tensor Product and Localization]. For a ring map \( R \to S \), let \( q \subset \text{Spec} \, S \), \( p = q \cap R \), then \( (M \otimes_R S)_q = M_p \otimes_{R_p} S_q \) for any \( R \)-module \( M \).

Proof: \( (M \otimes_R S)_q = M \otimes_R S_q = M \otimes_R R_p \otimes_{R_p} S_q = M_p \otimes_{R_p} S_q \). □

Noetherian

Def. (4.1.1.38) [Noetherian Module]. Let \( R \) be a commutative ring and \( M \) an \( R \)-module, then \( M \) is called Noetherian iff every ascending chain of submodules stabilizes.

\( R \) is called a Noetherian ring iff \( R \) is Noetherian over itself.

Prop. (4.1.1.39). Let \( R \in \mathcal{C} \text{Ring} \) and \( 0 \to M_1 \to M \to M_2 \) be an exact sequence in \( \text{Mod}_R \), then \( M \) is Noetherian iff \( M_1, M_2 \) are both Noetherian.

Prop. (4.1.1.40). Let \( A \) be a Noetherian ring, then quotient ring, f.g. module, f.g. algebra, localization and power series of \( A \) are Noetherian. Hence graded algebra of a Noetherian ring \( A \) by an ideal \( I \) is Noetherian. Products of Noetherian rings are Noetherian.

Proof: Only need to prove \( A[X] \) and \( A[[X]] \), localization and others are quotients of these. For an ascending chain of ideal \( I_j \) of \( A[X] \), we consider the coefficients ideal \( I_{i,j} \) of \( X^i \) of \( I_j \), then there are only f.m. different \( I_{i,j} \), so we have \( I_j \) stabilize as well.

Similarly for \( A[[X]] \), we prove any ideal \( I \) is f.g. Consider the lowest terms coefficient ideal at degree \( i \), then it is ascending and stabilize, then a set of generators as a whole generate \( I \). □

Remark (4.1.1.41). The subring of a Noetherian ring is NOT necessarily Noetherian, by the example of \( k[X_1, \ldots, X_n, \ldots] \subset k(X_1, \ldots, X_n, \ldots) \).

Prop. (4.1.1.42). When \( A \) is Noetherian and is quipped with \( I \)-adic topology, then \( I \) is f.g., and there is a surjective ring map \( A[[X]] \to A^\wedge \), mapping to the generators of \( I \), hence the completion is Noetherian. (It is surjective can be seen by the Cauchy sequence construction of completion).

Prop. (4.1.1.43). If \( R \to R' \) is ring map of f.t., then if \( S \in \mathcal{C} \text{Ring} / R \) and \( S \) is Noetherian, then \( S \otimes_R R' \) is Noetherian, because \( S \times_R R' \) is of f.t. over \( S \), and use (4.1.1.40).

Cor. (4.1.1.44). For \( k \in \text{Field}, S \in \mathcal{C} \text{Ring} / k \), then for any f.g. field extension \( K/k \), \( S \otimes_k K \) is Noetherian. (Because there is a f.g. algebra \( B \) over \( k \) that \( K \) is the localization of \( B \), and use (4.1.1.40)).

Prop. (4.1.1.45). If \( R \) is Noetherian and \( M \) is a f.g. \( R \)-module, then there is a filtration \( \{M_i\} \) of \( M \) that the quotients are all isomorphic to \( R/p_i \) where \( p_i \) are primes.

Proof: \( M \) is generated by \( x_i \), so \( (x_i) \cong R/I_i \), and so we modulo \( x_i \), then the result follows by induction. So we may assume \( M = R/I \). We use Noetherian condition to choose a maximal element \( J \) that is a counterexample, then \( J \) is not a prime, so there are \( a, b \notin J \) that \( ab \in J \). Then we have a filtration \( 0 \subset aR/(J \cap aR) \subset R/J \). Notice \( R/(J + bR) \to aR/(J \cap aR) \to 0 \), and the second quotient is \( R/(J + aR) \), so they all can be factorized. □
**Prop.(4.1.1.46).** A Noetherian ring has only f.m. minimal prime ideals.

*Proof:* This is a consequence of (5.4.1.20)(5.4.1.21) and (3.8.3.4). □

**Prop.(4.1.1.47)[Cohen].** If $R \in \mathbb{CRing}$ and every prime ideal is f.g., then $R$ is Noetherian.

*Proof:* Suppose $P$ is not Noetherian. Firstly the set of non-finitely generated ideals has the chain property: if $I_i$ is a chain of non-f.g. ideals of $R$, then $I = \cup_{i \in \Phi} I_i$ is non-f.g., otherwise there are $(f_i) = I$, but $\{f_i\} \in I_h$ for some $h$, thus $I_h$ is f.g.. Then we use the Zorn’s lemma to find a maximal non-f.g. ideal $I$. We show that $I$ is a prime ideal:

$I \neq R$ because $R = (1)$. So if $a, b \in R \setminus I$ that $ab \in I$, then $I + (a)$ and $I + (b)$ is f.g. by $p_i + r_i a$, by maximality, and let $K = (P : a)$, then $I \subset I + (b) \subset K$, thus $K$ is f.g., so does $aK$.

Now I claim $I = (p_1) + \ldots + (p_n) + aK$: one direction is clear, and if $r \in I \subset I + (a)$, then $r = \sum c_i(p_i + r_i a)$, thus $(\sum c_i r_i)a = r - \sum c_i p_i \in I$, thus $\sum c_i r_i \in K$, thus $r = \sum c_i p_i + (\sum c_i r_i)a \in (p_1) + \ldots + (p_n) + aK$.

So now $I$ is f.g., contradiction, which shows $I$ is a prime, but this contradicts the hypothesis. □

**Prop.(4.1.1.48)[Modules over Noetherian Ring are Noetherian].** Let $R$ be a Noetherian ring, then any submodule of a finite module $M$ over $R$ is finite. Thus any module over $R$ is a Noetherian module (4.1.1.38). In particular, any module over $R$ is of f.p.

*Proof:* it suffices to prove the first assertion: we use induction on the minimal number of generators of $M$: if it is generated by 1 element, then $M \cong R/I$ for some ideal $I$, thus $N \subset M$ is isomorphic to some $J/I$, so it is finite because $J$ is finite. If the minimal number of generators of $M$ is greater than 1, then there exists an exact sequence

$$0 \to M' \to M \to M'' \to 0$$

where $M', M''$ has fewer number of generators. Now there is also an exact sequence

$$0 \to N \cap M' \to N \to N' \to 0,$$

and the minimal number of generators of $N$ is smaller than the sum of that of $M'$ and $M''$, thus it is also finite. □

**Prop.(4.1.1.49)[Artin-Tate].** Let $R$ be a Noetherian ring and $S$ a f.g. $R$-algebra. If $T \subset S$ is an $R$-subalgebra that $S$ is a finite module over $T$, then $T$ is f.g. over $R$.

*Proof:* Cf.[Sta]00IS. □

**Prop.(4.1.1.50)[Krull-Akizuki].** If $R$ is a Noetherian domain of dimension 1 with fraction field $K$, $L/K$ a finite extension of fields, then for any ring $A$ s.t. $R \subset A \subset L$, $A$ is Noetherian.

*Proof:* Cf.[Sta]00PG. □

### 2 Lengths

**Def.(4.1.2.1) [Lengths].** The *length* of a $R$-module $M$ is the supremum of lengths of chains of submodules of $M$, denoted by $\text{length}_R(M)$.

**Prop.(4.1.2.2).** Length is an additive function on $\text{Mod}_R$. □
Prop. (4.1.2.3). If $\text{length}_R(M) < \infty$, then any maximal chain of submodules has the same length.

Proof: Let $l(M)$ be the minimal length of a maximal chain, then if $M \subseteq N$, then firstly $l(M) < l(N)$, because a maximal chain of $M$ restricts to a maximal chain of $N$, and if the length is the same, then each term is in $M$, so $N \subset N$, contradiction. Now any chain has length $l(M)$, because if there is a chain $M_i$, then $l(M_0) < l(M_1) < \ldots < l(M)$.

Prop. (4.1.2.4). Let $R \in \mathcal{C}$Ring and $S$ a multiplicative set of $R$, then $\text{length}_R(M) \geq \text{length}_{S^{-1}R}(S^{-1}M)$.

Proof: This is because any $S^{-1}R$-submodule of $S^{-1}M$ is of the form $S^{-1}N$ where $N$ is a $R$-submodule of $M$.

Prop. (4.1.2.5). If $R$ is a ring with a maximal ideal $\mathfrak{m}$, $M$ is an $R$-module that $\mathfrak{m}M = 0$, then $\text{length}_R(M) = \dim_{k(\mathfrak{m})}(M)$.

Prop. (4.1.2.6)[Length over a Local Ring]. Let $(R, \mathfrak{m})$ be a local ring, and $M \in \text{Mod}_R$ is of finite length, then $\mathfrak{m}^nM = 0$ for some $n \in \mathbb{N}$.

Conversely, if $\mathfrak{m}$ is f.g. and $M$ is a finite $R$-module, and $\mathfrak{m}^nM = 0$ for some $n \in \mathbb{N}$, then $\text{length}_R(M) < \infty$.

Proof: $M$ is clearly a finite module over $R$. Take $n = \text{length}_R(M)$. If $f_1, \ldots, f_n \in \mathfrak{m}$ and $x \in M$ s.t. $f_1 \ldots f_n x \neq 0$, then by Nakayama the submodules

$$0 \subset (f_1 \ldots f_n)x \subset (f_2 \ldots f_n)x \subset (f_n)x \subset M$$

are all different, so $\text{length}_R(M) \geq n$, contradiction.

For the converse, use additivity on the filtration $0 = \mathfrak{m}^nM \subset \mathfrak{m}^{n-1}M \subset \ldots \subset M$, where each quotient is finite over $R$ and annihilated by $\mathfrak{m}$, so we conclude by (4.1.2.5).

Prop. (4.1.2.7). If $(A, \mathfrak{m})$ is a local ring and $B$ is a ring over $A$ with f.m. maximal ideals $\mathfrak{m}_i$ s.t. each $\mathfrak{m}_i$ is over $\mathfrak{m}$ and $k(\mathfrak{m}_i)/k(\mathfrak{m})$ is finite, then there for any $M \in \text{Mod}_B$ with $\text{length}_B M < \infty$,

$$\text{length}_A M = \sum_i [k(\mathfrak{m}_i) : k(\mathfrak{m})] \text{length}_{B \mathfrak{m}_i} M_{\mathfrak{m}_i}.$$  

Prop. (4.1.2.8). Let $A \to B$ be a flat local maps of local rings, then for any $M \in \text{Mod}_A$,

$$\text{length}_A(M) \text{length}_B(B/\mathfrak{m}_A B) = \text{length}_B(M \otimes_A B).$$

Proof: Cf.[Sta]02M1.

Cor. (4.1.2.9). Let $A \to B \to C$ be local maps of local rings, $C/B$ is flat, and $\mathfrak{m}_A$ the maximal ring of $A$, then

$$\text{length}_B(B/\mathfrak{m}_A B) \text{length}_C(C/\mathfrak{m}_B C) = \text{length}_C(C/\mathfrak{m}_B C).$$

Prop. (4.1.2.10)[Order of Vanishing]. If $R$ is a semi-local Noetherian domain of dimension 1 and $a, b$ are not zero-divisors, then $f(a) = \text{length}(R/(a))$ satisfies $f(a) + f(b) = f(ab) < \infty$.

So this $R \subset K$ and has fraction field $K$, then $f$ extends to an additive function on $K^*$, denoted by $\text{ord}_R(f)$.

Proof: It is finite by [Sta]00PF. It is additive because length is additive (4.1.2.1) and $0 \to R/(a) \to R(ab) \to R(b) \to 0$. 

□
3 Artinian Ring

Def. (4.1.3.1) [Artinian Rings]. A ring $A$ is called Artinian if any descending chain of ideals of $A$ stabilizes.

For example, a f.g. $k$-algebra that is a finite $k$-module is an Artinian ring.

Lemma (4.1.3.2). Let $A$ be an Artinian ring, then $A$ has f.m. maximal ideals.

Proof: Consider $m_1 \supset m_1 \cap m_2 \supset \ldots$, then it is a descending chain, by Chinese remainder theorem. So it has f.m. maximal ideals. \qed

Lemma (4.1.3.3). If $A$ is an Artinian ring, then the Jacobson radical is nilpotent.

Proof: Consider the Jacobson radical $I$, $I^n = I^{n+1}$ for some $n$, let $J = \text{Ann}(I^n)$, it suffices to show $J = A$. If not, choose a minimal $J'$ that contains $J$ but not $J$ (exists by Artinian property), then $J' = J + Ax$, and $IJ' \subseteq J$ by Nakayama, so $xI^{n+1} \subseteq JI^n = 0$, so $x \in J$, contradiction. \qed

Prop. (4.1.3.4) [Characterization of Artinian Rings]. The following are equivalent:

1. $A$ is Artinian.
2. $A$ is Noetherian of dimension 0.
3. $\text{length}_A A < \infty$.
4. $A$ is a finite product of local Artinian rings.
5. $A$ is Noetherian, Jacobson (4.2.6.4), and has f.m. maximal ideals.

Proof: 1 $\iff$ 3: if $\text{length}_A A < \infty$, then $A$ is clearly Artinian. Conversely, if $A$ is Artinian, then by (4.1.3.2) (4.1.3.3) (4.2.6.7) $A$ a finite product of its localization of maximal ideals, so we may assume $A$ is local with maximal ideal $m$. Then $m^n = 0$ for some $n$ by (4.1.3.3), and $m^i/m^{i+1}$ has length the same as their dimension as a $A/m$ vector space, by (4.1.2.5), which is finite because $A$ is Artinian, so $\text{length}_A A < \infty$.

1 + 3 $\rightarrow$ 5: $A$ has f.m. maximal ideals by (4.1.3.2). It is Jacobson by (4.1.3.3). $\text{length}_A A < \infty$ clearly implies $A$ is Noetherian.

5 $\rightarrow$ 2: By (4.2.6.7).

2 $\rightarrow$ 5: all prime ideals are maximal, so $\text{Spec} A$ is discrete, so $A$ has f.m. maximal ideals, and it is clearly Jacobson.

5 $\rightarrow$ 3: By (4.2.6.7), $R$ is a product of its local rings, and the local rings are all Noetherian and Jacobson (4.2.6.6), so by Nakayama, they have finite lengths. So also $R$ has finite length.

5 $\rightarrow$ 4: By lemma (4.2.6.7) below, $A$ is a product of its localization, and its localizations also satisfies 5, and by 5 $\rightarrow$ 3 $\rightarrow$ 1, they both have descending conditions.

4 $\rightarrow$ 5: An Artinian ring is Noetherian and Jacobson by 1 + 3 $\rightarrow$ 5, then so does their product. \qed

Cor. (4.1.3.5) [Reduced Artinian Ring]. A reduced local Artinian ring is a field. In particular, $A$ reduced Artinian ring is a product of fields.

Proof: An Artinian local ring $A$ is Jacobson (4.1.3.4) so the maximal ideal $m = 0$ as $A$ is reduced. \qed

Prop. (4.1.3.6). For an Artinian local ring $A$, the following are equivalent:

1. $A$ is a PID.
2. the maximal ideal \( \mathfrak{m} \) is principal.
3. \( \dim_k(\mathfrak{m}/\mathfrak{m}^2) \leq 1 \).

*Proof:* It suffices to prove \( 3 \implies 1 \): If \( \mathfrak{m} = \mathfrak{m}^2 \), then \( \mathfrak{m} = 0 \) by Nakayama, so \( A \) is a field. If \( \dim_k(\mathfrak{m}/\mathfrak{m}^2) = 1 \), then \( \mathfrak{m} \) is principle by Nakayama. And \( \mathfrak{m} \) is nilpotent by (4.1.3.4), so for any ideal \( a \) there is a minimal \( n \) that \( a \subset \mathfrak{m}^n \). Now choose \( y \in a - \mathfrak{m}^{n+1} \), then \( y = ux^r \), and \( u \notin (x) \), so \( u \) is a unit, thus \( x^r \in a \), meaning \( a = \mathfrak{m}^n \) hence principal. \( \square \)

### 4 Local Properties

**Def.** (4.1.4.1) *Local properties.* A property \( P \) of rings or modules over a ring is called **local property** iff \( X \) has \( P \) iff \( X_f \) all has \( P \) for a covering \((f_1, \ldots, f_n) = 1\).

A property of morphisms of rings is called **local on the target** iff \( R \to S \) has \( P \) iff \( R_{f_i} \to S_{f_i} \) has \( P \) for a covering \((f_1, \ldots, f_n) = 1 \) in \( R \).

**Prop.** (4.1.4.2) *Stalkwise Properties.* For a commutative ring \( R \), a property \( P \) is called stalkwise if \( A \) satisfies \( P \) iff all \( A_{\mathfrak{m}} \) satisfies \( P \) where \( \mathfrak{m} \) are maximal ideals, and iff all \( A_{\mathfrak{p}} \) satisfies \( P \) where \( \mathfrak{p} \) are prime ideals of \( A \).

1. Trivial is stalkwise for modules over \( R \). Hence so does injectivity and surjectivity because localization is exact.
2. Torsion-free is stalkwise for modules over \( R \) if \( R \) is integral.
3. Flatness for modules over \( R \).
4. Flatness for rings over \( R \) on the source.
5. Formal unramifiedness for rings over \( R \), both on the target and source.
6. (universally)catenary is stalkwise.
7. reducedness is stalkwise.
8. Integral+integrally closed is stalkwise.
9. normal is stalkwise.
10. regular is stalkwise.

*Proof:*

1. It suffice to prove an element is trivial on every localization then it is 0. For this, consider the annihilator \( \text{Ann}(x) \), it is not contained in any maximal ideal so it contains 1.
2. if \( xf = 0 \) but \( f \neq 0 \), then \( x \in \text{Ann}(f) \neq (1) \), so \( \text{Ann}(f) \subset \mathfrak{m} \) maximal, so \( f \) is torsion in \( M_{\mathfrak{m}} \) over \( R_{\mathfrak{m}} \). Conversely, if \( f \) is torsion in \( R_{\mathfrak{m}} \), then it is clearly torsion over \( R \).
3. We use the definition (4.4.1.2). Notice \( (IM)_{\mathfrak{p}} = I_{\mathfrak{p}} M_{\mathfrak{q}} \) and every ideal of \( R_{\mathfrak{p}} \) is of the form \( I_{\mathfrak{p}} \). Then use the fact injective is stalkwise (4.1.4.2).
4. We use the definition (4.4.1.2). Notice \( (I \otimes_R S)_{\mathfrak{q}} = I_{\mathfrak{p}} \otimes_{R_{\mathfrak{p}}} S_{\mathfrak{q}} \) for all primes \( \mathfrak{q} \) of \( S \) and \( \mathfrak{p} = \mathfrak{q} \cap R \). And every ideal of \( R_{\mathfrak{p}} \) is of the form \( I_{\mathfrak{p}} \). Then use the fact injective is stalkwise (4.1.4.2).
5. Because formally unramified is equivalent to \( \Omega_{R/S} = 0 \) (4.4.6.1), so we get the result by functorial properties of \( \Omega_{S/R} \) (4.4.3.6) and triviality is stalkwise (4.1.4.2).
6. For any two prime ideals \( \mathfrak{p} \subset \mathfrak{q} \), we can choose a maximal ideal containing them.
7. use (4.1.1.33).

8. If $A$ is integrally closed, then clearly any localization of $A$ is integrally closed. Conversely, if $r \in K(A)$ is integral over $A$ but $r \notin A$, let $I = \{ s \in A \mid rs \in A \}$, then $I \neq A$, so $I \subset \mathfrak{m}$ for some maximal ideal $\mathfrak{m}$, then $r \notin A_{\mathfrak{m}}$, so $A_{\mathfrak{m}}$ is not integrally closed, contradiction.

9. By definition.

10. By definition.

Remark (4.1.4.3). Our main technique of proving local properties are using affine communication theorem (5.4.1.2).

Prop. (4.1.4.4) [Local Properties]. For a fixed ring $R$,

1. Every property that is stalkwise is a local property. (4.1.4.2) The properties listed below should be not stalkwise.

2. Every property that satisfies faithfully flat descent is a local property. The properties listed below should not satisfy faithfully flat descent.

3. Noetherian.

4. F.t. ring maps on the source.

5. F.p. ring maps on the source.


7. Nagata for rings.

Proof:

1.

2.

3. If $A$ is Noetherian, then $A_{f_i}$ are Noetherian by (4.1.1.40). Conversely, if $A_{f_i}$ are all Noetherian and $I_1 \subset I_2 \subset \ldots$ is an ascending chain of ideals of $A$, consider $A \to \prod A_{f_i}$ faithfully flat, thus $I_1 \otimes_A (\prod A_{f_i}) \subset I_2 \otimes_A (\prod A_{f_i}) \subset \ldots$ is an ascending chain of $\prod A_{f_i}$. Now $\prod A_{f_i}$ are Noetherian by (4.1.1.40), so this chain stabilizes. But this ring map is faithfully flat, so the original chain must also stabilizes.

4. Let $(g_1, \ldots, g_n) = 1$, choose $\sum h_i g_i = 1$, and let $x_{ij} = y_{ij}/g_i^{n_{ij}}$ generates $S_{g_i}$. Now let $S'$ be the sub-$R$-algebra of $S$ generated by $y_{ij}, g_i, h_i$. Then $(S')_{f_i} \to S_{f_i}$ is surjective for any $i$, so $S' \to S$ is also surjective, by (4.1.4.2). Then $S' = S$, and $S$ is f.g. over $R$.

5. Cf. [Sta]00EP.

6. If $A$ is N-1, then $A_{f_i}$ are N-1 because taking integral closure commutes with localization. The same for N-2. Conversely, if all $A_{f_i}$ are N-1 or N-2, so is $A$ because finiteness is local (4.1.4.4). The universal Japanese case follows from the N-2 case.

7. This follows from the localness of Noetherian and N-2 (4.1.4.4).
5 Miscellaneous

Fitting Ideals

Def. (4.1.5.1) [Fitting Ideals]. Let \( R \in \mathfrak{C} \mathfrak{R} \)ing and \( M \) be a finite \( R \)-module, then for any presentation
\[
\oplus_{j \in J} R \rightarrow R^{\oplus n} \rightarrow M \rightarrow 0
\]
given by a \( n \times J \) matrix \( A \), the ideal generated by the \( (n-k) \times (n-k) \) matrices of \( A \) is independent of the presentation chosen, called the \( k \)-th Fitting ideal of \( A \), denoted by \( \text{Fit}_k(M) \).

6 Rings and Categories

Quotient by Equivalence Relations

Prop. (4.1.6.1) [Quotients by Equivalence Relations]. Let \( u_0, u_1 : A_0 \rightarrow A_1 \) be an equivalence in the dual category of \( \mathfrak{C} \mathfrak{R} \)ing\(_R_{\mathfrak{R}0}(3.1.1.24)\). If \( u_0 \) is locally free of constant rank \( r \), then a quotient \( u : A \rightarrow A_0 \) exists, and \( u \) is locally free of constant rank \( r \).

Proof: Cf. [Mil17b]P592. \( \square \)

Morita Equivalence

Basic References are [Morita Equivalence] and [Fuller Rings and Categories of Modules].

Def. (4.1.6.2). Two ring \( R, S \) are called Morita equivalent if the category of mod-\( R \) is equivalent to the category of mod-\( S \).

Prop. (4.1.6.3). For an Abelian category \( \mathcal{A} \) satisfying AB3 (i.e. arbitrary sum exists), An object \( P \) of \( \mathcal{A} \) is a progenerator if the functor \( h' : X \mapsto \text{Hom}_\mathcal{A}(P, X) \) is exact and and strict: \( h'(X) = 0 \) implies \( X = 0 \). Then \( h' \) determines an equivalence from \( \mathcal{A} \) to mod-\( R \), where \( R = \text{Hom}_\mathcal{A}(P, P) \).

Similarly, if \( \mathcal{A} \) is an Abelian Noetherian category and \( P \) is a progenerator, then \( R \) is Noetherian and \( \mathcal{A} \) is equivalent to the category of finitely generated \( R \)-categories.

Proof: Essentially surjective: construct using direct limit and cokernel.

Notice that \( h'(X) \cong h'(X') \rightarrow X \cong X' \) by strictness and A4 axiom. So let \( X = \text{Coker}(P^{\oplus I}, P^{\oplus J}) \),
\[
\text{Hom}(h'(X), h'(Y)) = \text{Hom}(\text{Coker}(h'(P^{\oplus I}), h'(P^{\oplus I})), h'(Y)) = \ker(\text{Hom}(h'(P^{\oplus I}), h'(Y)) \rightarrow \text{Hom}(h'(P^{\oplus I}), h'(Y)))) = \ker(h'(Y^{\Pi}) \rightarrow h'(Y^{\Pi})) = \text{Hom}(X, Y)
\]
\( \square \)

Prop. (4.1.6.4). In the case when \( \mathcal{A} \) is the category mod-\( R \), \( P \) is a generator \( \iff \ h' : X \mapsto \text{Hom}_R(P, X) \) is faithful \( \iff \) every \( M \) is a quotient of direct sums of \( P \). And a progenerator is a f.g. projective generator.
Prop. (4.1.6.5). Let $P$ be a $(A,B)$-bimodule, iff $P$ is a progenerator as a right $B$ module, then it is a progenerator as a left $A$ module.

Prop. (4.1.6.6). Let $P$ be a progenerator as a

Prop. (4.1.6.7) [Morita]. The following are equivalent:
- categories $A$-mod and $B$-mod are equivalent.
- categories mod-$A$ and mod-$B$ are equivalent.
- There exist a finitely generated progenerator $P$ of mod-$A$ that $B \cong \text{End}_A P$.

Proof: $2 \rightarrow 3$: $A$ is a progenerator in mod-$A$, thus when $A \sim B$, $F : \text{mod-}A \rightarrow \text{mod-}B$, $A \cong \text{End}_A A = \text{End}_B F(A)$, and $F(A)$ is a left $A$ module as well as a progenerator of $B$. Thus there is a $(A,B)$-bimodule $P$ that $A \cong \text{End}_B P$, and a $(B,A)$-bimodule $Q$ that $B \cong \text{End}_A Q$. \hfill $\square$

Prop. (4.1.6.8). There can be defined another Morita invariance that $R \sim S$ iff there are $(R,S)$-bimodule $P$ and $(S,R)$-bimodule $Q$ that $P \otimes_S Q \cong R$ as a $(R,R)$-bimodule and $Q \otimes_R P \cong S$ as a $(S,S)$-bimodule. This will immediately generate equivalence between $R$-mod and $S$-mod as well as equivalence between mod-$R$ and mod-$S$ by tensoring. And $P$ and $Q$ are projective modules respectively, because equivalence is a kind of adjoint.

Prop. (4.1.6.9). Let $D$ be a division ring over $k$ of finite degree and $A = M_n(D)$. Let $S = D^r$ with $A$ acting by left multiplication and $D$ acting by right multiplication, then there $S$ is a simple $A$-module, and every $A$-module is a direct sum of copies of $S$. This means that $S \otimes_D -$ induces an equivalence from $\text{Mod}_D$ to $\text{Mod}_A$.

Prop. (4.1.6.10) [Properties Preserved under Morita Invariance]. Cf. [Rings and Categories of Modules P54].

7 Spectra

Lemma (4.1.7.1). In Spec $A$, a subset $U$ is retrocompact iff it is quasi-compact iff it is a finite union of standard opens $D(f_i)$. In particular, any constructible subset of Spec $A$ is a finite union of morphisms of the form $D(f_i) \cap V(g_1, \ldots, g_m)$.

Proof: Retrocompact is quasi-compact because Spec $A$ is quasi-compact. A quasi-compact subset is equivalent to a finite union of $D(f_i)$. Now for any quasi-compact subset $V = \bigcup_i D(g_j)$, $U \cap V = \bigcup_{ij} D(f_ig_j)$ is also quasi-compact, so $\bigcup D(f_i)$ is retrocompact. \hfill $\square$

Lemma (4.1.7.2). Let $R$ be a ring, then
- the image of any standard open subsets of Spec $R[X]$ is qc open in Spec $R$.
- for $g, f \in R[X]$ with $g$ monic, the image of $D(f) \cap V(g)$ is qc open in Spec $R$.

Proof: 1: For any prime $\mathfrak{p}$ of $R$, the primes mapping to $\mathfrak{p}$ has a minimal one, $\mathfrak{p}[X]$, so $\mathfrak{p}$ is in the image of Spec $R[X] \rightarrow$ Spec $R$ iff $f \in \mathfrak{p}[X]$, which means the image is $D(a_0,a_1,\ldots,a_n)$, where $f = a_0 + a_1X + \ldots + a_nX^n$.

2: $R[X]/g$ is finite free over $R$, let $P(T) = T^d + r_{d-1}T^{d-1} + \ldots + r_0$ be the characteristic polynomial of $f$ acting on $R[X]/g$ by left multiplication, then $\mathfrak{p} \in V(r_0,\ldots,r_{d-1})$ iff $f$ acts nilpotently on $R[X]/g \otimes_R k(\mathfrak{p})$, which is equivalent to $\mathfrak{p}$ being in the image of $D(f) \cap V(g)$ (by base change to $k(\mathfrak{p})$ argument). \hfill $\square$
Lemma (4.1.7.3) [Affine Chevalley]. The Spec map of a f.p. ring map maps constructible sets to constructible sets.

Proof: Suppose \( S = R[X_1, \ldots, X_n](f_1, \ldots, f_m) \), then it suffices to show for the case \( S = R/(f_1, \ldots, f_m) \) and \( S = R[X] \).

If \( S = R/(f_1, \ldots, f_m) = R/I \), it suffices to show the image of \( D(\overline{g}) \cap V(\overline{h_1}, \ldots, \overline{h_m}) \) is retrocompact in \( \text{Spec } R \); in fact its image is just \( D(g) \cap V(h_1, \ldots, h_m) \cap V(I) \), where \( g, h_i \) are any inverse images in \( R \).

For the second case, we first prove some localizing result: If \( S = R_f \), then the compact open subsets of \( \text{Spec } S \) are compact open subsets of \( \text{Spec } R \), so \( \text{Spec } S \to \text{Spec } R \) maps constructible sets to constructible sets. Now for any \( c \in R \), \( \text{Spec } R = \text{Spec } R/c \coprod \text{Spec } R_c \), so to prove the proposition for \( R \), it suffices to prove for \( R_c \) and \( R/c \).

Let \( D(f) \cap V(g_1, \ldots, g_n) \subset \text{Spec } R[X] \), where \( f, g_i \) are polynomials. We can use induction on the degree series \( \deg(g_1) \leq \deg(g_2) \leq \cdots \leq \deg(g_n) \). If the leading coefficient of \( g_1 \) is invertible, then we can use reduction to \( R/c \) and \( R_c \) to either reduces the degree of \( g_1 \) or reduce to the case it is invertible. If it is invertible, then we can use Euclidean division. Eventually, it can be reduced to the case \( D(f) \cap V(g) \) where \( g \) is monic, or \( D(f) \). This is proved in the above lemma (4.1.7.2). □

Lemma (4.1.7.4). For a Noetherian local ring \((A, m)\), \( \text{Spec } A - m \) is affine iff \( \dim A \leq 1 \).

Proof: If \( \dim A = 0 \), this is true, if \( \dim A = 1 \), let \( f \in m \) not in any other minimal primes of \( A \), then \( \text{Spec } A - m = \text{Spec } A_f \).

Conversely, Cf. [[Sta]0BCR]. □

Idempotents

Prop. (4.1.7.5) [Clopen Subsets]. The clopen subsets of \( \text{Spec } A \) corresponds to idempotents in \( A \).

Proof: This is all equivalent to the fact that there exists \( e + f = 1, ef = 0 \):

If \( A = U \coprod V \), then both \( U, V \) are closed hence qc, so \( \text{Spec } A = U \cup V(\overline{f}_i) \coprod U \cup V(\overline{g}_j) \), then \( f_i g_j \) is nilpotent by (4.2.6.2). Denote \( I = (\overline{f}_i), J = (\overline{g}_j) \), then \( (IJ)^N = 0 \) and \( I + J = A \), there are \( 1 = x + y, x \in I^N, y \in J^N \).

For uniqueness, if \( e_1 \neq e_2 \), then \( 0 \neq e_1 - e_2 = e_1(e_2 + f_2) - e_2(e_1 + f_1) = e_1 f_2 - e_2 f_1 \), so may assume \( e_1 f_2 \neq 0 \), and it is not nilpotent, so there is a \( e_1 f_2 \subset p \), which is a contradiction. □

Cor. (4.1.7.6). A local ring has no non-trivial idempotents, and then an idempotent is defined by the maximal ideals that it vanishes.

Cor. (4.1.7.7). If \( I \) is an ideal of \( R \) that \( I = I^2 \), and \( I \) is f.g., then \( V(I) \) is open and closed in \( \text{Spec } R \), and \( V(I) = R_e \) for some idempotent \( e \).

Proof: By Nakayama, there is a \( a \) \( f = 1 - e \) with \( e \in I \) that \( f I = 0 \). So \( e - e^2 = 0 \) and \( f^2 = f \).

\( V(I) = D(f) = D(e) \). □

Lemma (4.1.7.8). If \( I \) is a locally nilpotent ideal, then \( R \to R/I \) induces a bijection on idempotents.

Proof: Because \( R \to R/I \) induces a homeomorphism on the spectra, and clopen subsets of the spectrum corresponds to the idempotents (4.1.7.5). □

Lemma (4.1.7.9). Let \( R \) be a ring and \( T \subset \text{Spec } R \) is a set. Then the following are equivalent:
\begin{itemize}
\item $T$ is closed and is a union of connected components of $\text{Spec } R$.
\item $T$ is an intersection of clopen subsets.
\item $T = V(I)$ where $I$ is generated by idempotents.
\end{itemize}

**Proof:** 1 and 2 are equivalent by (3.8.4.3), and $2 \rightarrow 3 \rightarrow 1$ are easy.

**Prop. (4.1.7.10).** Let $R$ be a ring, then any connected component of $\text{Spec } R$ is of the form $V(I)$, where $I$ is an ideal generated by idempotents that any idempotent of $R$ maps to either $0$ or $1$ in $R/I$.

**Proof:** By (3.8.4.2) and (3.8.4.13), a connected component of $\text{Spec } R$ is an intersection of clopen subsets, so it is of the form $V(I)$ where $I$ is generated by idempotents. The last assertion is equivalent to $V(I)$ being connected.

**Going-up and down**

**Def. (4.1.7.11) [Going-up and Going Down].** Going-up and down for topological spaces is defined in (3.8.3.7). A ring map $R \to S$ is said to satisfy the going-up property iff its $\text{Spec}$ map does, equivalently, for any prime ideal $q \subsetneq S$ and prime ideal $p \subsetneq q \cap R$, there exists a prime ideal $q' \subset neq q$ that $q' \cap R = p$.

It is said to satisfy the going-down property iff its $\text{Spec}$ map does, equivalently, for any prime ideal $q \subsetneq S$ and prime ideal $q \cap R \subsetneq p$, there exists a prime ideal $q' \subsetneq q$ that $q' \cap R = p$.

**Prop. (4.1.7.12).** Going-up and Going-down are stable under composition, trivially.

**Prop. (4.1.7.13) [Integral Map satisfies Going-Up].** Integral ring map satisfies going-up (4.2.1.5).

Flat ring map satisfies going-down (4.4.1.19).

**Lemma (4.1.7.14).** If the image of the $\text{Spec}$ map of a ring map is closed under specialization, then this image is closed.

**Proof:** Let it be $R \to S$, let $I$ be the kernel, then the image is contained in $V(I)$, so we may replace $R$ be $R/I$, then $R \subsetneq S$. Now we show the image contains all the minimal primes of $R$: for a minimal prime $p$, $A_p \subsetneq B_p$, thus $B_p$ is not-empty, and thus has a maximal ideal, whose intersection with $A_p$ can only be $p$ by hypothesis, thus $p$ is in the image of Spec. Then the image is all of Spec $R$ by hypothesis, thus closed.

**Cor. (4.1.7.15) [Going-up and Spec Closed].** Going-up is equivalent to Spec map closed.

**Proof:** If going-up holds, then Spec map is closed by (4.1.7.14). Conversely, a closed map satisfies going-up, by (3.8.3.8).

**Prop. (4.1.7.16).** If $R \to S$ is a ring map that satisfies going-up, and $P \subset S$ is a maximal ideal, then $P \cap R$ is also a maximal ideal.

**Prop. (4.1.7.17) [Krull].** If $A \subset B$ is an integral extension of integral domains, and $A$ is normal, then going-down holds.
Prop. (4.1.7.22) [Zerodivisors in a Reduced Ring]. Let \( R \) be a reduced ring, then 
\[
\mathfrak{p} = \mathfrak{p}^2 \quad \text{implies} \quad \mathfrak{p} = 0.
\]

Proof: For \( \mathfrak{p} \) is minimal, \( \mathfrak{p}^2 = 0 \Rightarrow \mathfrak{p} = 0 \).

Prop. (4.1.7.23) [Irreducible Components of Spectrum]. Let \( R \) be a ring, then 
\[
\text{Spec}(R) = \bigcup_{\mathfrak{p} \in \text{Min}(R)} \{ \mathfrak{p} \}.
\]

Proof: By (4.2.6.1), \( \mathfrak{p} \subseteq \mathfrak{p}^2 \Rightarrow \mathfrak{p} = 0 \).

Lemma (4.1.7.20). If \( \mathfrak{p} \) is a minimal prime of \( R \), then \( \mathfrak{p} \mathfrak{R}_\mathfrak{p} \) is locally nilpotent by (4.2.6.1). In particular, if \( R \) is reduced, then \( \mathfrak{R}_\mathfrak{p} \) is a field.

Prop. (4.1.7.21) [Zerodivisors in a Reduced Ring]. Let \( R \) be a reduced ring, then

- \( R \to \prod_{\mathfrak{p}} \mathfrak{R}_\mathfrak{p} \) is an embedding into a product of fields.
- \( \bigcup_{\mathfrak{p}} \mathfrak{R}_\mathfrak{p} \) is the set of zerodivisors of \( R \).

Proof: 1. By (4.1.7.20), \( \mathfrak{R}_\mathfrak{p} \) are fields. In particular, the kernel of \( R \to \mathfrak{R}_\mathfrak{p} \) is \( \mathfrak{p} \). Then the kernel of the map \( R \to \prod_{\mathfrak{p}} \mathfrak{R}_\mathfrak{p} \) is \( \bigcap_{\mathfrak{p}} \mathfrak{R}_\mathfrak{p} = 0 \) by (4.2.6.1).

2. If \( xy = 0 \) and \( x \neq 0 \), then \( x \notin \mathfrak{p} \) for some minimal prime \( \mathfrak{p} \) by (4.2.6.1), thus \( y \in \mathfrak{p} \). Conversely, if \( y \in \mathfrak{p} \) for some minimal prime \( \mathfrak{p} \), then \( y \) is mapped to \( 0 \in \mathfrak{R}_\mathfrak{p} \), which means there are some \( x \notin \mathfrak{p} \) that \( xy = 0 \).

Prop. (4.1.7.22). If \( R \) is a ring with f.m. minimal primes \( \mathfrak{q}_i \) and \( \bigcup_i \mathfrak{q}_i \) is the set of zerodivisors of \( R \), then the ring of fractions of \( R \) is equal to \( \prod_i \mathfrak{R}_{\mathfrak{q}_i} \).

Proof: Cf. [Sta] 02LX.

Prop. (4.1.7.23) [Irreducible Components of Spectrum]. The irreducible closed subsets of \( \text{Spec}(R) \) are exactly the sets of the form \( V(\mathfrak{p}) \) for some prime \( \mathfrak{p} \subseteq R \). The irreducible components of \( \text{Spec}(R) \) are exactly the sets of the form \( V(\mathfrak{p}_i) \) for some minimal prime \( \mathfrak{p}_i \).

Prop. (4.1.7.24) If \( R \) is a ring and \( \mathfrak{p} \) a minimal prime of \( R \). If \( W \subseteq \text{Spec}(R) \) is a quasi-compact open subset of \( \text{Spec}(R) \) not containing \( \mathfrak{p} \), then there exists some \( f \in R \) that \( \mathfrak{p} \subseteq D(f) \) and \( D(f) \cap W = \emptyset \).

Proof: 
\[
W = \bigcup_{i=1}^n D(f_i) \quad \text{and} \quad f_1 \notin D(f_i), f_i \in \mathfrak{p} \quad \text{for each} \quad i.
\]

Then (4.1.7.20) says \( f_i \) are nilpotent in \( \mathfrak{R}_\mathfrak{p} \), so there is some \( g \in R \) that \( gf_i \) are nilpotent in \( R \) for any \( i \), which means \( g \) satisfies the requirement.

Prop. (4.1.7.25). For \( R \subseteq S \), all the minimal primes of \( R \) are in the image of the Spec map of a minimal prime of \( S \).

Proof: 
Localize w.r.t. to the minimal prime \( \mathfrak{p} \), then it is a local ring with only one prime. And \( S_\mathfrak{p} \) is nonzero because localization is exact, so it has a maximal ideal \( \mathfrak{q} \). Now we choose a minimal prime of \( S \) contained in \( \mathfrak{q} \), then it is also mapped to \( \mathfrak{p} \).
Universal Homeomorphism

Cf. [Sta]10.45 and [Sta]28.44.

Prop. (4.1.7.26). If \( \varphi : R \to S \) is a ring map and \( p \) is a prime number that satisfies:
- \( S \) is generated over \( R \) by elements \( x \) that there is \( n \) that \( x^{p^n} \in \varphi(R) \) and \( p^n x \in \varphi(x) \).
- \( \ker(\varphi) \) is locally nilpotent.

then \( \text{Spec} \, S \to \text{Spec} \, R \) is a homeomorphism, and any base change of \( \varphi \) satisfies the above conditions, so it is a universal homeomorphism.

In particular, this applies to any base change of a field extension \( k'/k \) that is purely inseparable, because it is f.f. hence injective.

Proof: Cf. [Sta]0BRA. \( \square \)
4.2 Commutative Algebra II

Main references are [Sta].

1 Integral Extensions

Def. (4.2.1.1) [Totally Integrally Closed]. For two rings \( A \to B \), \( f \in B \) is called **almost integral** (or totally integral when almost mathematics is performed:) over \( A \) if \( f^n \) lies in a f.g. \( A \)-module of \( B \). It is clear that the elements of totally integral elements of \( B \) is a subring. And \( A \) is called **totally integrally closed** in \( B \) iff any \( f \in B \) totally integral over \( A \) is in \( A \).

Prop. (4.2.1.2). For a ring map \( \varphi : A \to B \), an element \( x \) is integral over \( A \) iff \( x \) is contained in a finite \( A \)-module in \( B \). In particular, the elements of \( B \) that are integral over \( A \) is a ring containing \( \varphi(A) \).

Proof: If \( x \) is integral, then \( \varphi(A)[x] \) is finite. If \( \varphi(A)[x] \) is finite, then there is a set of generators of polynomials in \( x \). Then for \( m \) large, \( x^m = \sum a_i f_i(x) \), so \( x \) is integral over \( A \).

Prop. (4.2.1.3) [Integral Extension of Field]. For \( A \subseteq B \), if \( B \) is integral over \( A \), then \( A \) is a field iff \( B \) is a field.

Proof: If \( A \) is a field, \( y^{-1} = -a_n^{-1}(y^{n-1} + \ldots + a_{n-1}) \in B \). If \( B \) is a field, \( x^{-1} = -(b_1 + b_2 x + \ldots + b_m x^{m-1}) \in A \).

Cor. (4.2.1.4). If \( B \) is integral over \( A \), then a prime \( p \subset B \) is maximal iff \( p \cap A \) is maximal.

Proof: Look at the integral extension \( A/(p \cap A) \to B/p \).

Prop. (4.2.1.5) [Going-Up]. Let \( A \to B \) integral. Then:

1. There is no inclusion relation between prime ideals of \( B \) lying over a fixed prime ideal of \( A \).
2. if \( A \subseteq B \), then the Spec map is surjective. In particular, for any \( p \subseteq A \), \( pB \cap A = p \).
3. The going-up holds. In particular, the Spec map of an integral ring map is closed, by (4.1.7.15).

Proof:

1. If \( p \cap A = p' \cap A = q \), localize at \( q \), then \( p, p' \) are both maximal ideals of \( B_q \) by (4.2.1.4), they cannot contain each other.
2. For any prime \( p \) of \( A \), since \( A_p \subseteq B_p \), \( B_p \neq 0 \), so it has a maximal ideal (4.1.1.5), and use (4.2.1.4).
3. for any prime ideal \( q \) of \( B \) and \( p = q \cap A \), replace \( A \to B \) by \( A/p \subseteq B/q \), then we can use 2.

2 Graded Rings

Cf. [Matsumura Ch11].

Def. (4.2.2.1) [Graded Rings]. A **graded ring** is a ring \( A = \bigoplus A_n \) that \( A_mA_n \subseteq A_{m+n} \). A **graded module** over a graded ring \( A \) is a module \( M = \bigoplus M_n \) that \( A_mA_n \subseteq M_{m+n} \).

Notice that often we mean \( \mathbb{Z}_{\geq 0} \)-graded rings when we say graded rings. For a \( \mathbb{Z}_{\geq 0} \)-graded ring \( A \), the subset \( A_+ = \bigoplus_{n=1}^\infty A_n \) is an ideal of \( A \), called the **irrelevant ideal**.
Def. (4.2.2.2) [Twisted Modules]. Let $A$ be a graded ring and $M$ a graded $A$-module, denote $M(n)$ the graded $A$-module s.t. $M(n)_m = M_{m+n}$.

Lemma (4.2.2.3). Let $A = \bigoplus_{n=0}^{\infty} A_n$ be a graded ring, then a set of homogenous elements $f_i \in A_+$ generate $A$ as an algebra over $A_0$ if and only if they generate $A_+$ as an ideal of $A$.

Proof: If $f_i$ generate $A$ as an algebra over $A_0$, then every element of $A_+$ is a polynomial in $f_i$ with constant coefficients in $A_0$, thus $f_i$ generates $A_+$ as an ideal. Conversely, if $f_i$ generate $A_+$ as an ideal, then for any homogenous element $f$ we can use induction on the degree of $f$ to show that $f$ is a polynomial in $f_i$. □

Prop. (4.2.2.4) [Noetherian Graded Rings]. A graded ring $A = \bigoplus_{n=0}^{\infty} A_n$ is Noetherian if and only if $A_0$ is Noetherian and $A_+$ is f.g. as an ideal of $A$.

Proof: If $A$ is Noetherian, then clearly $A_+$ is f.g. and $A_0 = A/A_+$ is Noetherian. Now if $A_+$ is f.g. as an ideal of $A$, then it is generated by f.m. homogenous elements $f_i$, so we see $f_i$ generates $A$ as an algebra over $A_0$, which means $A$ is a quotient of a polynomial ring over $A_0$, thus Noetherian by (4.1.1.40). □

Def. (4.2.2.5) [Homogenous Ideals]. Let $A_\bullet$ be a graded ring, then a homogenous ideal $I_\bullet$ of $A_\bullet$ is a ring that is generated by homogenous elements.

Prop. (4.2.2.6) [Equivalent definition of Homogenous Ideals]. Let $S_\bullet$ be a graded ring, then

- an ideal $I$ of $S_\bullet$ is homogenous iff it contains the degree $n$ part of each of its element for any $n$.
- The set of homogenous ideals of $S_\bullet$ is stable under sum, product, intersection and radical.
- A non-trivial homogenous ideal $I$ of $S_\bullet$ is a prime ideal iff for any homogenous elements $a, b$, if $ab \in I$, then $a \in I$ or $b \in I$.

Proof: 1: If $I$ contains the degree $n$ part of each of its element for any $n$, then clearly it is generated by homogenous elements. Conversely, if it is generated by homogenous elements, then any element $f = \sum a_i f_i$, where $f_i$ is homogenous. Then we can see $[f]_n = \sum [a_i]_{n-\deg f_i} f_i$ is also in $I$.

2: Use 1 and the definition. For radicals, we show $\sqrt{I}$ contains all its homogenous parts: if $f \in \sqrt{I}$, then $f^n \in I$ for some $n$, then we see that the minimal degree part $[f]_m$ of $f$ also satisfies $[f]_m^n \in I$, because $I$ contains the homogenous parts of each of its elements. Then we can use induction to show that all the homogenous parts of $f$ is in $\sqrt{I}$.

3: One direction is trivial, for the other, if $a = \sum a_i, b = \sum b_i$ satisfies $ab \in I$, and $a \notin I, b \notin I$, and $a_i, b_j$ homogenous. Let $i_0, j_0$ be the minimal numbers that $a_{i_0} \notin I, b_{j_0} \notin I$, then $a_{i_0} b_{j_0}$ is not in $I$, contradicting the fact $I$ is homogenous. □

Prop. (4.2.2.7). Let $R \to S$ be a homomorphism of graded rings, then the integral closure of $R$ in $S$ is a homogenous ideal of $S$.

Proof: Consider the base change $\varphi : R \otimes_{R_0} R_0[t, t^{-1}] \to S \otimes_{S_0} S_0[t, t^{-1}]$, where $\deg(t) = 0$, and the integral closure is denoted by $A$. Then there is an automorphism of $\varphi$: $s \mapsto t^{\deg s} \cdot s$. This automorphism thus preserves the integral closure. If $s = s_n + s_{n+1} + \ldots + s_m \in S$ is integral over $R$, to show each $s_i$ are integral over $S$. We may assume $n > 0$ because $s_0$ is clearly integral over $R_0$. 


Now we use induction on $m$. If $m > n$, consider $t^n s_n + \cdots + t^m s_m$ is also in $A$, we see $(t^m - t^i)s_i \in A$ by induction hypothesis.

Notice $S \subseteq S[t, t^{-1}]/(t^m - t^i - 1) = S[t]/(t^m - t^i - 1)$ is injective, and the image of $(t^m - t^i)s_i$ is $s_i$, which is integral over $R[t]/(t^m - t^i - 1)$, and this ring is finite over $R$, so $s_i$ is also integral over $R$. \hfill $\square$

**Proposition 4.2.2.8.** Let $A$ be a graded ring that is f.g. over $A_0$ and $M$ be a f.g. graded $A$-module, then each $M_n$ is a finite $S_0$-module.

**Definition 4.2.2.9 [Reductions of Graded Rings].** Let $S$ be a graded ring and $d \geq 1$, define $S^{(d)}$ the graded ring $\oplus_{n \geq 0} S_{nd}$. And for a graded $S$-module $M$, define $M^{(d)} = \oplus_{n \in \mathbb{Z}} M_{nd}$.

**Proposition 4.2.2.10.** If $S$ is a graded ring that is f.g. over $S_0$, then for $d$ sufficiently divisible, $S^{(d)}$ is generated by the degree 1 part over $S_0$.

**Proof:** Let $S$ be generated by homogeneous elements $f_1, \ldots, f_r$. Let $M = \text{lcm}(\deg(f_1), \ldots, \deg(f_r))$, then for any $f \in S_{Nm}$ and $N \geq r$, by pigeonhole principle, there are some $i$ s.t. $f_i^{M/\deg(f_i)} | f$. Thus any monomials of degree $nrM$ is a product of polynomials of degree $rM$. So $d = rM$ satisfies the hypothesis. \hfill $\square$

**Topology Defined by Ideals**

**Definition 4.2.2.11 [Filtrations on Graded Modules].** Let $A$ be a ring, $M$ a graded $A$-module, and $a$ be an ideal of $A$, an $a$-filtration of $M$ is a descending sequence of submodules $M = M_0 \supseteq M_1 \supseteq \cdots$ that $aM_n \subseteq M_{n+1}$. It is called a stable filtration iff there is an $N$ that $aM_n = M_{n+1}$ for $n \geq N$.

For an ideal $a \subseteq A$, there can be associated a graded ring $A^* = \oplus a^n$, and an $a$-filtration $M$ can be associated a graded module over $A^* : M^* = \oplus M_n$. When $A$ is Noetherian, then so is $A^*$, because it is a quotient of a polynomial ring over $A(4.1.1.40)$.

**Lemma 4.2.2.12.** If $A$ is a Noetherian ring and $M$ is a f.g. $A$-module that has a $a$-filtration $M_n$, then $M^*$ is f.g. over $A^*$ iff $M_n$ is a stable filtration.

**Proof:** As every $M_n$ is finite over $A$, if it is stable, then $M^*$ is generated over $A^*$ by all the generator of $M_n, n \leq N$, so it is f.g.. Conversely, if it is f.g., then it is clear that $M_n$ is a stable filtration. \hfill $\square$

**Proposition 4.2.2.13 [Artin-Rees].** For $A$ Noetherian and $I$ an ideal, let $N \subseteq M$ be finite $A$-modules, then if $M_n$ is a stable filtration of $M$, then $M_n \cap N$ is a stable filtration of $N$.

In particular, let $M_0 = I^n M$, then $I^n M \cap N = I^{n-r}(I^r M \cap N)$, hence the $I$-adic topology on $M$ induce the $I$-adic topology on $N$.

**Proof:** This is immediate from the lemma above, as $N^*$ is an $A^*$-submodule of $M^*$, and $A^*$ is Noetherian(4.2.2.11). \hfill $\square$

**Corollary 4.2.2.14 [Krull’s Intersection Theorem].** Notation as in(4.2.2.13), let $N = \bigcap I^n M$, then the $I$-adic topology on $N$ is trivial, by Artin-Rees, thus $IN = N$. So Nakayama tells us there is an element $a \in 1 + I$ that $aN = 0$. Thus if $I \subseteq \text{rad}(A)$ or $A$ is an integral domain, $N = 0$. This can be used to use induction to prove some theorem.

In particular, for any prime ideal $p$ containing $I$, use the above on $R_p$ shows $N_p = 0$. But also $N$ is f.g., so there exists an element $g \not\in p$ that $N_p = 0$. \hfill $\square$
Cor. (4.2.2.15) [Krull]. For a Noetherian, if \( I \subset \text{rad}(A) \) or \( A \) is a domain, then \( \bigcap_{n=1}^{\infty} I^n = 0 \).

Prop. (4.2.2.16). Notice for any ring \( A \) and a non-zero-divisor \( f \), if \( I = \bigcap_n f^n A \), then \( fI = I \), needless of the Noetherian property.

Proof: If \( x \in I \), \( x = fy \), because \( x \in f^n A \), \( fy = f^n t \) for some \( t \), so \( y = f^{n-1} t \), so \( f \in I \). Thus \( I = fI \).

Def. (4.2.2.17) [Hilbert-Serre]. Let \( A \) be a Noetherian graded ring with \( A_0 \) Artinian that \( A_+ \) is generated by \( A_1 \). For a f.g. graded \( A \)-module \( M = \bigoplus M_n \), we have \( l(M_n) \) is a numerical polynomial of \( n \) sufficiently large, called the Hilbert Polynomial. Its degree is the dimension of \( \text{Supp} M \subset \text{Proj}(A) \).

Proof: We prove by induction on the minimal number of generators of \( A_1 \) (it is finite by (4.2.2.4)). If it is 0, then \( M_n = 0 \) for \( n \) large and the result holds. Now choose \( x \in S_1 \) as one of the minimal set of generators, then the induction hypothesis applies to \( S/(x) \).

Firstly, if \( x \) acts nilpotently on \( M \), then we do induction on the minimal number \( r \) that \( x^r M = 0 \). If \( r = 1 \), then \( M \) is a module over \( S/(x) \) and the assertion holds. If \( r > 1 \), then we can find an exact sequence \( 0 \to M' \to M \to M'' \to 0 \) that \( M', M'' \) has smaller \( r \), then we have the desired result, because \( l \) is additive.

Next, if \( x \) doesn’t act nilpotently on \( M \), let \( M' \subset M \) is the largest submodule that \( x \) acts nilpotently, then there is an exact sequence \( 0 \to M' \to M \to M/M' \to 0 \). So we can assume multiplication by \( x \) is injective on \( M \).

Let \( \overline{M} = M/xM \), then for any \( d \), there are exact sequences
\[
0 \to M_d \xrightarrow{x} M_{d+1} \to \overline{M}_{d+1}.
\]
so \( l(M_{d+1}) - l(M_d) = l(\overline{M}_{d+1}) \). Then we finish by (20.1.2.15).

Cor. (4.2.2.18). Let \( k \) be a field, \( I \subset k[X_1, \ldots, X_n] \) be a non-zero graded ideal, and \( M = k[X_1, \ldots, X_n]/I \), then the numerical polynomial \( n \mapsto \dim_k(M_n) \) has degree \( < d - 1 \).

Proof: The numerical polynomial associated to \( k[X_1, \ldots, X_n] \) is \( n \mapsto \binom{n-1+d}{d} \), and for any non-zero homogenous element \( f \in I \) of degree \( e \), \( f \cdot k[X_1, \ldots, X_n]_{d-e} \subset I_d \); thus \( \dim_k(M_n) < \binom{n-1+d}{d} - \binom{n-e-1+d}{d-1} \), which means the numerical polynomial has degree \( < d - 1 \).

Prop. (4.2.2.19) [Hilbert Polynomial and Dimension]. For a Noetherian local ring \( A \), the Hilbert polynomial of a f.g. module \( M \) w.r.t \( m \) has degree \( \dim M \). And \( \dim M \) is the smallest integer \( r \) s.t. there exists \( x_1, \ldots, x_r \) that \( l(M/x_1 M + \ldots, x_r M) < \infty \).

Proof: Cf. [Mat P76].

3 Completions

This subsubsection should be combined with the derived completion.

Prop. (4.2.3.1). Let the topology on a \( A \)-module be defined by countable filtration of submodules, then iff \( M \) is complete, then \( M/N \) is complete in the quotient topology.

Proof: Write \( x_{i+1} - x_i = y_i + z_i \) with \( y_i \in M_n \) and \( z_i \in N \), then the image of the limit of \( \sum y_i \) is the limit of \( x_i \).
Def. (4.2.3.2) [Completeness]. Let \( I \) be an ideal of \( R \), the \( I \)-adic completion of a \( R \)-module is a functor \( \varphi : M \mapsto \hat{M} = \lim M/I^nM. \) An \( R \)-module is called \( I \)-adically complete if the natural map \( M \mapsto \hat{M} \) is an isomorphism.

This is compatible with the general notion of completion of a topological Abelian groups (10.3.1.5).

Prop. (4.2.3.3). Let \( R \) be a ring and \( I \subset R \) be an ideal, \( \varphi : M \rightarrow N \) be a map of \( R \)-modules. Then
- If \( M/I^2M \rightarrow N/I^2N \) is surjective, then \( \hat{M} \rightarrow \hat{N} \) is surjective. In particular, this holds for \( M \rightarrow N \) surjective.
- If \( 0 \rightarrow K \rightarrow M \rightarrow N \rightarrow 0 \) is exact and \( N \) is flat, then \( 0 \rightarrow \hat{K} \rightarrow \hat{M} \rightarrow \hat{N} \rightarrow 0 \) is exact.
- \( M \otimes_R \hat{R} \rightarrow \hat{M} \) is surjective for any finite \( R \)-module \( M \).

Proof: Cf. [Sta] 0315. \( \square \)

Prop. (4.2.3.4). Let \( I \) be a f.g. ideal of \( A \) and \( M \) an \( A \)-algebra, then \( \hat{M} \) is \( I \)-adically complete and \( \hat{I}^n\hat{M} = \ker(\hat{M} \rightarrow M/I^nM) = (I^nM)^\wedge \).

Proof: Because \( I \) is f.g., so does \( I^n \). If \( I^n = (f_1, \ldots, f_r) \). Applying (4.2.3.3) to \((f_1, \ldots, f_r) : M^r \rightarrow I^nM\) shows
\[
\hat{M}^r \rightarrow (I^nM)^\wedge = \lim_{n \geq n} I^nM/I^nM = \ker(\hat{M} \rightarrow M/I^nM)
\]
but the image is clearly \( I^n\hat{M} \), so \( \hat{M}/I^n\hat{M} \cong M/I^nM \). Taking inverse limit yields \((M^\wedge)^\wedge = M^\wedge \). \( \square \)

Cor. (4.2.3.5) [Completion is Complete]. Let \( I \) be a f.g. ideal of \( A \) and \( (M_n) \) an inverse system of \( A \)-modules that \( I^nM_n = 0 \), then \( M = \lim M_n \) is \( I \)-adically complete.

Proof: We have maps \( M \rightarrow M/I^n \rightarrow M_n \), taking limit, we get \( M \rightarrow \hat{M} \rightarrow M \), so \( M \) is a direct summand of \( \hat{M} \). Since \( \hat{M} \) is \( I \)-adically complete by (4.2.3.4), so does \( M \). \( \square \)

Prop. (4.2.3.6). If \( I \) is a f.g. ideal of \( A \) and \( (M_n) \) is an inverse system of \( A \)-modules that \( M_n = M_{n+1}/I^nM_{n+1} \), then \( M = \lim M_n \) is \( I \)-adically complete and \( M/I^nM = M_n \).

Proof: \( \hat{M} \) is \( I \)-adically complete by (4.2.3.5), and \( M \rightarrow M_n \) are all surjective because the transition maps are surjective. Consider the inverse system \( N_n = \ker(M \rightarrow M_n) \). Since \( M_n = M_{n+1}/I^nM_{n+1} \), the map \( N_{n+1} + I^nM \rightarrow N_n \) is surjective, and thus \( N_{n+1}/(N_{n+1} \cap I^{n+1}M) \rightarrow N_n/(N_n \cap I^nM) \) is surjective.

Taking the inverse limit of the exact sequences
\[
0 \rightarrow N_n/(N_n \cap I^nM) \rightarrow M/I^nM \rightarrow M_n \rightarrow 0,
\]
we get an exact sequence
\[
0 \rightarrow \lim N_n/(N_n \cap I^nM) \rightarrow \hat{M} \rightarrow M.
\]
As \( M \) is \( I \)-adically complete, \( \hat{M} = M \), thus \( \lim N_n/(N_n \cap I^nM) = 0 \), thus \( N_n/(N_n \cap I^nM) = 0 \) for any \( n \) as \( n \) the transition maps are surjective. Then \( M/I^nM = M_n \), as desired. \( \square \)

Cor. (4.2.3.7) [Spectrum Map of Completions]. \( \text{Spec } R^\wedge \rightarrow \text{Spec } R \) has image \( \text{Spec } R/I \subset \text{Spec } R \). This follows from (4.2.3.18) and \( R/I \cong R^\wedge/I \).
\textbf{Prop.(4.2.3.8).} If $I$ is an ideal of $R$ and $0 \to M \to N \to Q \to 0$ is an exact sequence that $Q$ is annihilated by a power of $I$, then completion produces an exact sequence

$$0 \to \widehat{M} \to \widehat{N} \to Q \to 0$$

\textit{Proof:} If $I^n Q = 0$, then $Q/I^n Q = Q$ cor $n \geq c$, and $I^n M \subset M \cap I^n N \subset I^{n-c} M$ because of this. Then $\widehat{M} = \varprojlim M/(M \cap I^n N)$ by (3.1.1.41), and we apply (4.3.3.2) to the inverse system of exact sequences

$$0 \to M/(M \cap I^n N) \to N/I^n N \to Q \to 0$$

to conclude. \hfill $\Box$

\textbf{Cor.(4.2.3.9).} If $A$ is a ring with a nonzero-divisor $t$ and there is an exact sequence $0 \to M \to N \to Q \to 0$ of $A$-modules that $IQ = 0$, then $M$ is $t$-adically complete iff $N$ is $t$-adically complete.

\textit{Proof:} Use snake lemma. \hfill $\Box$

\textbf{Cor.(4.2.3.10).} Take $I = (f)$ and $M = N = R$, then we see that if $t$ is a nonzero-divisor in $R$ then $t$ is a nonzero-divisor in $R$.

\textbf{Prop.(4.2.3.11).} \textit{The completion of a submodule $N \subset M$ is the closure of} $\varphi(N)$ \textit{(By direct construction). The completion of} $M/N$ \textit{is} $M^*/N^*$ \textit{because it is right exact.}

\textbf{Cor.(4.2.3.12).} If $N$ is open in $M$ then $M/N \cong M^*/N^*$ because $M/N$ is discrete hence complete.

\textbf{Prop.(4.2.3.13).} If $A$ is Noetherian and $M$ is finite $A$-module, then the natural map $M \otimes_A A^* \to M^*$ is an isomorphism (use $M$ is finite presentation and tensor & completion is right exact), and five lemma.

\textbf{Cor.(4.2.3.14).} If $A$ is Noetherian, $A \to A^\wedge$ is flat (because flatness is check for finite module).

And when $A$ is complete Hausdorff, any finite module $M$ is complete Hausdorff and hence any its submodule is complete thus closed in it. Hence the the completion of a submodule $N \subset M$ is $\varphi(N)A^*$ in $M^*/MA^*$. In fact this implies complete Hausdorff adic-ring is Zariski.

\textbf{Remark(4.2.3.15).} WARNING: If $A$ is not Noetherian, in general $A \to A^\wedge$ is not flat, Cf.[Sta]0AL8.

\textbf{Lemma(4.2.3.16).} Let $A$ be a ring and $I = (f_1, \ldots, f_r)$ be a f. g. ideal. If $M \to \varprojlim M/f_i^n M$ is surjective for each $i$, then $M \to \varprojlim M/I^n M$ is also surjective.

\textit{Proof:} Note that $\varprojlim M/I^n M = \varprojlim M/(f_1^n, \ldots, f_r^n)M$, as $I^n \subset (f_1^n, \ldots, f_r^n) \subset I^n$, and elements in $\varprojlim M/(f_1^n, \ldots, f_r^n)M$ can be written as an infinite sum $\xi = \sum_n \sum_i f_i^n x_{n,i}$. There is an element $x_i$ mapping to $\sum_n f_i^n x_{n,i}$ for any $i$, thus $\sum x_i$ maps to $\xi$. \hfill $\Box$

\textbf{Lemma(4.2.3.17).} Let $A$ be a ring and $I \subset J$ be ideals, if $M$ is $J$-adically complete and $I$ is f.g., then $M$ is $I$-adically complete.

\textit{Proof:} It is clearly $I$-adically Hausdorff, and for completeness, by (4.2.3.16) it suffices to show for $I = (f)$: Let $x_n \in M$ with $x_n - x_{n+1} \in f^n M$, then $\{x_n\}$ is $J$-adically Cauchy, thus there is an element $x$ that $x - x_n \in J^n$, and we can replace $x_n$ by $x_n - x$ to assume $x_n \in J^n$. Now we prove $x_n \in (f^n)$: Assume $x_n - x_{n+1} = f^n z_n$, then

$$x_n = f^n (z_n + f \sum_{i=1}^{n+1} z_i)$$

This equation is true because it is $J$-adically Cauchy. \hfill $\Box$
**Properties of Complete Rings**

**Prop. (4.2.3.18).** If $A$ is $I$-adically complete, then $I \subset \text{rad} A$.

**Prop. (4.2.3.19).** Let $A$ be a ring with a non-zero-divisor $t$, then any limit of $t$-adically complete algebras is $t$-adically complete.

**Proof:** Check the definition directly. \qed

**Prop. (4.2.3.20) [Zariski Rings].** A Noetherian $I$-adic ring is called **Zariski ring** if it satisfies the following equivalent conditions:

- Every finite module is Hausdorff in the $I$-adic topology.
- Every submodule in a finite module is closed in the $I$-adic topology.
- Every ideal is closed.
- $I \subset \text{rad} A$.
- $A^\wedge \triangleleft A$ is f.f.

Hence every complete Hausdorff ring is Zariski.

**Proof:**

1 $\rightarrow$ 2: Apply it to the submodule $M/N$.

3 $\rightarrow$ 4: If $I \not\subseteq m$, then $I^n + m = A$, thus $\overline{M} = A$, contradiction.

4 $\rightarrow$ 1: by intersection theorem (4.2.2.14).

4 $\rightarrow$ 5: for any maximal ideal $m$, $I \subset m$ so it is open, thus $A^*/mA^* = A/m \neq 0$ by (4.2.3.12) thus f.f. by (4.4.1.5).

5 $\rightarrow$ 1: by (4.4.1.21), for any $m$ maximal, there is a maximal ideal $m'$ lying over $m$, so $IA^* \subset m^*$ by (4.2.3.14), thus $I \subset m$, hence $I \subset \text{rad} A$. \qed

**Cor. (4.2.3.21).** In a Zariski ring $A$, maximal ideals are open, thus $A/m \cong A^*/mA^*$ by (4.2.3.12), thus Spec $A^* \rightarrow$ Spec $A$ is bijection on closed pt.

**Prop. (4.2.3.22) [Cohen Structure Theorem].** If $A$ is a complete local ring containing a field $k$ that the residue field is separably generated over $k$, then there is a field $K$ containing $k$ that is a Cohen ring, i.e. complete local ring with a prime number as a uniformizer, that has the same residue field as $A$.

**Proof:** \qed

**Lemma (4.2.3.23) [Complete Interchanging Lemma].** If $R$ is a commutative ring, $x, y \in R$, if $x$ is not a zero-divisor in $R$ and $R$ is $x$-adically complete, and $y$ is not a zero-divisor in $R/x$ and $R/x$ is $y$-adically complete, then the same is true with $x, y$ interchanged.

**Proof:** \qed

4 Dimension

**Def. (4.2.4.1) [Dimensions and Heights].** For a $A$-module $M$, $\text{dim}(M)$ is defined as $\text{dim}(A/\text{Ann}(M))$.

The **height** of an ideal $I$ in $A$ is defined as the infimum of heights of the prime ideals over $I$.

The **dimension** of a ring $R$ is defined to be the supremum of heights of prime ideals of $R$.

**Prop. (4.2.4.2).** For any ring $A$ $\text{dim} A = \sup \text{dim} A_p$. 


Def. (4.2.4.3) [Catenary Rings]. \( A \in \mathcal{C}	ext{Alg} \) is called **catenary** if for any pair of primes \( p \subset q \subset A \), any maximal chain of primes \( p = p_0 \subset p_1 \subset \ldots \subset p_e = q \) has the same length. A Noetherian ring is called **uniformly catenary** if all f.g. algebras over it are catenary.

Prop. (4.2.4.4). \( A \in \mathcal{C}	ext{Alg} \) is catenary iff \( \text{Spec} \ A \) is a catenary space (3.8.3.34).

Prop. (4.2.4.5). Any quotient ring and localization of a (uniformly)catenary ring is catenary. Any quotient of a Noetherian uniformly catenary ring is uniformly catenary. Catenary and uniformly catenary are stalkwise properties (4.1.4.2).

Prop. (4.2.4.6). If \( (A, m) \) is a Noetherian local ring, then \( A \) is catenary iff \( p \to \dim(A/p) \) is a dimension function on \( \text{Spec} \ A \).

Proof: This follows from (3.8.4.13)(3.8.3.39) and (3.8.3.37).

Example (4.2.4.7) [Uniformly Catenary Rings]. The following are same examples of uniformly catenary Rings:

- A f.g. algebra over a uniformly catenary ring.
- A Noetherian C.M. rings.
- 1-dimensional Noetherian domains,
- Fields.

Proof: Cf. [Sta]00NM.?

Def. (4.2.4.8) [Hilbert Polynomials]. Let \( (A, m) \) be a Noetherian local ring, \( I \) an ideal of definition, then

**Dimension of Noetherian Local Rings**

Prop. (4.2.4.9). For a Noetherian local ring \( R \), the following three numbers are equal:

- \( \dim R \).
- \( d(R) \).
- the minimal number of elements needed to generate an ideal of definition of \( R \) (4.1.1.11).

A **system of parameters** is \( d \) elements \( g_1, \ldots, g_d \) that generate an ideal of definition of \( R \), where \( d = \dim R \).

Proof: Cf. [Sta]00KQ.?

Cor. (4.2.4.10). The dimension of a Noetherian local ring is finite, by item 3. Thus the codimension of a subscheme in a Noetherian scheme is finite.

Cor. (4.2.4.11). If \( A \) is a Noetherian local ring with maximal ideal \( \mathfrak{m} \), then \( \dim A \leq \dim_k \mathfrak{m}/\mathfrak{m}^2 \).

Proof: By Nakayama, if \( x_1, \ldots, x_d \in \mathfrak{m} \) generate \( \mathfrak{m}/\mathfrak{m}^2 \), then \( (x_1, \ldots, x_d) = \mathfrak{m} \).
4.2. COMMUTATIVE ALGEBRA II 387

Dimension and Ring Extensions

Prop. (4.2.4.12) [Dimension and Going-Up(Down)]. If \( A \to B \) is a ring map that Spec map is surjective and \( A \to B \) satisfies either going-up or going-down, then \( \text{dim } B \geq \text{dim } A \).

**Proof:** The hypothesis implies any chain of primes in \( A \) can lifted to a chain of primes in \( B \). \( \square \)

Prop. (4.2.4.13) [Dimensions and Noetherian Ring Extensions]. Let \( A \to B \) be a map between Noetherian rings, \( P \) a prime ideal of \( B \), \( p = P \cap A \), then:
- \( \text{ht}(P) \leq \text{ht}(p) + \text{ht}(P/pB) \), in other words \( \text{dim}(B_P) \leq \text{dim}(A_p) + \text{dim}(B_P/pB_P) \).
- equality holds if going-down holds. For example, if it is flat (4.1.7.13).

**Proof:**
1: Localize at \( p \) and \( P \), we may assume \( A, B \) are local rings with maximal ideals \( p \) and \( P \), then use the characterization (4.2.4.9) of dimension, if \( x_1, \ldots, x_d \) generate an ideal of definition of \( A_p \) and \( y_1, \ldots, y_e \) generate an ideal of definition of \( B_P/pB_P \), then \( x_1, \ldots, x_d, y_1, \ldots, y_e \) generate an ideal of definition of \( B_P \).
2: If going down holds, for any chain of primes in \( B_P \) containing \( pB_P \), we can lift the chain of primes in \( A_p \) to a chain of primes in \( B_P \) to get a longer chain, thus we get the other direction of inequality. \( \square \)

Prop. (4.2.4.14) [Dimension of Integral Extensions]. Let \( A \to B \) be an integral ring map, then:
1. Spec maps closed points to closed points, and \( \text{dim } (A) \geq \text{dim } (B) \), which equality if \( A \subset B \).
2. If \( A, B \) is Noetherian, \( \text{ht}(P) \leq \text{ht}(P \cap A) \)
3. If \( A, B \) is Noetherian and going down holds, then \( \text{ht}(J) = \text{ht}(J \cap A) \) for any ideal \( J \subset B \).

**Proof:**
1: By (4.2.4.5), there is no inclusion relation between prime over a fixed prime, so \( \text{dim } (B) \leq \text{dim } (A) \). On the other hand, if \( A \subset B \), then Spec map is surjective going-up holds (4.2.4.12), so \( \text{dim } (B) \geq \text{dim } (A) (4.2.4.12) \).
2: Follows from (4.2.4.13)(1) since \( \text{ht}(P/(P \cap A)B) = 0 \) by (4.2.4.15).
3: In this case, \( \text{ht}(P) = \text{ht}(P \cap A) \) holds by (4.2.4.13)(2), then use the surjectiveness of Spec for the integral extension \( A/J \cap A \subset B/J (4.2.4.15) \). \( \square \)

Cor. (4.2.4.15). If \( A \to B \) is integral and faithfully flat, then \( \text{dim } A = \text{dim } B \).

**Proof:** This follows from (4.2.4.14) and (4.4.1.28). \( \square \)

Prop. (4.2.4.16) [Dimension and Completion]. For a local ring \( A \), \( \text{dim } \hat{A} = \text{dim } A \).

**Proof:**

Noetherian Normalization

Prop. (4.2.4.17). For a Noetherian ring \( A \), \( \text{dim } A[X] = \text{dim } A + 1 \).

**Proof:** Let \( \mathfrak{p} \) be a prime ideal of \( A \) and let \( \mathfrak{q} \) be a prime ideal of \( A[X] \) maximal among primes lying over \( \mathfrak{p} \), then \( \text{ht}(\mathfrak{q}/\mathfrak{p}A[X]) = 1 \). In fact, by localizing, we can assume \( \mathfrak{p} \) is a maximal ideal, then \( A[x]/\mathfrak{p}A[x] \) is a polynomial ring over a field thus a PID and \( \text{ht}(\mathfrak{q}/\mathfrak{p}A[X]) = 1 \). Thus \( \text{ht}(\mathfrak{q}) = \text{ht}(\mathfrak{p}) + 1 \) by (4.2.4.13). Now we are done, because \( \text{Spec } A[X] \to \text{Spec } A \) is surjective. \( \square \)
Prop. (4.2.4.18) [Krull’s Height Theorem]. In a Noetherian domain \( R \), the height of an ideal generated by \( n \) elements is at most \( n \).

\textit{Proof:} Let \( p \) be a minimal ideal containing \( (f_1, \ldots, f_n) \), then it suffices to show \( \dim(R_p) \leq n \). In this case, \( (f_1, \ldots, f_n) \) is an ideal of definition of \( R_p \), thus we can use (4.2.4.9). \( \square \)

Prop. (4.2.4.19) [Number of Generators]. To show an ideal \( I \subset A \) cannot be generated by smaller than \( n \) element, choose a maximal ideal \( m \), then show that \( \dim_{A/m} I/mI \geq n \).

Cor. (4.2.4.20).
- \((x, z)\) is not principal in \( k[x, y, z] \).
- \((wz - xy)\) is not principal in \( k[x, y, z] \).
- \((xy, yz, xz)\) is not generated by two elements in \( k[x, y, z] \).

Lemma (4.2.4.21). Let \( A = k[X_1, \ldots, X_n] \) be a polynomial ring over a field \( k \), and \( I \) is an ideal of \( A \) of height \( r \), then we can choose \( Y_1, \ldots, Y_n \in A \) that \( A \) is integral over \( k[Y_1, \ldots, Y_n] \) and \( I \cap k[Y_1, \ldots, Y_n] = (Y_1, \ldots, Y_r) \).

\textit{Proof:} We use induction on \( r \). \( r = 0 \) is easy. For \( r = 1 \), let \( f(X) \) be any non-zero polynomial in \( I \), then we can assign suitable integral weights \( d_1, d_2, \ldots, d_n \) to \( X_i \) such that monomials of \( f \) have different weights. Put \( Y_i = X_i - X_1^{d_i} \) for \( i \geq 2 \), and

\[ Y_1 = f(X) = f(X_1, Y_2 + X_1^{d_2}, \ldots, Y_n + X_1^{d_n}) = a_1X_1^N + g(X_1, Y_2, \ldots, Y_n) \]

where \( g \) has degree in \( X_1 \) lower that \( N \). Then \( X_1 \) is integral over \( k[Y_1, \ldots, Y_n] \), and hence \( X_1 = Y_1 + X_1^{d_1} \) is also integral over \( k[Y] \).

Now \((Y_1)\) is a prime ideal in \( k[Y] \) of height 1 and \( (Y_1) \in I \cap k[Y] \). Also notice \( I \cap k[Y] \) has height 1 by (4.2.4.14) (Because going-down holds by (4.1.7.17)), so \( (Y_1) = I \cap k[Y] \).

For \( r \geq 2 \), let \( J \subset I \) be an ideal with height \( r - 1 \), let \( J \) be an ideal of \( k[X] \) contained in \( I \) that \( \text{ht}(J) = r - 1 \). (This is possible by choosing \( f_i \) out of all minimal primes containing \((f_1, \ldots, f_{r-1})\) and use Krull’s Height Theorem). By induction hypothesis, there exists \( Z_1, \ldots, Z_n \) that \( k[X] \) is integral over \( k[Z] \), and \( J \cap k[Z] = (Z_1, \ldots, Z_{r-1}) \). Now \( \text{ht}(I \cap k[Z]) = r \) by the same argument above, thus there exist \( f \in I \cap k[Z] \setminus (Z_1, \ldots, Z_{r-1}) \), and do the same for \( r = 1 \) again, we can find the desired \( Y_i \) that \( Y_k = Z_k \) for \( k \leq r - 1 \). \( \square \)

Prop. (4.2.4.22) [Noetherian Normalization Theorem]. If \( A \) is a f.g. algebra over a field, then there are \( r \) alg. independent elements \( y_i \) that \( A \) is integral over \( k[y_i] \).

\textit{Proof:} Let \( A = k[X_1, \ldots, X_n]/I \) and \( \text{height}(I) = n - r \), then by the lemma we can choose \( Y_1, \ldots, Y_n \) that \( k[X_1, \ldots, X_n] \) is integral over \( k[Y_1, \ldots, Y_n] \) (so \( Y_1, \ldots, Y_n \) are algebraically independent) and \( I \cap k[Y_1, \ldots, Y_n] = (Y_{r+1}, \ldots, Y_n) \). Now we can just choose \( y_i = Y_i \) for \( i \leq r \). \( \square \)

Cor. (4.2.4.23) [Dimension and Transcendental Degree]. If \( A \) is a f.g. integral ring over a field \( k \), then \( \dim A = \text{tr.deg}_k A \).

\textit{Proof:} This is because integral extensions of integral Noetherian rings have the same dimensions (4.2.4.14) and their fraction fields have the same transcendental degrees. \( \square \)

Cor. (4.2.4.24). Let \( A, B \) be f.g. algebras over a field \( k \), then \( \dim(A \otimes_k B) = \dim A + \dim B \).
Cor. (4.2.4.25) [Dimension and Field Base Change]. Let $K/k$ be a field extension and $S$ a f.g. algebra over $k$, then $\dim S = \dim S \otimes_k K$.

Proof: By Noetherian normalization, there exists a finite injective map $k[d_1, \ldots, d_n] \to S$ where $n = \dim S$. Then there exists a finite injective map $K[d_1, \ldots, d_n] \to S_K$, so $\dim S \otimes_k K = n$, by (4.2.4.14) and (4.2.4.17).

Prop. (4.2.4.26) [Codimensions and Field Base Change]. Let $K/k$ be a field extension and $S$ a f.g. $k$-algebra. Let $\mathfrak{a}$ be a prime of $S$ and $q_K$ be a prime of $S_K$ lying over $\mathfrak{a}$, then

$$\dim(S_K \otimes_S k(q))_{q_K} = \dim(S_K)_{q_K} - \dim S_{\mathfrak{a}} = \deg k(q) - \deg k(q_K).$$

Moreover, for any $\mathfrak{a}$, we can choose $q_K$ so that this number is 0.

Proof: Cf.[Sta]0CWE.

Local Dimension over Fields

Prop. (4.2.4.27) [Local Dimension]. Let $S$ be an algebra f.g. over a field $k$, $X = \Spec S$ and $x \in X$, then the following three numbers are equal:

- the local dimension (3.8.3.25) $\dim_x(X)$.
- $\max \dim (Z)$ where $Z$ runs through irreducible components of $X$ passing through $x$.
- $\min \dim(S_m)$, where $m$ are maximal ideals containing $\mathfrak{p}_x$.

Proof: Cf.[Sta]00OT.

Lemma (4.2.4.28). Let $k$ be a field and $S$ a f.g. $k$-algebra, $X = \Spec S$, $x \in X$, then

$$\dim_x(X) = \dim S_{\mathfrak{p}} + \deg k(\mathfrak{p}).$$

Proof: Cf.[Sta]00P1.

Cor. (4.2.4.29). Let $S' \to S$ be a surjection of f.g. algebras over a field $k$, $\mathfrak{p}$ a prime ideal of $S$ and $\mathfrak{p}'$ its inverse image in $S'$, corresponding to $x, x'$ in $X = \Spec S, X' = \Spec S'$ resp., then

$$\dim_{x'}(X') - \dim_x(X) = \ht(\mathfrak{p}') - \ht(\mathfrak{p}).$$

Def. (4.2.4.30) [Relative Dimension]. Let $R \to S$ be a ring map of f.t., and $\mathfrak{a} \subseteq S$ be a prime over $\mathfrak{p} \subseteq R$, then we define the relative dimension of $S/R$ at $\mathfrak{a}$ to be $\dim_{\mathfrak{a}}(\Spec S)_{\mathfrak{p}}$. The supremum of all these numbers over $\mathfrak{a} \subseteq \Spec S$ is called the relative dimension of $S/R$, denoted by $\dim(S/R)$.

Lemma (4.2.4.31) [Local Dimension and Field Extension]. Let $K/k$ be a field extension, $S$ be a f.g. $k$-algebra, and $X = \Spec S$. Now if $\mathfrak{p}_K$ is an element of $S_K$ lying over $\mathfrak{p} \subseteq S$, then $\dim S_{\mathfrak{p}} = \dim_{\mathfrak{p}_K}(S_K)$.

Proof: The proof is by reduction to polynomial ring. Let $S = k[X_1, \ldots, X_n]/I$, let $\mathfrak{p}_K', \mathfrak{p}'$ be primes of $k[X_1, \ldots, X_n]$ and $K[X_1, \ldots, X_n]$ that is the image of $x$ and $x_K$, then there is a commutative diagram

$$
\begin{array}{ccc}
K[X_1, \ldots, X_n]_{\mathfrak{a}_K} & \longrightarrow & (S_K)_{q_K} \\
\downarrow & & \downarrow \\
k[X_1, \ldots, X_n]_{\mathfrak{a}_K} & \longrightarrow & S_{\mathfrak{a}}
\end{array}
$$
The vertical arrows are flat because they are local morphisms of flat maps, and their fibers are the same, so by (5.6.3.17), \( \text{ht}(q_K') - \text{ht}(q_K) = \text{ht}(q) - \text{ht}(q) \). Also use (4.2.4.29) on the horizontal maps, then we get the desired assertion. □

Prop. (4.2.4.32) [Semicontinuity of Dimensions]. Let \( f : R \to S \) be a ring map of f.t., then the map \( q \mapsto \dim_S(S\langle R) \) is a upper-semicontinuous function on \( \text{Spec}(S) \).

Moreover, if \( f \) is of f.p., then the set \( \{ q | \dim_S(S\langle R) \leq n \} \) is quasi-compact open in \( \text{Spec}(S) \).

Proof: Cf. [Sta]00QH, 00QJ. □

5 Support and Associated Primes

Def. (4.2.5.1) [Support of a Module]. The support \( \text{Supp}(M) \) of a module \( M \) is the set of all \( p \) that \( M_p \neq 0 \). When \( M \) is f.g., \( \text{Supp}(M) = V(\text{Ann}(M)) \).

Prop. (4.2.5.2) [Support is Non-Empty]. The support of a nonzero module is not empty, because triviality is stalkwise by (4.1.4.2).

Prop. (4.2.5.3). If \( 0 \to N \to M \to Q \to 0 \), then we have \( \text{Supp}(M) = \text{Supp}(N) \cup \text{Supp}(Q) \), this is because localization is exact.

Cor. (4.2.5.4).

Prop. (4.2.5.5). Let \( (R, m) \) be a Noetherian local ring and \( M \) a finite \( R \)-module, \( f \in m \), then
\[
\dim \text{Supp}(M) - 1 \leq \dim(\text{Supp}(M/fM)) \leq \dim(\text{Supp}(M))
\]

Proof: Cf. [Sta]0B52. □

Prop. (4.2.5.6). Let \( 0 = M_0 \subset M_1 \subset \ldots \subset M_n = M \) be a filtration of \( M \) that \( M_i/M_{i-1} \cong R/p_i \) where \( p_i \) are primes, by (4.1.1.45), then \( \text{Supp}(M) = \cup_i V(p_i) \).

In particular, the minimal primes in \( \{ p_i \} \) are the same as the minimal primes of \( \text{Supp}(M) \). Moreover, the multiplicity of a prime \( p_i \) equals \( \text{length}_{R/p_i} M_p \).

Proof: Cf. [Sta]00L7. □

Prop. (4.2.5.7). Let \( (R, m) \) be a Noetherian local ring and \( M \) a non-zero finite \( R \)-module, then \( \text{Supp}(M) = V(m) \) iff \( \text{length}_R(M) < \infty \).

Proof: Cf. [Sta]00L5. □

Prop. (4.2.5.8). Let \( A \) be Noetherian and \( I \) be an ideal, then \( I^n M = 0 \) for some \( n \) iff \( \text{Supp}(M) \subset V(I) \).

Proof: If \( I^n M = 0 \), then if \( I \nsubseteq P \), then \( M_P = 0 \). Conversely, we have a filtration of \( M \), and by (4.2.5.3) we have all the \( P_i \) include \( I \), so \( I^n \) annihilate \( M \). □

Prop. (4.2.5.9). If \( R \) is a ring and \( M \) is a f.p. \( R \)-module, then \( \text{Supp}(M) \) is a closed subset of \( \text{Spec} R \) whose complement is quasi-compact.

Proof: Let \( R^m \to R^n \to M \to 0 \), then the support of \( M \) is just the the locus that some minor of the linear map from \( R^m \to R^n \) doesn’t vanish. Then its complement is quasi-compact. □
Prop. (4.2.5.10). Let \((R, \mathfrak{m})\) be a Noetherian local ring and \(M\) is a finite \(R\)-module, then \(d(M) = \dim(\text{Supp}(M))\).

Proof: Cf.[Sta]00L8.

Prop. (4.2.5.11). Let \(R\) be a Noetherian ring and \(0 \to M' \to M \to M'' \to 0\) be an exact sequence of finite \(R\)-modules, then \(\dim \text{Supp}(M) = \max(\dim \text{Supp}(M'), \dim \text{Supp}(M''))\).

Proof: Cf.[Sta]0B51.

Associated Primes of a Module

Def. (4.2.5.12) [Associated Primes of a Module]. The weakly associated primes \(\text{Ass}(M)\) of an \(A\)-module \(M\) is the set of minimal primes of \(A/\text{Ann}(m)\) for some \(m \in M\).

The associated primes \(\text{Ass}(M)\) is the set of primes \(\{p = \text{Ann}(m)\}\) where \(m \in M\).

Prop. (4.2.5.13). \(\text{Ass}_R(M) \subset \text{WeakAss}_R(M)\), and if \(R\) is Noetherian, the converse is also true.

Proof: Cf.[Sta]058A.

Prop. (4.2.5.14) [Associated Primes and Exact Sequence]. For an exact sequence \(0 \to M_1 \to M \to M_2 \to 0\), \(\text{WeakAsso}(M) \subset \text{WeakAsso}(M_1) \cup \text{WeakAsso}(M_2)\) and \(\text{WeakAsso}(M_1) \subset \text{WeakAsso}(M)\).

Proof: Cf.[Sta]0548?

Cor. (4.2.5.15) [F.M. Associated Primes]. For a finite module \(M\) over a Noetherian ring \(A\), \(\text{Ass}_A(M)\) is finite by (4.1.1.45).

Prop. (4.2.5.16) [Associated Primes and Support]. \(\text{WeakAsso}(M) \subset \text{Supp} M\), and their minimal elements are the same.

If \(M \neq 0\), \(\text{WeakAsso}(M) \neq \emptyset\) by (4.2.5.2), and \(\text{WeakAsso}(A/I)\) contains all the minimal primes over \(I\).

Proof: If \(p = \text{Ann}(m)\), then \(m\) is nonzero in \(M_p\), so \(M_p\) is nonzero, i.e. \(p \in \text{Supp}(M)\).

For the second assertion, we first prove for \(M\) finite, and then write any module as sum of finite submodules, and use the fact \(\text{Supp}\) and \(\text{ass}\) are all unions of those of the submodules. Cf.[Sta]05C4 0588?

Prop. (4.2.5.17) [Weakly Associated Primes and Zero-divisors]. Let \(M\) a \(R\)-module, then the union of the weakly associated primes of \(M\) is the set of zero-divisors in \(M\).

Proof: Elements in associated points are zero-divisors obviously, and conversely, if \(xm = 0\), then \(x \in \text{Ann}(m)\) and \(\text{Ann}(m)\) has an associated point \(q\) by (4.2.5.16). Now \(x\) must be in \(q\) and \(q\) is also an associated point of \(M\) by (4.2.5.16). Cf.[Sta]05C3?

Cor. (4.2.5.18). Use the prime avoidance (4.1.1.4), we can prove if \(R\) is Noetherian and \(M\) is a finite \(R\)-module, then \(I \subset p\) for some \(p \in \text{WeakAss}(M)\) iff \(I\) consists of zero-divisors.
Prop. (4.2.5.19) [Associated Primes and Maps]. For a ring map \( \varphi : R \to S \) and a \( S \)-module \( M \), then
\[
\text{Spec}(\varphi)(\text{Ass}_S(M)) \subset \text{Ass}_R(M) \subset \text{WeakAss}_R(M) \subset \text{Spec}(\varphi)(\text{WeakAss}_S(M)).
\]
Equalities hold if \( S \) is Noetherian. Also \( \text{WeakAss}_R(M) = \text{Spec}(\varphi)(\text{WeakAss}_S(M)) \) if \( \varphi \) is a finite ring map.

Proof: Cf. [Sta] 05C7, 05E1.

We prove it is equal. If \( p = \text{Ann}_R(m) \), then we let \( I = \text{Ann}_S(m) \), then \( R/p \subset S/I \subset M \), so by (4.1.7.25), there is a minimal prime of \( S \) over \( I \) that are mapped to \( p \), now this prime is in \( \text{Ass}(S/I) \) by (4.2.5.16) and also in \( \text{Ass}_S(M) \) by (4.2.5.14).

Prop. (4.2.5.20) [Associated Primes and Localization]. Let \( \varphi : \text{Spec} S^{-1}A \to \text{Spec} A \) and \( M \) an \( A \)-module, then

\[
\text{Ass}_A(S^{-1}M) = \text{Spec}(\varphi)(\text{WeakAss}_{S^{-1}A}(S^{-1}M)) = \text{WeakAss}_A(M) \cap \varphi(\text{Spec}(S^{-1}R)).
\]

Proof: Cf. [Sta] 05C9?.

The first equality is by (4.2.5.19). For the second, if \( \text{Ann}_A(x) = p \) and \( p \cap S = \emptyset \), then \( \text{Ann}_{S^{-1}A}(x/1) = S^{-1}(p) \). Conversely, if \( \text{Ann}_{S^{-1}A}(x/s) = S^{-1}p \), then \( p \cap S = \emptyset \), and \( \text{Ann}_A(x) \subset S^{-1}p \cap A = p \).

Cor. (4.2.5.21) [Associated Primes are Stalkwise]. Let \( R \) be a ring and \( M \) an \( R \)-module, \( p \subset R \), then the following are equivalent:

- \( p \subset \text{WeakAss}(M) \).
- \( pR_p \subset \text{WeakAss}(M_p) \).
- \( M_p \) contains some element \( m \) that \( \sqrt{\text{Ann}(m)} = pR_p \).

Proof: 1 \( \to \) 2: \( p \) is a minimal prime of \( I = \text{Ann}(m) \) for some \( m \in M \), so \( I_p \) is the minimal prime of \( \text{Ann}(m) \subset R_p \).

2 \( \to \) 3: As \( pR_p \) is the maximal prime, it is the only prime over \( \text{Ann}(m) \), so \( pR_p = \sqrt{\text{Ann}(m)} \).

3 \( \to \) 1: This means there are some \( m \in M \) that \( \sqrt{I_p} = pR_p \), which means that \( p \) is a minimal prime over \( \text{Ann}(m) \).

Prop. (4.2.5.22). If \( M \) is an \( R \)-module, then \( M \to \prod_{p \subset \text{WeakAss}(M)} M_p \) is injective.

Proof: Cf. [Sta] 05CB.

If \( m \neq 0 \in M \), there is an associated prime \( p \) of \( Rm(4.2.5.16) \), then it is an associated prime of \( M \), and then \( (x)_p \subset M_p \) is not zero.

Def. (4.2.5.23) [Embedded Primes]. A non-minimal prime in \( \text{Ass}_R(M) \) is called a embedded prime. Equivalently, it is an associated point that is not a generic point of \( \text{Supp}(M) \).

Prop. (4.2.5.24). For a reduced ring \( R \), \( \text{WeakAss}_R(R) \) is just the set of minimal primes of \( R \).

Proof: Cf. [Sta] 0EMA.

Cor. (4.2.5.25) [Reduced Ring No Embedded Primes]. A reduced ring has no embedded primes, because it has no nilpotent elements. Hence all its associated primes are just the minimal primes.

Def. (4.2.5.26) [Unmixed Ideals]. \( I \) is called unmixed if primes in \( \text{Ass}(A/I) \) all have the same height. In particular, they don’t contain each other.
Primary Decomposition

**Def.** (4.2.5.27). For $R$ Noetherian, a $R$-module $M$ is called **coprimary** iff it has only one associated primes. A submodule $N$ of $M$ is called **$p$-primary** iff $\text{Ass}(M/N) = \{p\}$. A ring is called **$p$-primary** iff $(0)$ is $p$-primary.

Notice coprimary is equivalent to the following: if $a \in A$ is a zero divisor for $M$, then for each $x \in M$, there is a $n$ that $a^n x = 0$, i.e. **locally nilpotent**. And for ideals in a Noetherian ring, this is equivalent to $r(I)$ is a prime.

**Proof:** If $M$ is $p$-primary, if $x \in M$ is nonzero, then $\text{Ass}(Rx) = \{p\}$, so $p$ is the unique minimal element of $\text{Supp}(Rx) = V(\text{Ann}(x))$ by (4.2.5.16). So $p$ is the radical of $\text{Ann}(x)$, i.e. $a^n x = 0$ for some $n$ (4.2.6.2).

Conversely, we know the ideal $p$ of locally nilpotent elements equals the union of the associated primes (4.2.5.17), so if $q \in \text{Ass}M = \text{Ann}(x)$, then by definition, $p \subseteq q$. So $p = q$, and thus $\text{Ass}M = \{p\}$.

**Lemma** (4.2.5.28). A primary ring has no nontrivial idempotent element, because $e$ and $1 - e$ will all belong to the same minimal ideal $p$.

**Lemma** (4.2.5.29). The intersection of $p$-primary submodules are $p$-primary. (Because there is a injection $M/Q_1 \cap Q_2 \to M/Q_1 \oplus M/Q_2$).

**Lemma** (4.2.5.30) [Associated Prime and Primary Decomposition]. If $N = \cap Q_i$ is an irredundant primary decomposition and if $Q_i$ belongs to $p_i$, then we have $\text{Ass}(M/N) = \{p_1, \ldots, p_r\}$.

**Proof:** There is a injection $M/N \to M/Q_1 \oplus \ldots M/Q_r$ which shows $\text{Ass}(M/N) \subseteq \{p_1, \ldots, p_r\}$. And for the inverse, notice $Q_2 \cap \ldots \cap Q_r/N$ is a submodule of $M/Q_1$, which shows $\text{Ass}(Q_2 \cap \ldots \cap Q_r/N) = \{p_1\}$ by (4.2.5.16).

**Prop.** (4.2.5.31). If $N$ is a $p$-primary submodule of a $R$-module $M$, and $p'$ is a prime ideal, then

- $N_{p'} = M_{p'}$ if $p \not\subseteq p'$.
- $N = M \cap N_{p'}$ if $p \subseteq p'$.

**Proof:** $M_{p'}/N_{p'} = (M/N)_{p'}$, and $\text{Ass}((M/N)_{p'}) = \text{Ass}(M/N) \cap \{\text{primes contained in } p'\} = \emptyset$ by (4.2.5.20). So $M_{p'} = M_{p'}$ by (4.2.5.16).

For the second, notice it suffices to show $M/N \to M_{p'}/N_{p'}$ is injective. But this is because $A - p'$ contains no nonzero-divisor, by (4.2.5.17).

**Cor.** (4.2.5.32) [Second Uniqueness of Primary Decomposition]. For an irredundant primary decomposition $N = \cap Q_i$, if $Q_1$ corresponds to $p_1$ and $p_1$ is minimal in $\text{Ass}(M/N)$, then $Q_1 = M \cap N_{p_1}$. In particular, the minimal prime part of a irredundant primary decomposition is uniquely determined.

**Proof:** By the above proposition, there are elements $u_i$ of $Q_i$, $i \neq 1$ that are mapped to units in $M_{p_1}$, so $Q_1 \cdot u_2 u_3 \ldots u_r$ is mapped onto the image of $Q_1 \to M_{p_1}$. Then $Q_1 = M \cap (Q_1)_{p_1} = M \cap N_{p_1}$.

**Prop.** (4.2.5.33). If $R$ is Noetherian and $M$ is a $R$-module, there are $p$-primary submodules $Q(p)$ for each $p \in \text{Ass}M$ that $(0) = \bigcap_{p \in \text{Ass}M} Q(p)$. 


Proof: For a $p \in \text{Ass}M$, we seek $Q(p)$ to be the maximal submodule $N$ that $p \notin \text{Ass}N$. This has a maximal ideal because of Zorn and the fact $\text{Ass}(\bigcup N_\lambda) = \bigcup \text{Ass}(N_\lambda)$. Then we have $\text{Ass}(M/Q(p)) = \{p\}$, otherwise there is another $p'$, then there is a $Q'/Q(p) \cong A/p'$. Now $Q'$ is bigger than $Q(p)$.

Finally, $(0) = \cap_{p \in \text{Ass}M} Q(p)$ because it has no associated primes. □

Cor. (4.2.5.34) [Primary Decomposition]. If $M$ is f.g. over a Noetherian ring $R$, then any submodule has a primary decomposition. (Notice $M$ has only f.m. associated primes).

Def. (4.2.5.35) [Symbolic Power]. For a prime ideal $p$ in a Noetherian ring, The $n$-th symbolic power $p^{(n)}$ is defined to be the $p$-primary component of $p^n$, who has only one minimal prime(hence one associated prime). The symbolic power is giving by $p^n A_p \cap A$ by (4.2.5.32).

6 Jacobson Radical and Nilradical

Nilradical

Def. (4.2.6.1) [Nilradical]. The nilradical of a commutative ring $R$ is defined to be the ideal consisting of nilpotent elements.

Prop. (4.2.6.2). The nilradical $\mathfrak{n}$ of a ring $A$ (4.2.6.1) is the intersection of all prime ideals.

Proof: Every nilpotent element is contained in every prime, and if $a$ is not nilpotent, then the localization $A_a$ is nonzero, hence there is a maximal ideal, i.e. there is a prime of $A$ not containing $a$. □

Cor. (4.2.6.3). In particular, $\text{Spec} A/\mathfrak{n} \to \text{Spec} A$ is a homeomorphism, and $A \to A/\mathfrak{n}$ induces a bijection on idempotents and units.

Jacobson Ring

Def. (4.2.6.4) [Jacobson Ring]. A commutative ring is called Jacobson if every prime ideal is an intersection of maximal ideals. In particular, the Jacobson radical equals the nilradical. This is equivalent to every radical ideal is an intersection of maximal primes.

Prop. (4.2.6.5). $R$ is Jacobson iff $\text{Spec} R$ is Jacobson space (3.8.3.21). In particular, the closed pts are dense in any closed subsets (Hilbert’s Nullstellensatz satisfied).

Proof: We need to show that a locally closed subset contains a closed pt, we assume this set is of the form $V(I) \cap D(f)$, $I$ is radical, then $f \notin I$, then by the condition, there is a $I \subset \mathfrak{m}$ that $f \notin \mathfrak{m}$, thus the result.

Conversely, for a radical ideal, let $J = \cap_{I \subset \mathfrak{m}} \mathfrak{m}$, then $J$ is radical and $V(J)$ is the closure of $V(I) \cap X_0$, $V(I) = V(J)$, and because they are both radical, $I = J$. □

Cor. (4.2.6.6). Being Jacobson is a local property, and quotient of Jacobson ring is Jacobson, and maximal ideals of $R_f$ are maximal in $R$. (Immediate from (4.2.6.5) (3.8.3.22) and (3.8.3.23)).

Prop. (4.2.6.7). If a Jacobson ring $A$ has f.m. maximal ideals, then it is the product of its localizations at maximal primes and $\dim A = 0$.

Proof: Any prime ideal $p$ is a finite intersection of maximal ideals, so it equals one of them, so $\dim A = 0$. Now $A/I = \oplus A/\mathfrak{m}_i$ by Chinese remainder theorem, so $\text{Spec} A/I$ is discrete with $n$ pts, so by (4.1.7.8) there are $n$ idempotents $e_i$ that $e_i \equiv \delta_{ij} \mod \mathfrak{m}_j$, $\sum e_i = 1$. Thus $R = \prod Re_i$. And $Re_i$ is just the localization at a maximal prime. □
Lemma (4.2.6.8). If \( R \) is a Jacobson domain and \( R \subset K \) where \( K \) is a field, and \( K \) is f.g. over \( R \), then \( R \) is a field and \( K/R \) is a finite field extension.

**Proof:** By induction, it suffices to consider the monogenic case \( A = R[a] \). So \( a \) is algebraic over quotient field of \( R \) because \( A \) is a field. Let \( \sum r_it^i \) be a polynomial satisfied by \( a \), and let \( \mathfrak{m} \) be a maximal ideal of \( R \) that \( r_n \notin R \)(exists because \( \text{rad } R = 0 \)). Then Nakayama says \( \mathfrak{m}A \notin A \). Then \( \mathfrak{m} = 0 \) because \( A \) is a field, hence \( R \) is a field. \( \square \)

Lemma (4.2.6.9). Let \( R \subset A \) be commutative domains s.t. \( A \) is f.g. over \( R \), then \( \text{rad } A = 0 \) if \( \text{rad } R = 0 \).

**Proof:** By induction, it suffices to consider the case \( A = R[a] \). If \( a \) is transcendental over quotient field of \( R \), then we finish by (2.4.2.12). Now assume \( a \) is algebraic over quotient field of \( R \), let \( \sum s_it^i, \sum t_it^i \) be the polynomials satisfied by \( a, b \) of minimal degrees, then \( s_0 = -\sum_{i=1}^{m} s_ib^i \neq 0 \in \text{rad } A \), and \( r_ns_0 \neq 0 \).

From the fact \( \text{rad } R = 0 \), we can find a maximal ideal \( \mathfrak{m} \) that \( r_ns_0 \notin \mathfrak{m} \). Then Nakayama says \( \mathfrak{m} \cdot S^{-1}A \notin S^{-1}A \).

In particular, \( \mathfrak{N} \notin A \). Choose a maximal ideal of \( A \) containing \( mA \), then it cannot contain \( s_0 \), contradicting \( s_0 \in \text{rad } A \). \( \square \)

**Prop. (4.2.6.10)** [Generalized Nullstellensatz]. If \( R \) is Jacobson and \( S \) is a finitely generated \( R \)-algebra, then:

- \( S \) is Jacobson.
- The maximal ideal of \( S \) intersect with \( R \) a maximal ideal, and the quotient ring extension is finite, (in particular algebraic).

In particular, a f.g. algebra over a ring of dimension 0, (e.g. Artinian ring or field) is Jacobson.

**Proof:** To show \( S \) is Jacobson, consider for any prime \( p \subset A \), \( A/p \) is a f.g. domain over \( R/p \cap R \). Because \( R \) is Jacobson, \( \text{rad}(R/p \cap R) = 0 \), so \( \text{rad}(A/p) = 0 \), by (4.2.6.9). And this shows \( A \) is Jacobson.

If \( \mathfrak{m} \) is maximal in \( S \), then \( R/\mathfrak{m} \cap R \rightarrow S/\mathfrak{m} \) satisfies the condition of (4.2.6.8), by (4.2.6.6), so the first two assertions are proved. \( \square \)

**Cor. (4.2.6.11).** If \( R \) is Jacobson and \( S \in \mathcal{CAlg}_{fg}(R) \) is reduced, then \( \cap_{\mathfrak{m} \subset R} \text{maximal } \mathfrak{m}S = 0 \).

**Proof:** This is because
\[
\cap_{\mathfrak{m} \subset R} \text{maximal } \mathfrak{m}S \subset \cap_{\mathfrak{M} \subset S} \text{maximal } (\mathfrak{M} \cap R)S \subset \cap_{\mathfrak{M} \subset S} \text{maximal } \mathfrak{M} = 0.
\]

**Zariski Pairs**

**Def. (4.2.6.12).** A pair \((A, I)\) is called a **Zariski pair** iff \( I \) is contained in the Jacobson radical of \( A \).

**Prop. (4.2.6.13).** If \((A, I)\) is a Zariski pair, then the map \( A \rightarrow A/I \) induces a bijection between the idempotents.

**Proof:** idempotents are determined by the maximal ideals that it vanishes (4.1.7.6), and \( A \rightarrow A/I \) induces a bijection on the maximal ideals. \( \square \)
7 Dedekind Domain

References are

Def. (4.2.7.1) [Dedekind Domain]. A Dedekind domain is an integrally closed Noetherian domain of dimension 1. A UFD is a Dedekind domain by (4.3.5.2).

Prop. (4.2.7.2) [Characterizing]. For a domain R, the following are equivalent:
1. R is a Dedekind domain.
2. R is Noetherian and each \( R_\mathfrak{m} \) is DVR for any maximal ideal \( \mathfrak{m} \).
3. each ideal of \( R \) can be written as a product of prime ideals uniquely.

Proof: \( 1 \iff 2 \) as normal is a stalkwise and (4.3.5.20).

\( 3 \rightarrow 2 \): If 3 is true, then \( \mathfrak{p} \neq \mathfrak{p}^2 \) for each prime \( \mathfrak{p} \), so choose \( x \in \mathfrak{p} - \mathfrak{p}^2 \), then for each \( y \in \mathfrak{p} \), \( (x, y) = \prod p_i \), then exactly one \( p_i \) (may assume \( p_1 \)) is contained in \( \mathfrak{p} \), so \( (x, y)\mathfrak{R}_p = p_1\mathfrak{R}_p \). Now in fact \( (x)\mathfrak{R}_p = p_1\mathfrak{R}_p \), because \( (x, y^2)\mathfrak{R}_p \) is also a prime, so \( y = ax + by^2 \) in \( \mathfrak{R}_p \), \( (1 - by)y = ax \in (x)\mathfrak{R}_p \) is a prime, so \( y \in (x)\mathfrak{R}_p \). This is for all \( y \in \mathfrak{p} \), so \( (x)\mathfrak{R}_p = p_1\mathfrak{R}_p \).

Now if \( (x) = p_1 \cdots p_r \), then \( p_1\mathfrak{R}_p = \mathfrak{p}\mathfrak{R}_p \), so \( p_1 = p \), and \( p \) is f.g. by the lemma (4.2.7.3) below. \( \mathfrak{p} \) is arbitrary, so \( R \) is Noetherian and \( R_\mathfrak{m} \) is DVR for \( \mathfrak{m} \) maximal, by (4.3.5.20).

\( 1 \rightarrow 3 \): if 1 is true, then any ideal is a unique intersection of primary ideals, and primary ideals are their radical are different, so they are coprime (4.1.1.7), so this is in fact a unique decomposition into products of primary ideals. And any primary ideal is a power of its radical, because this is the case after localization.

\[ \square \]

Lemma (4.2.7.3). \( I, J \) be ideals in a ring \( A \) and \(IJ = (f)\) where \( f \) is a non-zero-divisor, then \( I, J \) are f.g. and finitely locally free of rank 1 as \( A \)-modules.

Proof: The second assertion implies the first, by (4.3.1.7). \( f = \sum x_iy_i \), and \( x_iy_i = a_if \), so \( \sum a_i = 1 \) as \( f \) is non-zero-divisor. Now we show \( I_{a_i} \) as \( J_{a_i} \) is free of rank 1. Now after localization, \( f = xy \), so \( x, y \) are non zero divisors. Now if \( x' \in I \), then \( x'y = af = axy \) for some \( a \), so \( x' = ax \).

\[ \square \]

Fractional Ideals

Def. (4.2.7.4) [Fractional Ideals]. For \( A \) an integral domain and \( K \) its quotient field, then an \( A \)-submodule \( M \) of \( K \) is called a fractional ideal if \( xM \subset A \) for some \( x \neq 0 \).

Every f.g. submodule in \( K \) is a fractional ideal, and if \( A \) is Noetherian, then the converse is true, because it is of the form \( x^{-1}a \).

Prop. (4.2.7.5). An \( A \)-submodule \( M \) of \( K \) is called an invertible ideal if there is a submodule \( N \) that \( MN = A \). It follows that \( M, N \) are f.g., because there are \( \sum x_iy_i = 1 \), so \( M \) is generated by \( x_i \) and \( N \) is generated by \( y_i \).

Prop. (4.2.7.6). Invertibility is a stalkwise property.

Proof: Notice \( (A : M)_p = (A_p : M_p) \), and \( M \) is invertible iff \( M(A : M) = A \). Then use the fact isomorphism is stalkwise (4.1.4.2).

Prop. (4.2.7.7). A local domain is a DVR iff every non-zero fractional ideal of \( A \) is invertible.
Proof: If is a DVR, let \( m = (x) \), for any fractional ideal \( M < A = (x^r) \), then \( M = (x^{r-s}) \), where \( v(y) = s \). Conversely, if every non-zero fractional ideal of \( A \) is invertible, then they are all f.g. (4.3.5.20). If this is not true, choose a maximal element \( a \) in the set of ideals that is not a power of \( (x) \) (by Noetherian), then \( m^{-1}a \subset A = (x^r) \), then \( m^{-1}a = m^k \) for some \( k \), so \( a = m^{k+1} \), contradiction. □

Cor.(4.2.7.8) [Dedekind Domain Fractional Ideals are Invertible]. An integral domain is a Dedekind domain iff every non-zero fractional ideal is invertible.

Proof: Immediate from the proposition and (4.2.7.2). □

Def.(4.2.7.9) [Class Group]. Let \( \mathcal{O} \) be a Dedekind domain, we denote \( \text{Cl}(\mathcal{O}) \) the Abelian group of fractional ideals of \( \mathcal{O} \) modulo principal fractional ideals, called the class group of \( \mathcal{O} \).

Prop.(4.2.7.10) [Localizations of Dedekind Domains]. Let \((\mathcal{O}, F)\) be a Dedekind domain and \( S \subset \text{Spec} \mathcal{O} \) be a finite subset of maximal ideals of \( \mathcal{O} \), let \( \mathcal{O}_S \) denote the localization of \( \mathcal{O} \) at all such \( p_i \). Then there is an exact sequence of Abelian groups:

\[
1 \to \mathcal{O}^* \to \mathcal{O}_S^* \to \bigoplus_{p \in S} F^*/\mathcal{O}_p^* \to \text{Cl}(\mathcal{O}) \to \text{Cl}(\mathcal{O}_S) \to 1.
\]

Proof: The only non-trivial map is the map \( \bigoplus_{p \in S} F^*/\mathcal{O}_p^* \to \text{Cl}(\mathcal{O}) \) given by \( (\pi_p) \) mapsto \( \prod_{x \in S} p^{v_x(a_x)} \). □

Extensions of Dedekind Domains

References are [Neu99] Chap1.8..

Prop. (4.2.7.11) [Krull-Akizuki]. If \( A \) is a Noetherian domain of dimension 1 with fraction field \( K \) and \( L/K \) is a finite field extension, then the integral closure \( B \) of \( A \) in \( L \) is a Dedekind domain with fraction field \( L \), and \( \text{Spec} B \to \text{Spec} A \) is surjective, and have finite fibers and induces finite residue field extension.

Proof: Cf.[Sta]09IG or [Neu99]P77. □

Cor. (4.2.7.12). The integral closure of a Dedekind domain in a finite extension fields of its quotient fields is again a Dedekind domain.

Def.(4.2.7.13) [Situation]. Let \( \mathcal{O}_K \) be a Dedekind domain with quotient field \( K \), \( L/K \) a finite field extension, and \( \mathcal{O}_L \) the integral closure of \( \mathcal{O}_K \) in \( L \), which is also a Dedekind domain by (4.2.7.11).

Def.(4.2.7.14) [Conductors]. Let \( R \subset S \subset \text{Ring} \) the conductor of \( R \) in \( S \) is defined to

\[
c = \{ \alpha \in R | \alpha S \subset R \}.
\]

And if \((R, K)\) is an integral domain, the conductor of \( R \) is defined to be the conductor of \( R \) in the integral closure of \( R \) w.r.t. \( K \).

Prop. (4.2.7.15). Let \( R \) be a Noetherian integral domain with integral closure \( S \), then the conductor of \( R \) in \( S \) is nonzero iff \( S \) is f.g. as a \( R \)-module.
Proof: This follows from (4.2.7.4). □

Def. (4.2.7.16) [Conductors of an Element]. In situation (4.2.7.13) and \( \alpha \in \mathcal{O}_L \), then the conductor of \( \alpha \) w.r.t \( K \) is the conductor of \( \mathcal{O}_K[\alpha] \) in \( \mathcal{O}_L \), denoted by \( \mathfrak{d}(\alpha) \). It is non-zero by (4.2.7.4) as \( \mathcal{O}_L \) is f.g. over \( \mathcal{O}_K[\alpha] \).

Prop. (4.2.7.17) [Inertia and Ramification]. Situation as in (4.2.7.13), let \( p \) be a maximal prime of \( \mathcal{O}_K \), then \( p\mathcal{O}_L \cap \mathcal{O}_L \) by (4.2.1.5). Let \( p\mathcal{O} = \prod_i \mathfrak{P}_i^{e_i} \) be a decomposition. Denote \( e_i \) the ramification degree of \( \mathfrak{P}_i \) over \( p \), and \( f_i = [\mathcal{O}_L/\mathfrak{P}_i : \mathcal{O}_K/p] \) the inertia degree of \( \mathfrak{P}_i \) over \( p \).

Prop. (4.2.7.18) [Fundamental Identity]. Situation as in (4.2.7.13), if \( \mathcal{O}_L \) is a finite \( \mathcal{O}_K \)-module, then for any \( p = \prod_i \mathfrak{P}_i^{e_i} \),
\[
\sum e_if_i = [L : K].
\]

In particular, this applies to the case that \( L/K \) is separable.

Proof: By hypothesis, \( \mathcal{O}_{L,p} \) is a finite \( \mathcal{O}_Kp \)-module of rank \( [L : K] \), thus \( \mathcal{O}_L/p \) is an \( \mathcal{O}_K/p\mathcal{O}_L \)-module of rank \( n \). Notice there is an isomorphism \( \mathcal{O}_L/p\mathcal{O}_L \cong \prod_i \mathcal{O}_L/\mathfrak{P}_i^{e_i} \), thus
\[
[L : K] = \sum_i \dim_{\mathcal{O}_L/p} \mathcal{O}_L/\mathfrak{P}_i^{e_i} = \sum_i e_if_i.
\]

If \( L/K \) is separable, let \( \{\alpha_1, \ldots, \alpha_n\} \) be a basis of \( L/K \) with \( \alpha_i \in \mathcal{O}_K \), then any \( \alpha = a_1\alpha_1 + \ldots + a_n\alpha_n \in \mathcal{O}_L \) satisfies the following equations
\[
\text{tr}_{L/K}(\alpha_i \alpha) = \sum_j \text{tr}_{L/K}(\alpha_i \alpha_j) a_j
\]
for any \( i \). Notice \( \text{tr}(\alpha_i \alpha) \in \mathcal{O}_K \), so \( da \in \mathcal{O}_K \) by linear algebra, where \( d = \det(\text{tr}_{L/K}(\alpha_i \alpha_j)) \neq 0 \) by (2.2.5.34). So \( \mathcal{O}_L \subset d^{-1}(\alpha_1\mathcal{O}_K + \ldots + \alpha_n\mathcal{O}_K) \), so it is a finite \( \mathcal{O}_K \)-module, as \( \mathcal{O}_K \) is Noetherian. □

Thm. (4.2.7.19) [Dedekind-Kummer]. Situation as in (4.2.7.13), suppose \( L = K(\theta) \), where \( \theta \in \mathcal{O}_L \) has minimal polynomials \( p(X) \in \mathcal{O}_K[X] \)(such a \( \theta \) exists if \( L/K \) is separable, by (2.2.5.20)). Let \( \mathfrak{d} \) be the conductor of \( \theta \), then for any prime ideal \( p \) of \( \mathcal{O}_K \) prime to \( \mathfrak{d} \), let
\[
\mathfrak{p}(X) = \prod_i \mathfrak{p}_i(X)^{e_i}
\]
be the decomposition of \( \mathfrak{p}(X) \) into irreducible factors in \( \mathcal{O}_K/p[X] \), where \( \mathfrak{p}_i(X) \in \mathcal{O}_K[X] \) are monic polynomials, then
\begin{itemize}
\item \( \mathfrak{P}_i = p\mathcal{O} + p_i(\theta)\mathcal{O}_L \) are different primes ideals in \( \mathcal{O}_L \).
\item \( p\mathcal{O}_L = \prod_i \mathfrak{P}_i^{e_i} \).
\item The inertia degree \( f_i \) equals \( \text{deg}(\mathfrak{p}_i(X)) \).
\end{itemize}


Def. (4.2.7.20) [Ramification Notations]. Situation as in (4.2.7.17), let \( p\mathcal{O} = \prod_i \mathfrak{P}_i^{e_i} \), then
\begin{itemize}
\item splits completely in \( L \) if \( r = [L : K] \).
\item \( p \) is non-split in \( L \) if \( r = 1 \).
\end{itemize}
• $\mathfrak{P}_i$ is **unramified** over $\mathfrak{p}$ if $e_i = 1$ and the residue fields extension $(O_L/\mathfrak{P}_i)/(O_K/\mathfrak{p})$ is separable.

• $\mathfrak{P}_i$ is **ramified over** $\mathfrak{p}$ if it is not unramified over $\mathfrak{p}$.

• $\mathfrak{P}_i$ is **totally ramified** over $\mathfrak{p}$ if it is ramified over $\mathfrak{p}$ and $f_i = 1$.

• $\mathfrak{p}$ is called **unramified in** $L$ if all $\mathfrak{P}_i$ are unramified over $\mathfrak{p}$.

• $L/K$ is called a **unramified extension** if all primes of $O_K$ are unramified.

**Prop.(4.2.7.21)** [Almost Every Prime is Unramified]. Situation as in $(4.2.7.19)$, then a.e. prime $\mathfrak{p}$ of $O_K$ is unramified in $L$, by $(4.2.7.35)$.

**Prop.(4.2.7.22)**. Situation as in $(4.2.7.13)$, $O_L \otimes_{O_K} O_K, \mathfrak{p} = \prod_i O_L, \mathfrak{P}_i$.

*Proof:* Cf.[MIT notes, 11.7].

**Prop.(4.2.7.23)**. If a prime $\mathfrak{p}$ splits completely in two separable extension $LM$ of $K$, then it also splits completely in the composite $LM$.

*Proof:* We use the language of valuation. The extension of a valuation $v$ of $K$ corresponds to the set of equivalent classes of algebra map from $L$ to $K_v$ module conjugacy over $K_v$. So We only need to show that two different maps of $LM$ are not conjugate over $K_v$. But the restrict of them to $L$ or $M$ is different, thus not conjugate over $K_v$ by the assumption.

**Cor.(4.2.7.24)**. A prime splits completely in a separable extension $L$ if it splits completely in the Galois closure $N$ of $L$.

*Proof:* This is because the Galois closure is the composite of the conjugates of $L$.

But it also can be proven directly : Set $H = \text{Gal}(N/L), \mathcal{P}$ a prime of $N$ over $\mathfrak{p}$, then

$$H \backslash G/G_\mathcal{P} \rightarrow \{\text{Primes of } L \text{ over } \mathfrak{p}\}, \quad H \sigma G_\mathcal{P} \mapsto \sigma \mathcal{P} \cap L$$

is a bijection. So it splits completely in $L$ $\iff$ $G_\mathcal{P}$ is trivial $\iff$ it splits completely in $N$ by counting numbers.

**Differents and Discriminants**

**Def.(4.2.7.25)** [Differents]. Let $L/K$ be a finite separable field extension with separable residue field extension, and $O_K$ is a Dedekind domain with integral closure $O_L$ in $L$, there is a **trace form** on $L$: $(x, y) \rightarrow \text{tr}(xy)$, which is non-degenerate.

We define the **dual module** for a fractional ideal $I$ as $I^\vee = \{x \in L | \text{tr}(xI) \in O_K\}$. This is truly a fractional ideal because if $\alpha_i \in O_L$ is a basis of $L/K$, and let $d = \text{det}(\text{tr}(\alpha_i \alpha_j))$, then for any $a \in I \cap O_L$, $ad \cdot I^\vee \in O_L$, because if $x = \sum x_i \alpha_i \in I^\vee$, then $\sum ax_i \text{tr}(\alpha_i \alpha_j) = \text{tr}(x\alpha_j) \in O_K$, so solve the equation shows $dax_i \in O_K$.

The **different** of $K/L$ is defined to be $\mathcal{D}_{L/K} = ((O_L)^\vee)^{-1}$.

**Prop.(4.2.7.26)** [Properties of Differents]. Different is compatible with composition, localization w.r.t. a prime ideal and completion.


**Cor.(4.2.7.27)**. $\mathcal{D}_{L/K} = \prod \mathcal{D}_{L_{\overline{\mathfrak{p}}}/K_{\overline{\mathfrak{p}}}}$. 
Prop. (4.2.7.28). If $\mathcal{O}_L = \mathcal{O}_K[\alpha]$, then $\mathfrak{D}_{L/K} = (f'(\alpha))$, where $f(X) = \text{Irr}(\alpha, K; X)$.

Proof: By (2.2.5.30), if $f(X)/(X - \alpha) = \beta_0 + \beta_1X + \ldots + \beta_{n-1}X^{n-1}$, then $\mathcal{O}_L^\gamma = f'(\alpha)^{-1}(\beta_0, \ldots, \beta_{n-1})$. Now the result follows if $(\beta_0, \ldots, \beta_{n-1}) = \mathcal{O}_L$, which is easy to see if we write $\beta_i$ as polynomials of $\alpha$. □

Cor. (4.2.7.29). If $L/K$ is a finite separable extension of local fields, then

$$v_L(\mathfrak{D}_{L/K}) = \sum_{\sigma \in G, \sigma \neq 1} i_{L/K}(\sigma) = \int_{-1}^{\infty} |G(L/K)| - 1 dt.$$

Notation as in (12.2.2.27).

Prop. (4.2.7.30) [Different as Annihilator of Kähler Differential]. The different $\mathfrak{D}_{L/K}$ is the annihilator of $\Omega_{\mathcal{O}_L/\mathcal{O}_K}$.

Proof: It suffices to show the exact sequence

$$0 \rightarrow \mathfrak{D}_{L/K} \rightarrow \mathcal{O}_L \rightarrow \Omega_{\mathcal{O}_L/\mathcal{O}_K},$$

but because exactness is stalkwise (4.1.4.2), we can localized at a maximal ideal, then by (12.2.2.2), $\mathcal{O}_L = \mathcal{O}_K[x]$ is monogenous, thus $\Omega_{\mathcal{O}_L/\mathcal{O}_K}$ is cyclic, and the annihilator of $dx$ is $f'(x)$. So by (4.2.7.28) we are done. □

Prop. (4.2.7.31) [Ramification and Different]. A prime ideal $\mathfrak{p}$ of $L$ is ramified over $K$ iff $\mathfrak{p} | \mathfrak{D}_{L/K}$.

Let $e$ be the ramification of $\mathfrak{p}$, then the power $s$ of $\mathfrak{p}$ in $\mathfrak{D}_{L/K}$ is

$$s = e - 1 \quad \mathfrak{p} \text{ tamely ramified}$$

$$e \leq s \leq e - 1 + v_{\mathfrak{p}}(e) \quad \mathfrak{p} \text{ wildly ramified}.$$


Def. (4.2.7.32) [Discriminants]. Let the situation the same as in (4.2.7.25), the discriminant of $L/K$ $\delta_{L/K}$ is defined to be the set of discriminants $d(\alpha_1, \ldots, \alpha_n)(2.2.5.33)$ where $\alpha_i$ is a basis of $L/K$ that $\alpha_i \in \mathcal{O}_L$.

Because $d(\alpha_1, \ldots, \alpha_n) \subset \mathcal{O}_K$ and $\text{tr}_{L/K}$ is $\mathcal{O}_K$-linear, $\delta_{L/K}$ is an ideal of $\mathcal{O}_K$.

Prop. (4.2.7.33) [Differents and Discriminants].

$$\delta_{L/K} = N_{L/K} \mathfrak{D}_{L/K}.$$


Cor. (4.2.7.34) [Compositions and Discriminants]. For a tower of fields $K \subset L \subset M$, we have

$$\delta_{M/K} = \delta_{L/K}^{[M:L]} N_{L/K}(\delta_{M/L}).$$

Proof: Apply $N_{M/K} = N_{L/K} N_{M/L}$ to the equation $\mathfrak{D}_{M/K} = \mathfrak{D}_{M/L} \mathfrak{D}_{L/K}(4.2.7.26)$, we get

$$\delta_{M/K} = N_{L/K}(\delta_{M/L}) N_{L/K}(\mathfrak{D}_{L/K}^{[M:L]}) = N_{L/K}(\delta_{M/L}) \delta_{L/K}^{[M:L]}.$$
Cor. (4.2.7.35) [Ramification and Discriminant]. Let $L/K$ be a separable finite field extension, then a prime ideal $p$ of $K$ ramifies in $L$ iff $p | d_{L/K}$.

In particular, only f.m. primes are ramified in $L/K$, and the extension is unramified iff $d_{L/K} = 1$.

Proof: This follows from (4.2.7.31) and (4.2.7.33).

Cor. (4.2.7.36). $d_{L/K} = \prod \mathcal{P} d_{L_{\mathcal{P}}/K_{\mathcal{P}}}$.

Proof: This follows from (4.2.7.27) and (4.2.7.33).

Orders


Def. (4.2.7.37) [Orders]. An order is a Noetherian integral domain $O$ of dimension 1 whose conductor (4.2.7.14) is non-zero, or equivalently its integral closure in fraction field is finite over $O$ by (4.2.7.15). A Dedekind domain is an order.

Def. (4.2.7.38). If $A$ is Noetherian domain with fraction field $K$ and $L$ is a f.d. $K$-algebra, then an $A$-order is an $A$-lattice (12.2.4.17) in $L$ that is also a ring.

Prop. (4.2.7.39). Situation as in (4.2.7.13), if $L/K$ is separable, then a subring $O$ of $L$ is an $A$-order iff it is an order with integral closure $O_L$.

In particular, if $F$ is a number field, then the orders of $F$ are exactly subrings of $O_F$ that contains a basis of $F$.

Proof: If $O$ is an $A$-order, then every element of $O$ is integral over $A$, by acting on $O$. $O_K$ is contained in $O$, and $O \otimes_{O_K} K = L$, so the fraction field of $O$ is $L$. Thus the integral closure of $O$ in $L$ is $O_L$. Then $\dim O = 1$ as $\dim O_L = 1$ (4.2.4.14), and it is Noetherian because it is f.g. over $A$ (4.1.1.40). And $O_L$ is finite over $O_K$ by (4.2.7.18), thus is also f.g. over $O$. Thus $O$ is an order.

If $O$ is an order with integral closure $O_L$, then it is f.g. over $O_K$ as it is contained in the f.g. $O_K$-module $O_L$. And it contains a $K$-basis of $L$ because $L = K \mathcal{O}_L$ and $a \mathcal{O}_L \subset O$ for some $a \in O^\times$ because $O$ is an order. Thus $O$ is an $A$-lattice in $L$ that is a ring, so it is an $A$-order.

For the last assertion, notice that if it contains a basis of $F$ and is contained in $O_F$, then it must be a $\mathbb{Z}$-lattice of $F$, as $O_F$ is free because it is finite over $\mathbb{Z}$ (4.2.7.18).

Prop. (4.2.7.40). Let $F \in \mathbb{NField}$ and $\Lambda$ is a $\mathbb{Z}$-lattice in $F$, then the ring of multipliers

$$O = \{ \alpha \in O_F | \alpha \Lambda \subset \Lambda \}$$

is an order in $F$.

Proof: $O$ contains $(d)$ for some $d \in \mathbb{Z}_+$, because for any $\alpha \in O_F$, $\alpha \Lambda \subset F = \Lambda \otimes \mathbb{Q}$, so for some $d_\alpha \in \mathbb{Z}_+$, $d_\alpha \Lambda \subset \Lambda$.

Thus $O$ contains a basis of $F$. And $O$ is contained in $O_F$: if $\alpha \Lambda \subset \Lambda$, then $\alpha$ satisfies the equation of its characteristic polynomial, which has coefficients in $\mathbb{Z}$. So $\alpha \in O_F$. Thus $O$ is an order, by (4.2.7.39).
4.3 Commutative Algebra III

1 Projective

References are [Projective Modules], [Sta] and [Vak17].

Def.(4.3.1.1)[Projective Modules]. A module $P$ over a ring $R$ is called projective iff $\text{Hom}(P, -)$ is exact, or equivalent, for any surjective map of modules $F \to Q \to 0$, $\text{Hom}(P, F) \to \text{Hom}(P, Q)$ is surjective.

Prop.(4.3.1.2). Localization and tensor product preserves projective because they are left adjoints. And when tensoring f.f. map, then the converse is also true (4.4.2.1).

Prop.(4.3.1.3). A module over a ring is projective iff it is a direct summand of a free module, in particular, it is flat. Moreover, there is a free module $Q$ that $P \oplus Q = F$ free.

Proof: For the second assertion, we can choose an arbitrary $Q$ that $P \oplus Q$ free, and see $\bigoplus_{N}(P \oplus Q)$ is free. □

Lemma(4.3.1.4). A projective module is a direct sum of countably generated projective modules.

Proof: This follows from (2.2.4.28). □

Prop.(4.3.1.5)[Projective over Local Ring]. A projective module $P$ over a local ring $R$ or a PID is free.

Proof: Local ring case: By (4.3.1.4) and (2.2.4.29), it suffices to show that any element $x$ of $P$ is contained in a free direct summand of $P$. Because $P$ is projective, it is a direct summand of a free module $F, F = P \oplus Q$. Let $B$ be a basis of $F$ that the number of basis element in the expression of $x$ is minimal. Let $x = \sum a_i e_i$. Then no $a_i$ is contained in the ideal generated by other $a_j$, otherwise we can choose another basis to show this is minimal. Let $e_i = y_i + c_i$ be decompositions into $P$ and $Q$ components, and write $y_i = \sum a_{ij} e_i + t_i$, where $t_i$ is combination of elements in $B$ other than $e_i$. Now it suffices to show $\det(a_{ij})$ is invertible, because in this way $\{y_i\} \cup (B \setminus \{x_1\})$ is a basis of $F$ and $x = \sum a_i y_i$ because $x \in P$. And $N = \span\{y_i\}$ is a summand of $P$ because $N \subset P$ and both $N, P$ are summands of $F$.

To show $\det(a_{ij})$ is invertible, notice that by plugging $y_i = \sum b_{ij} e_j + t_i$ into $\sum a_i e_i = \sum a_i y_i$ shows $a_j = \sum a_{ij}$, thus by the argument before, $a_{ij}$ are non-invertible for $i \neq j$ and $1 - a_i$ is non-invertible, so $a_{ii}$ is invertible. Because $R$ is a local ring, we can easily see $\det(a_{ij})$ is invertible. □

PID case: directly from (2.2.4.21).

Prop.(4.3.1.6). If $R$ is a ring and $I$ is nilpotent ideal and $\overline{P}$ is a projective $R/I$-module, then there exists a projective $R$-module $P$ that $P/IP \cong \overline{P}$.

Proof: Cf. [Sta] P07LV. □

Finite Projective Modules

Prop.(4.3.1.7)[Finite Projective Modules]. Let $M$ be a $R$-module, the following are equivalent:

1. $M$ is finite projective.
2. $M$ is f.p. and flat.
3. $M$ is f.p. and all its localizations at (maximal)primes are free.
4. $M$ is finite locally free.
5. $M$ is finite and locally free.
6. $M$ is finite and all its localizations at primes are free and the function $p \rightarrow \dim_{k(p)} M \otimes_R k(p)$ is a locally constant function on $\text{Spec } R$.

Proof: 1 $\rightarrow$ 2: $M \otimes K = R^n$ for some $K$ and $n$, so $K$ is finite and $M = R^n/K$ is f.p. And $M$ is flat because it is a summand of $R^n(4.4.1.4)$.

2 $\rightarrow$ 4: For any prime $p$, choose a basis for the $k(p)$-vector space $M \otimes k(p)$, then by Nakayama, their inverse image generate $M$ for some $g \in p(2.2.4.8)$, and the kernel $K$ of this generation is finite because $M_g$ is f.p. And $K \otimes k(p) = 0$ by the flatness of $M_g$. Then by Nakayama again there is a $g' \in p$ that $M_{gg'} = 0(2.2.4.8)$.

4 $\rightarrow$ 3: Because f.p. is local(4.1.4.4).
3 $\rightarrow$ 2: Because flatness is trivial.
4 $\rightarrow$ 5: Because finite is local(4.1.4.4).
5 $\rightarrow$ 4, 4 $\rightarrow$ 6: Trivial.
6 $\rightarrow$ 4: Cf.[Sta]00NX.

2 + 3 + 4 + 5 + 6 $\rightarrow$ 1: Cf.[Sta]00NX.

Consider the stalk, it is all free by $(4.3.1.2)$ and $(4.3.1.5)$, thus by $(5.5.1.38)$, it is locally free. □

Cor.(4.3.1.8)[Partially Stalkwise]. If $P$ is a f.p., then finite projectiveness is a stalkwise property for $P$.

Cor.(4.3.1.9)[Projective and Flat]. A finite module over a Noetherian ring is projective iff it is flat.

Cor.(4.3.1.10). If $M$ is finite projective, then the canonical map $\text{Hom}(M, N) \otimes L \rightarrow \text{Hom}(M, N \otimes L)$ is an isomorphism.

Proof: By proposition above $M$ is f.p. and finite locally free, so by(4.3.7.7) and tensor commutes with localization, we can check locally, where $M$ is finite free so the isomorphism is obvious. □

Def.(4.3.1.11)[Characteristic Polynomials for Finite Projective Modules]. Let $M$ be a finite projective module over a ring $A$. then we can define a characteristic polynomial in $A[X]$ for any map of $A$-modules $M \rightarrow M$: if $M$ is free, then this map is defined as usual. In general, we can find an open covering $\text{Spec } A_{f_i}$ of $\text{Spec } A$ that $M_{f_i}$ is free over $A_{f_i}$. Thus we can define the characteristic polynomial locally and glue them together to get a characteristic polynomial in $A[X]$.

In particular, we can also define trace and norm of a $A$-module map $M \rightarrow M$. And when $B$ is a locally free $A$-algebra, then there are trace and norm maps $\text{tr}: B \rightarrow A$ and $\text{Nm}: B \rightarrow A$.

Prop.(4.3.1.12). Let $R$ be a ring and $I$ be a locally nilpotent ideal. If $\mathcal{P}$ is a finite projective module over $R/I$, then there exists a finite projective $R$-module $P$ that $P/IP \cong \mathcal{P}$.

Proof: Cf.[Sta]0D47. □

Prop.(4.3.1.13). Let $M$ be a $R$ module and $I$ a nilpotent ideal of $R$. If $M/IM$ is a projective $R/I$-module and $M$ is flat over $R$, then $M$ is a projective $R$-module.

Proof: Cf.[Sta]05CG. □
Thm. (4.3.1.14)[Serre-Suslin]. Every finite projective module over the polynomial ring \( k[x_1, \ldots, x_n] \) is free.

Proof: Cf.[Lan05]P850. □

Duality of Projective Modules

Prop.(4.3.1.15)[Basis Criterion of Projectiveness]. An \( A \)-module \( P \) is projective iff there are elements \( x_i \) in \( P \) and \( f_i \) in \( P^* \) that for any \( x \), \( f_i(x) = 0 \) a.e. \( i \), and \( \sum f_i(x)x_i = x \). Moreover, \( P \) is finite projective iff there are f.m. of them.

Proof: If \( P \) is projective, as a summand of a free module, then we can choose the coordinates of the inclusion map as \( f_i \), and choose the image of the quotient map of the coordinate as \( x_i \). The converse is verbatim. □

Cor.(4.3.1.16)[Finite Projective Duality]. If \( P \) is projective, then \( P \to P^{**} \) is injective, and if \( P \) is finite projective, then it is an isomorphism.

Proof: If \( f(x) = 0 \) for all \( f \in P^* \), then the proposition says \( x = 0 \). And if \( P \) is finite projective, it can be seen \( x_i, f_i \) forms a "basis" of \( P^* \)(finiteness used), so \( f_i \) generate \( P^* \), and similarly \( x_i \) generate \( P^* \), so \( P \to P^{**} \) is surjective. □

Cor.(4.3.1.17). If \( P \) is projective over \( R \), then \( P^* \neq 0 \).

Cor.(4.3.1.18). In the meanwhile of the proof, we already get: if \( P \) is finite projective, then \( P^* \) is finite projective, by(4.3.1.15).

Cor.(4.3.1.19). If \( P \) is finite projective, the the map \( P \otimes M \to \text{Hom}(P^*, M) \) is an isomorphism.

Proof: In(4.3.1.10), let \( N = R \) and let \( M = P^* \), then use the fact \( P \cong P^{**} \). □

Thm. (4.3.1.20)[Quillen-Suslin]. For \( k \in \text{Field} \), any finite projective module over \( k[X_1, \ldots, X_k] \) is free. (Highly nontrivial).

Proof: Cf.[Lan05]P850. □

Prop.(4.3.1.21). \( \prod Z \) is not free over \( Z \), by(2.1.4.4).

2 Injective

Prop.(4.3.2.1)[Baer’s Criterion]. A right \( R \)-module \( I \) is injective iff for every right ideal \( J \) of \( R \), every map \( J \to I \) can be extended to a map \( R \to I \). (Directly from (3.3.5.6)).

Cor.(4.3.2.2). A module over a PID is injective iff it is divisible.

Cor.(4.3.2.3). \( A \) is injective iff \( \text{Ext}^1(R/I, A) = 0 \) for every ideal \( I \) of \( R \).

Cor.(4.3.2.4)[Rank]. Let \( M \) a finite projective \( R \)-module, then \( M \) is said to have rank \( n \) if \( M/\mathfrak{m}M \) is of rank \( n \) over the field \( R/\mathfrak{m} \) for any arbitrary maximal ideal \( \mathfrak{m} \) of \( R \).

Prop.(4.3.2.5). The category of \( R \)-mod has enough injectives by(3.3.2.27), and it has enough projectives trivially.
Prop. (4.3.2.6). If $I$ is an injective $A$-module, then for any ideal $\alpha$ of $A$, $\Gamma_\alpha(I) = \{m|\alpha^nm = 0\}$ for some $n$ is injective.

Proof: Use Baer criterion, for any ideal $b$ of $A$, it is f.g. so there is a $n$ that $\phi(\alpha^n b) = 0$, and Artin-Rees tells us that $\phi(\alpha^N \cap b) = 0$ for some $N$. So we have an extension of $\phi$ over $b/b \cap \alpha^N$ to $A/\alpha^N \rightarrow I$, and this obviously factor through $\Gamma_\alpha(I)$, so it is done. □

Prop. (4.3.2.7). For an injective module $A$-module $I$, $I \rightarrow I$ if is surjective.

Proof: we have the sheaf of modules $\tilde{I}$ is flabby (5.7.1.4), thus the map to the stalk is surjective. □

Pontryagin Duality

Basic references are [Weibel Homological Algebra].

Def. (4.3.2.8). The Pontryagin dual $M^\vee$ of a left $R$-module $M$ is the right $R$-module $\text{Hom}_{ab}(M, Q/\mathbb{Z})$, where $(fr)(b) = f(rb)$.

It is easily verified that if $A \neq 0$, then $A^\vee \neq 0$, and $Q/\mathbb{Z}$ is an injective $\mathbb{Z}$-module, thus the Pontryagin dual is faithfully exact.

Prop. (4.3.2.9). $M$ is flat $R$-module iff $M^\vee$ is an injective right $R$-module (Because $\text{Hom}(-, Q/\mathbb{Z})$ is exact).

3 Homological Dimension

Def. (4.3.3.1). For a $R$-mod $A$, the projective dimension $\text{pd}(A)$ is the minimal length of a projective resolution of $A$. The injective dimension $\text{id}(A)$ is the minimal length of a injective resolution of $A$. The flat dimension $\text{fd}(A)$ is the minimal length of a flat resolution of $A$.

Prop. (4.3.3.2). If $R$ is Noetherian, then $\text{fd}(A) = \text{pd}(A)$ for every f.g. module $A$.

Proof: Use (4.3.3.3), we see that if we choose a syzygy and look at the $n$-th term, then it is f.p and flat, so we have it is projective by (4.4.1.14). □

Lemma (4.3.3.3)[pd]. If $\text{Ext}^{d+1}(A, B) = 0$ for every $B$, then for every resolution

$$0 \rightarrow M \rightarrow P_{d-1} \rightarrow \ldots, P_1 \rightarrow P_0 \rightarrow A \rightarrow 0$$

where $P_k$ is projective, then $M$ is projective. Hence we have $\text{pd}(A) \leq d$. (Use dimension shifting, the following two are the same).

Lemma (4.3.3.4)[id]. If $\text{Ext}^{d+1}(A, B) = 0$ for every $A$, then for every resolution

$$0 \rightarrow B \rightarrow P_0 \rightarrow \ldots, P_{n-1} \rightarrow M \rightarrow 0$$

where $P_k$ is injectives, then $M$ is injective. Hence we have $\text{id}(B) \leq d$

Lemma (4.3.3.5)[fd]. If $\text{Tor}^{d+1}(A, B) = 0$ for every $B$, then for every resolution

$$0 \rightarrow M \rightarrow F_{d-1} \rightarrow \ldots, F_1 \rightarrow F_0 \rightarrow A \rightarrow 0$$

where $F_k$ is flat, then $M$ is flat. Hence we have $\text{fd}(A) \leq d$
Prop. (4.3.3.6) [Global Dimension Theorem]. The following are the same for any ring $R$ and called the left global dimension of $R$:
1. $\sup \{id(B)\}$
2. $\sup \{pd(A)\}$
3. $\sup \{pd(R/I)\}$
4. $\sup \{d : \Ext_R^d(A, B) \neq 0 \text{ for some module } A, B\}$.

Proof: This follows from (4.3.3.3), (4.3.3.4) and (4.3.2.3). □

Prop. (4.3.3.7). A $\mathbb{Z}$ has global dimension 1 because injective is equivalent to divisible, and this shows that a quotient of an injective is injective.

Prop. (4.3.3.8) [Tor Dimension Theorem]. The following are the same for any ring $R$ and called the Tor dimension of $R$:
1. $\sup \{fd(A)\}$ for $A$ a left module.
2. $\sup \{fd(B)\}$ for $B$ a right module.
3. $\sup \{pd(R/I)\}$ for $I$ a left ideal.
4. $\sup \{pd(R/J)\}$ for $J$ a right ideal.
5. $\sup \{d : \Tor_R^d(A, B) \neq 0 \text{ for some module } A, B\}$.

Proof: This follows from (4.3.3.5) applied to $R$ and $R^{op}$ and also (4.4.1.2). □

Prop. (4.3.3.9) [Change of Rings]. Let $S \to R$ be a ring map, let $A \in \text{Mod}_R$, then we have $pd_S(A) \leq pd_R(A) + pd_S(R)$.

Proof: Use the Cartan-Eilenberg resolution and the total complex has length $pd_R(A) + pd_S(R)$. □

4 Depth

Regular sequences

Def. (4.3.4.1) [Regular Sequences]. If $R$ is a commutative ring and $M$ is an $R$-module, then a sequence $(f_1, \ldots, f_n)$ of elements of $R$ is called a $M$-regular sequence if $f_k$ is a nonzero-divisor of $M/(f_1, \ldots, f_{k-1})$ and $M/(f_1, \ldots, f_n) \neq 0$. If $M = R$, then it is simply called a regular sequence.

Prop. (4.3.4.2). If $R$ is a local ring, $M$ a finite $R$-module, and $(f_1, \ldots, f_n)$ is a $M$-regular sequence, then a permutation of this sequence is also an $M$-regular sequence.

Proof: By transposition of adjacent indices, we can assume $n = 2$. Then $x$ is a non-zero-divisor, and $x \in \mathfrak{m}$, so Now $(x, y)$ is an $M$-regular sequence iff $M \otimes_R \mathfrak{m} R/x$ is discrete and $M \otimes_R \mathfrak{m} R/y$ is discrete. Then it suffices to prove $y$ is injective on $M$: If $ym = 0$, then $m = xm'$ for some $m'$, because $y$ is injective on $M/x$, and then $ym' = 0$ also because $x$ is injective on $M$. Then $x$ is surjective on $\ker(y)$, thus $\ker(y) = 0$ by Nakayama. □

Prop. (4.3.4.3). Let $R$ be a ring and $0 \to M_1 \to M_2 \to M_3 \to 0$ be an exact sequence of $R$-modules. Then if a sequence $(f_1, \ldots, f_r) \in R^r$ is both $M_1$-regular and $M_3$-regular, then it is also $M_2$-regular.
4.3. COMMUTATIVE ALGEBRA III 407

**Proof:** Use the snake lemma, \( \ker(f_1|_M) = 0 \), and \( 0 \to M_1/fM_1 \to M_2/fM_2 \to M_3/fM_3 \to 0 \), then use induction. \( \square \)

**Prop.(4.3.4.4).** For any integers \( e_i \geq 1 \), \( (f_1, \ldots, f_n) \) is a \( M \)-regular iff \( (f_1^{e_1}, \ldots, f_n^{e_n}) \) is \( M \)-regular.

**Proof:** Use induction on \( n \). \( n = 1 \) is trivial, and it suffices to show that \( (f_1, f_2, \ldots, f_n) \) is \( M \)-regular. Then we use induction on \( e \): There is an exact sequence \( 0 \to M/f_1M \to M/f_1^2M \to M/f^{e-1}M \to 0 \), so by (4.3.4.3), if \( (f_1, \ldots, f_n) \) is \( M \)-regular, then \( (f_1, f_2, \ldots, f_n) \) is \( M \)-regular. Conversely, if \( (f_1, f_2, \ldots, f_n) \) is \( M \)-regular, then \( f_2 \) is injective on \( M/f_1^2M \), so also injective on \( M/f_1M \), thus injective on \( M/f^{e-1}M \) by induction hypothesis, and also there is a further exact sequence \( 0 \to M/(f_1, f_2)M \to M/(f_1^2, f_2)M \to M/(f^{e-1}, f_2)M \to 0 \), so we can consider \( f_3 \), and then so on, thus show \( (f_1, f_2, \ldots, f_n) \) is \( M \)-regular. \( \square \)

**Prop.(4.3.4.5).** Let \( R \) be a ring, then the following are equivalent:

- any permutation of \( (f_1, \ldots, f_r) \) is a regular sequence.
- Any subsequence of \( (f_1, \ldots, f_r) \) is a regular sequence.
- \( (f_1X_1, \ldots, f_rX_r) \) is a regular sequence of \( R[X] \).

**Proof:** 1 \( \to \) 2: Trivial. 2 \( \to \) 1: Use induction on \( r \): If \( r = 2 \) and \( (x, y) \) is regular, we have \( M \otimes_R R/x, M \otimes_R R/y \) are both discrete, and \( M \otimes_R R/x \otimes_R R/y \) is also discrete, thus \( M \otimes_R R/x \otimes_R R/y \) is also discrete and \( (y, x) \) is regular. For \( r > 2 \), it suffices to show \( f_{\sigma(r)} \) is regular in \( M/(f_{\sigma(1)}, \ldots, f_{\sigma(r-1)}) \). If \( \sigma(r) = r \), then we are done, otherwise, \( f_r \) and \( f_{\sigma(r)} \) are both injective on \( M/(f_1, \ldots, f_{\sigma(r)}, \ldots, f_{r-1}) \) by induction hypothesis, and \( (f_{\sigma(r)}, f_r) \) is a regular sequence for this ring, then so is \( (f_{\sigma(r)}, f_r) \) by the \( r = 2 \) case, thus we are done.

3 \( \iff \) 2: Notice as a \( R \)-module, \( R[X_1, \ldots, X_r]/(f_1X_1, \ldots, f_iX_i) \) is a direct sum of the modules \( R/I(EX_1^{i_1} \ldots X_r^{i_r}) \), where \( I_E \) is generated by those \( f_j \) that \( j \leq i \) and \( e_j > 0 \). Then \( f_{i+1}X_{i+1} \) is injective on this iff \( f_{i+1} \) is injective on \( R/I_e \) for \( E \). Then it is clear that this is equivalent to 2. \( \square \)

**Def.(4.3.4.6) [Quasi-Regular Sequence].** Let \( f_1, \ldots, f_c \in R \) and \( J = (f_1, \ldots, f_c) \), let \( M \) be a \( R \)-module, then there is a canonical map \( M/JM \otimes_R R/J[X_1, \ldots, X_c] \to \otimes_{n \geq 0} J^n M/J^{n+1} M \). Then \( (f_1, \ldots, f_c) \) is called \( M \)-quasi-regular sequence iff this is an isomorphism.

**Depth**

**Prop.(4.3.4.7) [Rees].** For a f.g. module \( M \) and \( IM \neq M \),

\[
\text{depth}_I(M) = \min \{ i | \text{Ext}_A^i(A/I, M) \neq 0 \} = \min \{ i | \text{Ext}_A^i(N, M) \neq 0 \}
\]

where \( \text{depth}_I(M) \) is the length of the maximal \( M \)-regular sequence in \( I \), \( N \) is a finite \( A \)-module with \( \text{Supp}(N) \subset V(I) \).

**Proof:** If No elements of \( I \) are \( M \)-regular, then \( i \subseteq \cup \text{Ass}(M) \) thus in one of them, so \( \text{Hom}_A(k, M_p) = 0 \), and we have \( N_p/PN_p = N \otimes_A k_p \) nonzero by Nakayama, thus \( \text{Hom}_k(N \otimes_A k_p, k_p) \neq 0 \), thus \( \text{Hom}_A(N_p, M_p) = (\text{Hom}_A(N, M))_p \neq 0 \), so \( \text{Ext}_A^0(N, M) \neq 0 \). Other dimensions follows by induction, consider the cokernel of \( M \xrightarrow{\alpha} M \).

Conversely, use induction, then we have an injection \( \text{Ext}_A^i(N, M) \xrightarrow{a_i} \text{Ext}_A^i(N, M) \) for \( i < n \). And the condition shows that \( I \subset \sqrt{\text{Ann}(M)} \), so \( a_i N = 0 \), thus the result. \( \square \)
Cor. (4.3.4.8). Two maximal regular sequence in a f.g. module have the same length.

Cor. (4.3.4.9). For a module \( M \) over a Noetherian ring \( A \), we know \( \Gamma_I(M) = \{ m | I^nm = 0 \text{ for some } n \} \), and \( H^i_I \) is its right derived functor, then we have \( \text{depth}_I(M) \geq n \iff H^i_I(M) = 0 \) for \( i < n \). (Because derived functor commutes with colimits, consider \( N = A/I^k \)).

Lemma (4.3.4.10) [Ischebeck]. For a Noetherian local ring \( A \), if \( M, N \) are finite modules, then we have \( \text{Ext}^i_A(N, M) = 0 \) for \( i < \text{depth} \). (Proof: □)

Prop. (4.3.4.11). Let \( A \) be a local ring and \( M \) is finite \( A \)-module, then \( \text{depth}(M) \leq \text{dim} A/P \leq \text{dim} M \) for every \( P \in \text{Ass}(M) \). (Because \( \text{Hom}(A/P, M) \neq 0 \).)

Proof: □

Prop. (4.3.4.12) [Auslander-Buchsbaum Formula]. For a local ring \( R \), if \( M \) is a finitely generated \( R \)-module, then \( \text{pd}(M) < \infty \), then we have \( \text{depth}(R) = \text{depth}(M) + \text{pd}(M) \).

Proof: Cf. [Weibel P109]. □

### Cohen-Macaulay

Def. (4.3.4.13) [Cohen-Macaulay Modules]. For a Noetherian local, a f.g. \( A \)-module \( M \) is called **Cohen-Macaulay** if \( \text{depth}(M) = \text{dim} M \). In view of (4.3.4.11), this is equivalent to \( \text{depth}(M) = \text{dim} A/P \) for all \( P \in \text{Ass}(M) \). A **Cohen-Macaulay ring** is a ring \( A \) that is Cohen-Macaulay over itself.

A localization of a C.M local ring is C.M, so we call a ring **Cohen-Macaulay** if all its localization at primes are C.M.

Prop. (4.3.4.14) [Gorenstein Ring]. A ring \( R \) is called **Gorenstein** iff \( \text{id}_R < \infty \). A Gorenstein local ring is C.M. In this case, \( \text{depth}(R) = \text{id}_R = \text{dim} R \), and \( \text{Ext}^q_R(R/m, R) \neq 0 \iff q = \text{dim} R \).

Proof: Cf. [Weibel P107]. □

Prop. (4.3.4.15). A ring is C.M. iff for all ideals, the associated primes of \( A/I \) all have the same height as \( I \), i.e. unmixed.

Proof: □

Prop. (4.3.4.16). If a local ring is C.M. and \( I = (x_1, \ldots, x_r) \) is a regular sequence, then \( (x_1, \ldots, x_r) \) is .

Proof: \(?\) Isn’t this always true? □

Prop. (4.3.4.17). Let \( A \) be a Noetherian local ring and \( M \) a f.g. module, if a set of elements \( (x_1, \ldots, x_r) \) forms a regular sequence for \( M \), then \( \text{dim} M/(x_1, \ldots, x_r) = \text{dim} M - r \). The converse is also true when \( A \) is C.M. If this is the case, then \( A/(x_1, \ldots, x_r) \) is also C.M.

Proof: By (4.2.2.19), we have \(<\), for the converse, \( \text{Supp}(M/fM) = \text{Supp}(M) \cap \text{Supp}(A/fA) = \text{Supp}(M) \cap V(f) \), and when \( f \) is \( M \)-regular, \( V(f) \) doesn’t contain any \( \text{Ass}(M) \) thus no minimal elements of \( \text{Supp}(M) \), so \( \text{dim}(M/fM) < \text{dim} M \), thus we have \( >\).

When \( A \) is C.M.: \(?\) □
Prop. (4.3.4.18). Let \( R \to S \) be a local homomorphism of Noetherian local rings, if \( R \) is C.M. and \( S \) is finite flat over \( R \) or \( S \) is flat over \( R \) and \( \dim S \leq \dim R \), then \( S \) is C.M., and \( \dim R = \dim S \).

Proof: Cf.[Sta]00R5.

5 Normal & Regular Rings

Normal Ring

Def. (4.3.5.1) [Normal Rings]. A normal domain is a domain and is integrally closed in its fraction field.

A domain is normal iff all its localizations are normal, so we can define a normal ring to be a ring that all its stalks are normal local rings. In particular, a normal ring is reduced.

Proof: The localization of a normal domain is normal, and the converse follows from \( A = \cap A_m \) (4.1.1.33).

Prop. (4.3.5.2) [UFD is Normal]. A UFD is a normal domain.

Proof: If \( A \) is a UFD, then for any \( x \in \text{Frac}(A) \) integral over \( A \), checking the primes dividing the coefficients, we see \( x \in A \).

Prop. (4.3.5.3). A normal ring \( R \) is integrally closed in its ring of fractions.

Proof: Let \( x \in \text{Q}(R) \) be integral over \( R \), and \( I = \{ f \in R | fx \in R \} \), then for any prime \( p \) of \( R \), \( R \to R_p \) is injective, so \( R_p \subset \text{Frac}(R) \otimes_R R_p \), and \( x \otimes 1 \) is integral over \( R_p \), thus \( x \otimes 1 \in R_p \), which means \( x \otimes 1 = 1 \otimes a/f \) for some \( a, f \in R, f \notin p \). This means \( f'(fx - a) = 0 \in Q(R) \) for some \( f' \notin p \), so \( f f' \in I \), and thus \( I \) is not contained in any prime ideal, so \( I = 1 \) and \( x \in R \).

Prop. (4.3.5.4). Let \( R \) be a reduced ring with f.m. minimal prime ideals, then the following are equivalent:

- \( R \) is a normal ring.
- \( R \) is integrally closed in its ring of fractions.
- \( R \) is a finite product of normal domains.

In particular, a Noetherian normal domain is a finite product of normal domains (4.1.1.46).

Proof: 3 \( \to 1 \) is trivial, 1 \( \to 2 \) is by (4.3.5.3), for 2 \( \to 3 \): let \( p_i \) be the minimal prime ideals of \( R \), then \( \text{Frac}(R) = \prod_{i=1}^{r} Q_{p_i} \) (4.1.7.22), with each \( Q_{p_i} \) field because \( R \) is reduced. Denote the idempotents of \( \text{Frac}(R) \) by \( e_i \). Then \( e_i \) is integral thus in \( R \). These idempotents make \( R \) into a product of domains, which are just \( R/p_i \), because the kernel of the map \( R \to R_{p_i} \) is \( p_i \). Now \( R \) is integrally closed in \( \text{Frac}(R) \) implies each \( R/p_i \) is integrally closed in \( R_{p_i} \), thus \( R \) is a finite product of normal domains.

Def. (4.3.5.5) [Normalization]. The normalization of an integral domain is the alg.closure of it in its quotient field. It commutes with localization.

Def. (4.3.5.6) [Completely Normal Domains]. A domain is called completely normal iff all almost normal elements are in \( A \), i.e. \( \{ u | \exists a, au^n \in A \forall n \} \in A \). For Noetherian ring, completely normal is equivalent to normal.

Proof: Cf.[Sta]00GX.
Prop. (4.3.5.7). A is a normal domain, then so does $A[X]$. If $A$ is Noetherian normal domain, then so does $A[[X]]$.

Proof: Cf.[Sta]030A, 0BI0.

Prop. (4.3.5.8). Direct limits of normal rings are normal.

Proof: Let $p$ be an ideal of $R = \lim\rightarrow R_i$, $p_i = p \cap R_i$, then $R_p = \lim\rightarrow (R_i)_{p_i}$, so it suffices to prove for normal domains, the rest is easy.

Prop. (4.3.5.9) [Closure in Separable Extension]. Let $R$ be a Noetherian normal domain with field of fraction $K$ and $L/K$ is a finite separable field extension, then the integral closure $S$ of $R$ in $L$ is finite over $R$.

Proof: Let $\text{tr} : L \times L \rightarrow K : (x, y) \mapsto \text{tr}(xy)$ be the trace pairing, then as $L/K$ is finite separable, this is non-degenerate. Now if $x \in L$ is integral over $R$, then $\text{tr}(x) \in R$. So if $x_1, \ldots, x_n$ are integral and form a basis of $L$ over $K$, then $M = \{y \in L | \langle x_i, y \rangle \in R\}$ is an $R$-module and $M \cong R^n$, and $S \subset M$, so $S$ is finite over $R$ as $R$ is Noetherian.

Prop. (4.3.5.10) [Field Extension]. Let $A$ be a $K$-algebra, and $L/K$ is a field extension, then if $A_L$ is a normal integral domain, so is $A$. And the converse is also true if $L/K$ is separable.

Prop. (4.3.5.11) [Algebraic Hartogs’s Lemma]. Principal ideals in a Noetherian normal domain is unmixed and $A = \bigcap_{ht} p=1 A_p$.

Proof: Cf.[Matsumura P124], [Rising Sea, P320], [Sta]031T.

Prop. (4.3.5.12) [Krull]. If $A$ is a normal domain with fraction field $K$, $L$ is a normal extension field of $K$ and $B$ is the integral closure of $A$ in $L$ that $A \subset B$ is integral, then any two prime ideals of $B$ lying over a prime in $A$ are conjugate by an action of $G_{L/K}$.

Proof: Firstly if $G_{L/K}$ is finite, and $P, P'$ be primes of $B$ that $P \cap A = P' \cap A$. Let $P_i = \sigma_i(P)$. If $P' \neq P_i$ for any $i$, then $P' \nsubseteq P_i$ for any $i$ by(4.2.1.5), so there is some $x \in P'$ not in any of $P_i$. Now let $y = (\prod_i \sigma_i(x))^q$ where $q = 1$ if char$(K) = 0$ and $q = p^r$ for $r$ large if char$(K) = p$, then $y \in K$ thus in $A$ because $A$ is normal, and it is not in $P$ by hypothesis. But $y \in P' \cap A = P \cap A$, contradiction.

For the infinite field extension case, let $K'$ be the fixed field of $G_{L/K}$ so that $K'/K$ is purely inseparable, then there is clearly exactly one prime of $K'$ over any prime of $A$. So we can assume $L/K$ is Galois, then use profinite group technique to find a $\sigma \in G_{L/K}$ that $\sigma(P) = P'$. 

Prop. (4.3.5.13) [Hironaka]. Let $A$ be a local Noetherian domain that is a localization of an algebra of f.t. over a field $k$. Let $t \in A$ that

- $tA$ has only on eminimal associated prime ideal $p$.
- $t$ generate the maximal ideal of $A_p$.
- $A/p$ is normal.

Then $p = tA$ and $A$ is normal.

Proof: Cf.[Hartshorne P264].

Prop. (4.3.5.14) [Quadratic Extension is Normal]. If $A$ is a UFD that $2$ is invertible in $A$ and $f \in A \setminus A^2$, then $A[Z]/(Z^2 - f)$ is integral and normal.
Proof: It is integral by (2.2.3.13). To show it is normal, assume $F(T) \in B[T]$ that $f(\alpha) = 0$, where $\alpha \in K(B) \backslash B$, then by replacing $F$ by $\overline{F}$, we can assume $F(T) \in A[T]$. We can assume $\alpha \notin K(A)$, thus $\alpha = g+hZ$, then the minimal polynomial of $\alpha$ is $Q(T) = T^2 - 2gT + (g^2 - h^2 f) \in K(A)[T]$. Then $F(T) = P(T)Q(T)$ in $K(A)[T]$. By Gauss’s lemma, $2g, g^2 - h^2 f \in A$, so $g, f \in A$ by hypothesis. □

Cor. (4.3.5.15). If $k$ is a field of characteristic $\neq 2$, then
- $k[x_1, \ldots, x_n]/(x_1^2 + \ldots + x_m^2)$ is integral normal for $n \geq m \geq 3$.
- $k[x, y, z, w]/(wz - xy)$ is normal. (Diagonalize).

Prop. (4.3.5.16). $\mathbb{Z}[\sqrt{n}]$ is integrally closed for $n \equiv 3 \mod 4$, and $\mathbb{Z}[1+\sqrt{n}]$ is integrally closed for $n \equiv 1 \mod 4$, by (12.2.4.14).

Regular Ring

Def. (4.3.5.17) [Regular Rings]. A Noetherian local ring $(A, \mathfrak{m}, k)$ is called regular local if it $\dim A = \dim k[\mathfrak{m}/\mathfrak{m}^2]$. This is equivalent to $\text{rank}_k \mathfrak{m}/\mathfrak{m}^2 \leq \dim A$, or $A \cong k[X_1, \ldots, X_d]$ by (4.2.2.19).

Localization of a regular local ring at primes are regular local, Cf.[Sta]0AFS. Hence we define a regular ring to be a Noetherian ring that all its localization at primes are regular local.

Proof: Cf. [Matsumura P139]. □

Prop. (4.3.5.18). If $A$ is regular, then $A[X_1, \ldots, X_n]$ is regular, and $A[[X_1, \ldots, X_n]]$ is regular.

Proof: Cf. [Matsumura P176]. □

Prop. (4.3.5.19)[Auslander-Buchsbaum]. A regular local ring is UFD. In particular it is a normal domain. Thus a regular ring is normal and thus reduced (4.3.5.1).

Proof: Cf. [Matsumura P142],[Weibel P106]. □

Cor. (4.3.5.20). A regular local ring of dimension 0 is a field, and a regular local ring of dimension 1 is a DVR.

Prop. (4.3.5.21). A regular local ring is Gorenstein hence C.M..

Proof: □

Prop. (4.3.5.22)[Regular Local Ring and Regular Sequences]. Let $(R, \mathfrak{m})$ be a regular local ring of dimension $d$,
- If $x_1, \ldots, x_c$ be a sequence that maps to linearly independent elements in $\mathfrak{m}/\mathfrak{m}^2$, then $(x_1, \ldots, x_c)$ is a regular sequence, and $R/(x_1, \ldots, x_c)$ is a regular local ring of dimension $d-c$.
- If $I \subset \mathfrak{m}$ and $R/I$ is a regular local ring, then $I = (x_1, \ldots, x_c)$ where $(x_1, \ldots, x_c)$ is a regular sequence.
- If $(x_1, \ldots, x_c)$ is a regular sequence in $\mathfrak{m}$ and $R/(x_1, \ldots, x_c)$ is a regular local ring, then $R$ is also a regular local ring.
Proof: 1: We can complete it to a sequence \((x_1, \ldots, x_d)\) that \((x_1, \ldots, x_d)\) generate \(m/m^2\), then by Nakayama \((x_1, \ldots, x_d) = m\). Now by Krull’s height theorem (4.2.4.18), \(R/(x_1)\) has dimension \(\geq d - 1\) and \((x_2, \ldots, x_d)\) generate the maximal ideal, so \(R/(x_1)\) is a regular local ring by definition. Now \(x_1 \neq 0\) because \(R\) is a domain (4.3.5.19), thus we can use induction to show \((x_1, \ldots, x_c)\) is a regular sequence.

2: Let \(\dim(R/I) = d - c\), then the hypothesis shows \((I + m^2)/m^2 \cong I/mI\) has rank \(c\), thus we can choose \((x_1, \ldots, x_c) \in I\) that generate \(I/mI\). Thus by Nakayama \(I = (x_1, \ldots, x_c)\), and \((x_1, \ldots, x_c)\) is a regular sequence by item 1.

3: By induction, it suffices to prove the \(c = 1\) case, then any lift of \(x_1\) together with \(d - 1\) generator of the maximal ideal of \(R/m\) is a set of generator of \(m\).

\[\square\]

Cor. (4.3.5.23). A regular local ring is C.M., by item 1.

Prop. (4.3.5.24). If a quotient of a Noetherian local ring by a non-zerodivisor is regular, then it is itself regular.

Prop. (4.3.5.25) [Serre]. A Noetherian local ring \(A\) is regular iff the global dimension of \(A\) is finite.

\[\text{Proof:} \quad \text{Cf.} \{\text{Mat P139}\}. \quad \square\]

Prop. (4.3.5.26). For \(A\) a regular local ring and \(M\) a f.g. \(A\)-module,

\[pd(M) + \text{depth } M = \dim A.\]

\[\text{Cf.} \{\text{Hartshorne P237}\}.\]

Cor. (4.3.5.27). For a f.g. module \(M\) over a regular local ring \(A\), \(pd(M) \leq n\) iff \(\text{Ext}^i(M, A) = 0\) for all \(i > n\).

\[\text{Proof:} \quad \text{This is because we can use dimension shifting to show} \ \text{Ext}^i(M, N) = 0 \quad \text{for all } N \text{ f.g., then (4.3.3.3) says that} \ pd(M) \leq n. \quad \square\]

Prop. (4.3.5.28) [Regular and Regular Sequence]. Let

Prop. (4.3.5.29). Let \(R \to S\) be a flat local homomorphism of Noetherian local rings that \(R\) is regular, \(S/mS\) is regular, then \(S\) is also regular.

\[\text{Proof:} \quad \text{Cf.} \{\text{Sta}031E\}. \quad \square\]

Serre Conditions \(R_k \& S_k\)

Def. (4.3.5.30). A ring is called \(R_k\) if for all prime \(p\) of height \(\leq k\), \(A_p\) is regular.

A ring is called \(S_k\) if \(\text{depth}(A_p) \geq \min(k, \text{ht}(p))\) for all prime \(p\).

A module \(M\) is called \(S_k\) if \(\text{depth}(M_p) \geq \min(k, \dim \text{Supp } M_p)\) for all prime \(p\).

Prop. (4.3.5.31).

- \(M\) is \(S_1\) if \(M\) has no associated embedded primes. Cf. [Sta]031Q.
- A Noetherian ring is reduced iff it is \(R_0\) and \(S_1\). Cf. [Sta]031R.
- (Serre Criterion) A Noetherian ring is normal iff it is \(R_1\) and \(S_2\). Cf. [Sta]031S.
- A ring is C.M. iff it is \(S_N\).
4.3. COMMUTATIVE ALGEBRA III

Proof: □

Cor. (4.3.5.32) [Regular and Normal]. A regular ring is normal, and normal ring is regular in codimension 1.

Proof: By (4.3.5.31), it suffices to prove that a regular ring satisfies R1 and S2. A regular ring is C.M. (4.3.5.21) so it is S2 by (4.3.5.31), it is R1 by (4.3.5.17) □

Cor. (4.3.5.33) [Normal and Regular Dimension 1]. A Noetherian local ring of dim 1 is normal iff it is regular. i.e. integral domain and integrally closed iff maximal ideal is principal.

6 Geometric Properties

Def. (4.3.6.1).
- A k-algebra S is called geometrically reduced/integral/connected... over a field k iff for any field extension k'/k, Spec S_{k'} is reduced/integral/connected...
- A Noetherian k-algebra S is called geometrically regular iff for any f.g. field extension K/k, S_{K} is regular (Notice A \otimes k k' is Noetherian (4.1.1.44), so this makes sense).

Prop. (4.3.6.2) [Geometrically reduced]. If S is a k-algebra, the following are equivalent.
1. S is geometrically reduced.
2. S \otimes_k \overline{k} is reduced.
3. S \otimes_k k^{per} is reduced.
4. S \otimes_k k' is reduced for any finite purely inseparable field extension k'/k.
5. S \otimes_k k^{1/p} is reduced.
6. residue fields of S at maximal points are reduced.
7. S \otimes_k R is reduced for every reduced k-algebra R.

Proof: 1 \rightarrow 7: We can assume R is f.g., thus R is contained in a finite product of fields Cf.[Sta]030V?, and then we can assume R is a product of fields, and we are done.
1 \rightarrow 2 \rightarrow 3 \rightarrow 4 is clear. 3 \rightarrow 5 is clear.
4 \rightarrow 1: For any field extension K/k, we can assume WLOG K/k is f.g., thus?
5 \rightarrow 1: ? 6: Cf.[Sta]030V and [Gortz 135]. □

Prop. (4.3.6.3) [Geometrically Irreducible]. Let S be a k-algebra, the following are equivalent:
1. S is geometrically irreducible.
2. For any finite separable field extension k'/k, the spectrum of S_{k'} is irreducible.
3. The spectrum of S_{k^{sep}} is irreducible.
4. The spectrum of S_{k} is irreducible.

Proof: Cf.[Sta]037K.? □

Prop. (4.3.6.4). Let S be a geometrically irreducible k-algebra and R is a k-algebra, then the map

\text{Spec}(R \otimes_k S) \rightarrow \text{Spec} R

induces a bijection on irreducible components.
Proof: Cf.[Sta]037O. □

**Prop.(4.3.6.5)[Geometrically Integral].** Let $S$ be a $k$-algebra, the following are equivalent:
1. $S$ is geometrically integral.
2. For any finite separable field extension $k'/k$, $S_{k'}$ is an integral domain.
3. $S_k$ is an integral domain.
4. $S \otimes_k R$ is an integral domain for any integral domain $R$ over $k$.

Proof: This follows from(4.3.6.3)(4.3.6.2) and(4.3.6.4). □

**Prop.(4.3.6.6).** It suffices to check geometrically regular for $k'/k$ finite purely inseparable.

Proof: Cf.[Sta]0381. □

7 Finitely Presentedness

**Finite Presented Modules**

**Def.(4.3.7.1)[Finitely Presented Modules].** A finitely presented module is a module of the form $R^m/R^n$.

Finite presentation is stable under base change because tensoring is right exact.

**Prop.(4.3.7.2).** Given an exact sequence of $R$-modules $0 \rightarrow M_1 \rightarrow M_2 \rightarrow M_3 \rightarrow 0$,
- If $M_1, M_3$ are f.p., then so does $M_2$.
- If $M_3$ is f.p. and $M_2$ is f.g., then $M_1$ is f.g.
- If $M_2$ is f.p. and $M_1$ is f.g., then $M_3$ is f.p.

Proof: 1: e can find an commutative diagram

$$
\begin{array}{cccc}
0 & \rightarrow & R^m & \rightarrow & R^{m+n} & \rightarrow & R^m & \rightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \\
0 & \rightarrow & M_1 & \rightarrow & M_2 & \rightarrow & M_3 & \rightarrow & 0
\end{array}
$$

and use the snake lemma to see the kernel is f.g..

2: Use the diagram

$$
\begin{array}{cccc}
R^m & \rightarrow & R^n & \rightarrow & M & \rightarrow & 0 \\
\downarrow & & \downarrow & & \downarrow_{id} & & \\
0 & \rightarrow & M_1 & \rightarrow & M_2 & \rightarrow & M_3 & \rightarrow & 0
\end{array}
$$

cokernel of $\alpha$ are all finite, so $M_1$ is finite.

3: Choose a presentation $R^m \rightarrow R^n \rightarrow M_2$ and a surjection $f : R^k \rightarrow M_1$, then we can lift $f$ to $R^k \rightarrow R^m$, and then $M_3$ can be written as a quotient $R^{m+k} \rightarrow R^m \rightarrow M_3$. □

**Cor.(4.3.7.3).** A direct summand of a f.p. module is f.p..

**Prop.(4.3.7.4).** If $R \rightarrow S$ is a f.g. ring map and a $S$-module $M$ is f.p. over $R$, then it is f.p. over $S$.

Proof: Let $S = R[x_1, \ldots, x_n]$, and $M = R[y_1, \ldots, y_m]/(\sum a_{ij}y_j), 1 \leq i \leq t$, then as $M$ is a $S$-module, we let $x_iy_j = \sum a_{ijk}y_k$, and forms a quotient $S^{m+n+t} \rightarrow S^m \rightarrow N \rightarrow 0$, where $S^{m+n+t}$ corresponds to the relations $\sum a_{ij}y_j$ and $x_iy_j - \sum a_{ijk}y_k$. Then there is a surjective $A$-module map $N \rightarrow M$, and we check it is injective: if $z = \sum b_jy_j$ are mapped to 0, where $b_j \in S$, then we can transform $z$ into the shape $\sum c_jy_j$, where $c_j \in R$ by relations $x_iy_j - \sum a_{ijk}y_k$. Thus it is zero by definition.
Prop. (4.3.7.5) [Direct Limits of F.P. Modules]. Any module is a direct limit of f.p. modules. This can be seen by considering all finite submodules and f.m relations between them.

Prop. (4.3.7.6) [Characterizing Finite and F.P. Modules]. Let $N$ be an $R$-module, then

- $N$ is finite $R$-module iff for any filtered colimits $M = \varinjlim M_i$ of $R$-modules, the map $\varinjlim \text{Hom}(N, M_i) \to \text{Hom}(N, \varinjlim M_i)$ is injective.
- $N$ is a f.p. $R$-module iff for any filtered colimits $M = \varinjlim M_i$ of $R$-modules, the map $\varinjlim \text{Hom}(N, M_i) \to \text{Hom}(N, \varinjlim M_i)$ is a bijection.

Proof: \[ \text{If } N \text{ is generated by } x_i \text{ and a map } f : N \to M_i \text{ maps to } 0 \in \text{Hom}(N, \varinjlim M_i), \text{ then there is a } j \text{ that } f : M_j \to M_i \to M_j = 0. \text{ Thus } f = 0. \text{ Conversely, } N \text{ is the sum of its f.g. submodules } N', \text{ thus } N \to \varinjlim N/N_i = 0, \text{ which implies the identity map } N \to N \text{ vanishes for some } N/N' \text{ where } N' \text{ is a finite submodule of } N, \text{ so } N = N' \text{ and } N \text{ is a finite.} \]

2: If $M$ is f.p., we can get the assertion by writing $M$ as a quotient of free modules and use the fact filtered colimit is exact (4.1.4.24). Conversely, write $N$ as a filtered colimits of f.p. modules (4.3.7.5), then $\text{id} : M \to M$ factors through some f.p. module, so it is a direct summand of a f.p. module, thus f.p. by (4.3.7.3). \qed

Cor. (4.3.7.7) [FP and Localization]. For $M$ f.p., $S^{-1} \text{Hom}_R(M, N) = \text{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N)$ for any $R$-module $N$. (Use the presentation and Hom is left exact).

Proof: $\text{Hom}_{S^{-1}R}(S^{-1}M, S^{-1}N) \cong \text{Hom}_R(M, S^{-1}N)$ by duality, and then we can use (4.3.7.6), as localization is a filtered colimit. \qed

Finitely Presented Ring Map

Def. (4.3.7.8) [Finitely Presented Ring Map]. A ring map is called of finite presentation iff it is a quotient of a free algebra by a free algebra.

Prop. (4.3.7.9). Finite presentation is stable under composition (choose a presentation form to see) and base change because tensoring is right exact.

It is local on the source and target by (4.1.4.4).

Prop. (4.3.7.10). For $S$ f.p. over $R$, then the kernel of any surjective ring map $R[X_1, \ldots, R_n] \twoheadrightarrow S$ is f.g.

Proof: Let $S = R[Y_1, \ldots, Y_m]/(f_1, \ldots, f_k)$, then if $\alpha(X_i) \cong g_i(Y)$, then $\alpha : R[X_1, \ldots, R_n] \to R[Y_1, \ldots, X_m, Y_1, \ldots, Y_m](f_1, \ldots, f_k, X_i - g_i).$ And the $Y_i$ are in the image, thus we let $Y_i$ are mapped onto by $h_j(X)$, then $\ker \alpha = (f_i(h_j(X)), X_i - g_i(X)).$ \qed

Prop. (4.3.7.11). If $g \circ f : R \to S' \to S$ is of finite presentation and $f$ is of finite type, then $g$ is of finite presentation.

Proof: Let $S' = R[y_1, \ldots, y_n]$ and $S = R[X_1, \ldots, X_n]/(f_1, \ldots, f_m)$, then let $h_i(X) \cong y_i$ in $S$, then $S = S'[X_1, \ldots, X_n]/(f_1, \ldots, f_m, h_i - y_i).$ \qed

Prop. (4.3.7.12) [Normal Form of F.P.]. If $S$ is f.p. over $R$ that $S$ has a presentation $S = R[X_1, \ldots, X_n]/I$ that $I/I^2$ is free over $S$, then $S$ has a presentation $R[X_1, \ldots, X_m]/(f_1, \ldots, f_c)$ that $(f_1, \ldots, f_c)/(f_1, \ldots, f_c)^2$ is freely generated by $f_1, \ldots, f_c$. 

Proof. Cf. [Sta]07CF.

Prop. (4.3.7.13) [Finite Type Locally of Finite Presentation]. If $R \to S$ is a injective map of f.t. of domains, then there are $f \neq 0 \in R, g \neq 0 \in S$ that $R_f \to S_f g$ is of f.p.

Proof: Use induction on the number of generators of $S/R$. If $S = R[x]$, then $S = R[X]/q$. If $q = 0$, then $S$ is of f.p. If $g = fx^d + a_d x^{d-1} + \ldots + a_0$ be a polynomial of minimal degree in $q$, then $R \to S_f$ is of f.p.

The more generator case can be reduced to the single generator case, because f.p. ring map is stable under composition (4.3.7.9).

Lemma (4.3.7.14) [Filtered Colimits and F.P.]. Let $R \to A$ be a ring map, then the category of f.p. $R$-algebras $A'$ with an $R$-algebra map $A' \to A$ is filtered, and the colimit is just $A$.

Proof: Cf. [0BUF].

8 Nagata & Excellent Rings

Def. (4.3.8.1) [Japanese & Nagata Rings]. Let $R$ be a domain with quotient field $K$, then $R$ is called N-1 iff the integral closure of $R$ in $K$ is a finite $R$-module.

$R$ is called N-2 or Japanese iff for any finite field extension $L/K$, its integral closure in $L$ is a finite $R$-module.

A ring $R$ is called universally Japanese if for any domain $S$ of f.t. over $R$, $S$ is Japanese.

A ring $R$ is called Nagata if it is Noetherian and for any prime $p$, $R/p$ is Japanese.

All these properties are local properties (4.1.4.4). And they are in fact stable under any localizations.

Prop. (4.3.8.2) [Nagata]. Let $R$ be a ring, the following are equivalent:

- $R$ is Nagata,
- any f.g. $R$-algebra is Nagata.
- $R$ is universally Japanese and Noetherian.

Proof: Cf. [Sta]0334.

Prop. (4.3.8.3) [Nagata and Formal Fibers]. Let $(A, m)$ be a Noetherian local ring, then $A$ is Nagata iff the formal fibers of $A$ are geo.reduced.

Proof: Cf. [Sta]0BJ0.

Excellent Rings

Def. (4.3.8.4) [G-Rings]. A G-ring is a Noetherian ring s.t. for any prime $p \subset R$, the map $R_p \to R_p$ is regular.

Def. (4.3.8.5) [Excellent Rings]. A quasi-excellent ring is a ring that is Noetherian, G-ring and J-2. A excellent ring is a quasi-excellent ring that is universally catenary.

Prop. (4.3.8.6). Quasi-excellent rings are Nagata.

Proof: Cf. [Sta]07QV.
Prop. (4.3.8.7) [Examples]. The following rings and f.g. algebras over them are excellent rings:
- fields.
- Noetherian complete local rings
- Dedekind domain with fraction field of characteristic 0.
In particular, ring of integers in all local fields and number fields are excellent.

Proof: Cf.[Sta]0335. □

Cor. (4.3.8.8). The above rings are all Nagata, by (4.3.8.6).

9 Separability

Main references are [Matsumura Ch10], [Weibel Chap P309] and [Sta]10.41, 10.43.

Def. (4.3.9.1) [Separable Algebra]. A f.d semisimple algebra $R$ over a field $k$ is called separable iff for every field extension $K/k$, $R \otimes_k K$ is semisimple.

Def. (4.3.9.2). A field extension $K/k$ is called separably generated iff it $K$ is a separable algebraic extension of a purely transcendental field $L/k$.

A field extension $K/k$ is called separable iff all f.g. subextensions are separably generated.

An algebra $A/k$ is called separable iff $A \otimes_k k'$ is reduce for any $k'/k$ algebraic.

Prop. (4.3.9.3). If $k \subset K$ is a f.g. field extension, then there is a finite purely inseparable field extension $k \subset k'$ that $k' \subset k'K$ is separable.

Proof: □

Prop. (4.3.9.4) [Separable and Geo.Reduced]. Let $K/k$ be a field extension, then $K/k$ is separable iff $K/k$ is geometrically reduced.

Proof: Cf.[Sta]030W. □

Cor. (4.3.9.5). If $K/k$ is a separable field extension and $S$ is a reduced $k$-algebra, then $S \otimes_k K$ is reduced.

Proof: Cf.[Sta]030U. □

Cor. (4.3.9.6). A separably generated field extension is separable.

10 Henselian Ring

Main References are [Sta]Chap10.148.

Def. (4.3.10.1). A local ring $(R, m, k)$ is called Henselian iff for every $f \in R[X]$ and $a_0 \in k$ that $f(a_0) = 0$ and $f'(a_0) \neq 0$, then there is a root $\alpha$ of $f$ lifting $a_0$. It is called strict Henselian if moreover its residue field is separably closed.
**Henselian Pairs**

**Def. (4.3.10.2).** A **Henselian pair** is a pair \((A, I)\) that is Zariski and for any \(f, g\) in \(A[T]\) monic and \(\overline{f} = \overline{g}h \in A/I[T]\) that is coprime and monic, there is a factorization \(f = gh\) lifting the decomposition.

In particular, if \(f\) has a simple root \(\overline{x}\) in \(A/I\), then it has a root \(x \in A\) lifting \(\overline{x}\).

**Prop. (4.3.10.3).** Filtered limits of Henselian pairs is Henselian, this is clear from the definition (4.3.10.2).

**Lemma (4.3.10.4).** If \(A\) is a ring with ideal \(I\), if \(\overline{f} = \overline{g}h\) be a factorization of a polynomial \(f \in A[T]\) in \(A/I[T]\), then there is an étale ring map \(A \to A'\) that \(A/IA \cong A'/IA'\), and a factorization \(f = gh' \in A'[T]\) lifting the factorization.

**Proof:** Cf. [Almost Ring Theory, 5.1.9].

**Prop. (4.3.10.5) [Topological Invariance of Étale Sites].** If \(I\) is locally nilpotent, then \((A, I)\) is Henselian, in particularly \(A_{et} \cong (A/I)_{et}(4.3.10.9)\).

**Proof:** First if \(A \to S\) is étale, then \(A/I \to S/IS\) is étale by base change (4.4.7.5) and the map is essentially surjective by (4.4.7.15). And any map \(B/IB \to B'/IB'\) can be lifted to \(B \to B\) because étale is smooth and use (4.4.5.16). And the lifting is unique, otherwise if \(f, g\) are two lifting, because étale is unramified, so if we choose an idempotent \(e\) generating the kernel of \(B \otimes_A I \to B \to B'\), then \(f \otimes g(e) \in IB'\), which is locally nilpotent, thus \(f \otimes g(e) = 0\), thus \(f = g\).

For then Henselian, \(I\) is clearly contained in the Jacobson radical, and for the decomposition, by (4.3.10.4) these is an étale map \(A \to A'\) that \(A/IA \cong A'/IA'\) that lifts the factorization, but \(A = A'\), by what we have seen above.

**Cor. (4.3.10.6) [Complete Pair is Henselian].** If \((A, I)\) is a pair that \(A\) is \(I\)-adically complete, then \((A, I)\) is Henselian.

**Proof:** \(I\) is in the Jacobson radical because \(1 + I\) consists of units, and by (4.3.10.5) and (4.3.10.4) we can lift the decomposition to \(A/I^n\) inductively. As \(A = \lim A/I^n\), we are done.

**Prop. (4.3.10.7) [Equivalent Definitions of Henselian Pair].** The following are all equivalent to \((A, I)\) being Henselian:
- Given any étale ring map \(A \to A'\), then any \(A' \to A/I\) lifts to an \(A\)-algebra map \(A' \to A\).
- For any finite/integral \(A\)-algebra \(B\), the map \(B \to B/IB\) induces a bijection on idempotents.
- (Gabber) \((A, I)\) is Zariski and every monic polynomial \(f(T) \in A[T]\) of the form \(T^n(T - 1) + a_nT^n + \ldots + a_1T + a_0\) with \(a_i \in I\) has a root \(\alpha \in 1 + I\).

Moreover, root in item 3 is unique.

**Proof:** Cf. [Sta]09XI.

**Cor. (4.3.10.8).** If \((A, I)\) is Henselian and \(A \to B\) is integral, then \((B, IB)\) is also Henselian.

**Prop. (4.3.10.9) [Henselian Lifting].** If \((A, I)\) is a Henselian pair, then there is a natural equivalence of categories: \(A_{et} \cong (A/I)_{et}\).

**Proof:** Cf. [Sta]09ZL.

**Prop. (4.3.10.10).** A Zariski pair \((R, I)\) is Henselian iff the pair \((\mathbb{Z} \oplus I, I)\) is Henselian. In particular, the property of being Henselian only depends on the non-unital ring \(I\).

**Proof:** Cf. [Almost Ring Theory, 5.1.9].
4.4 Commutative Algebra IV

1 Flatness

Def. (4.4.1.1) [Flatness]. A module $M$ over a ring $R$ is called flat if $M \otimes_R - : \text{Mod}_R \rightarrow \text{Mod}_R$ is an exact functor. This is compatible with the definition (5.2.2.15).

Prop. (4.4.1.2). Flatness need only be checked for finite modules, and it is equivalent to $\text{Tor}_1(M, A/I) = 0$ for any $f.g.$ ideal $I$ (i.e., $I \otimes M \rightarrow M$ is injective).

Proof: This is because of (5.3.3.12) and the fact tensor product commutes with colimit. □

Cor. (4.4.1.3). If $0 \rightarrow M' \rightarrow M \rightarrow M'' \rightarrow 0$, then $M'$ and $M''$ flat implies $M$ is flat.

Prop. (4.4.1.4). If $M$ is flat then $\text{Tor}_i^R(M, N) = 0$ for all $i > 0$, because we have: if $0 \rightarrow M_1 \rightarrow M_2 \rightarrow M_3 \rightarrow 0$ with $M_2, M_3$ flat, then $M_1$ is flat (Use 9 entry sequence and the fact that $\text{Tor}$ is symmetric (4.6.2.5)). So $\text{Tor}_{n+1}(M_3, N) = \text{Tor}_n(M_1, N) = 0$ by induction.

And a direct summand of a flat module is flat. Thus we have the class of flat modules is adapted $- \otimes N$ for all $N$ (because free is flat).

Prop. (4.4.1.5) [Faithfully Flatness]. The following are equivalent:

- $M$ is flat and for any $N \neq 0$, $N \otimes_R M \neq 0$.
- $M$ is flat and for any (maximal) prime ideal $\mathfrak{m}$ of $R$, $k(\mathfrak{m}) \otimes_R M \neq 0$. (When $\mathfrak{m}$ is maximal, which means $\mathfrak{m}M \neq M$).

And such a $M$ is called faithfully flat over $R$.

Proof: $1 \rightarrow 2$ is easy. $2 \rightarrow 1$: any nonzero module has a submodule $R/I$, choose a maximal ideal $\mathfrak{m}$ containing $I$, then $(A/I) \otimes_A M \subset N \otimes_A M$ surjects to $k(\mathfrak{m}) \otimes_A M \neq 0$. □

Prop. (4.4.1.6) [Flatness and Base Change].

- (Faithfully) Flatness is stable under base change.

Flatness satisfies f.f. descent (4.4.2.1).

- Flatness is stable under filtered colimit because filtered colimit commutes with tensoring (2.2.4.13) and is exact (4.1.1.24). In particular, $S^{-1}A$ is flat (4.1.1.27).

- Let $S \rightarrow S'$ be a map of $R$-algebras, $M$ is an $S$-module, $M' = M \otimes_S S'$, then if $M$ is flat over $R$, so does $M'$. The converse also holds if $S \rightarrow S'$ is f.f.

- If $R \rightarrow S$, and a $S$-module $M$ is $R$-flat and $S$-f.f., then $R \rightarrow S$ is flat.

Proof:

4: For any injection of $R$-modules $N \rightarrow N'$, use the fact $\text{ker}(N \otimes_R M \rightarrow N' \otimes_R M) \otimes_S S' = \text{ker}(N \otimes_R M' \rightarrow N' \otimes_R M')$.

5: For any injection of $R$-modules $N \rightarrow N'$, use the fact $\text{ker}(N \otimes_R S \rightarrow N' \otimes_R S) \otimes_S M = \text{ker}(N \otimes_R M \rightarrow N' \otimes_R M')$. □

Prop. (4.4.1.7) [Equational Criterion of Flatness]. For a $R$-module $M$, a relation $\sum f_i x_i = 0$ where $f_i \in R, x_i \in M$ are called trivial iff $\overrightarrow{f} = A \overrightarrow{y}$ for some $A \in M_{n \times n}(R), \overrightarrow{y} \in M^n$, and $\overrightarrow{f^t} A = 0$. Then $M$ is flat iff all relations of elements of $M$ is trivial.
Proof: Assume $M$ if flat over $R$, and $\sum f_i x_i = 0$ is a relation in $M$, Let $I = (f_1, \ldots, f_n)$ and let $K = \ker(R^n \to I : (x_i) \mapsto \sum x_i f_i)$, then $\sum f_i \otimes x_i = 0 \in I \otimes_R M$ by flatness, then $\sum e_i \otimes x_i \in K \otimes_R M$. Let $\sum e_i \otimes x_i = \sum k_j \otimes y_j$, and $k_j = \sum_i a_{ij} e_i$, then this is the desired relations.

Conversely, suppose every relation is trivial, and $I$ is an ideal of $R$, let $x = \sum f_i \otimes x_i \subset I \otimes M$ be an element mapping to $0 \in R \otimes M = M$, then $\sum f_i x_i$ is a relation, so it is trivial, and then $x = \sum f_i \otimes x_i = \sum f_i \otimes (a_{ij} y_j) = (\sum (f_i a_{ij}) y_j) = 0$. \hfill \qed

Prop. (4.4.1.8) [Gororov-Lazard]. Any flat $A$-module is isomorphic to a direct limit of finite free modules.

Proof: Cf. [Sta] 058G.

Prop. (4.4.1.9). Flat module is torsion-free.

Proof: If $x \in R$ is a nonzero-divisor, $R \xrightarrow{\cong} R$ is injective, thus $M \xrightarrow{\cong} M$ is also injective. \hfill \qed

Prop. (4.4.1.10) [Flat over Local Rings]. A finite module $M$ over a local ring $A$ is flat iff it is free. In particular, finite modules over a field are all flat.

Proof: Let $A/\mathfrak{m} = k$, choose a $k$-basis $x_i$ of $M/\mathfrak{m}M$, then they generate $M$ by Nakayama. It suffices to prove that $x_i$ are independent over $R$. For this, use equational criterion of flatness (4.4.1.7), we prove that if $x_i$ is independent over $k$, then they are independent over $A$. Use induction, if $x \neq 0$ in $M/\mathfrak{m}$, if $fx = 0$ for some $f \in A$, then $x = \sum a_j y_j$, it $fa_j = 0$, but then some $a_j$ is a unit, so $f = 0$.

If $\sum f_i x_i = 0$, then by hypothesis, $f_i \in \mathfrak{m}$, and there are $y_j$ such that $x_i = \sum a_{ij} y_j$, $\sum f_i a_{ij} = 0$. As $x_n \notin \mathfrak{m}M$, there is a $a_{nj} \notin \mathfrak{m}$, so $f_n = \sum (-a_{ij}/a_{nj}) f_i$. Then $\sum_{i \neq n} f_i(x_i - a_{ij}/a_{nj} x_n) = 0$, but $x_i - a_{ij}/a_{nj} x_n$ is also independent over $k$, so by induction, $f_i = 0$, also does $f_n$, so we are done. \hfill \qed

Prop. (4.4.1.11) [Flat over Bézout Domains]. A module $M$ over a Bézout domain $R$ is flat iff it is torsion-free.

Proof: One direction is clear by (4.4.1.9). If it is torsion-free, we use the equational criterion of flatness (4.4.1.7):

Let $\sum a_i x_i = 0$ where $a_i \in R^*$, $x_i \in M$, then consider $(a_1, \ldots, a_n) = (a)$, thus $a_i = ab_t$ for some $b_t \in R$, and $\sum c_i b_t = 1$ for some $c_i \in R$ as $R$ is a domain. Because $M$ is torsion-free, $\sum a_i x_i = 0$. Notice $\overrightarrow{x} = (1 - \overrightarrow{c} \overrightarrow{b}^t) \overrightarrow{x}$, so we can take $\overrightarrow{y} = \overrightarrow{x}$, $A = 1 - \overrightarrow{c} \overrightarrow{b}^t$. Then $\overrightarrow{b}^t A = \overrightarrow{b}^t - \overrightarrow{b}^t \overrightarrow{c} \overrightarrow{b}^t = 0$. \hfill \qed

Cor. (4.4.1.12) [Flat over Valuation Rings]. A module over a valuation ring is flat iff it is torsion free. In particular, if $(A, \mathfrak{m})$ is a DVR with a uniformizer $t$, then $M \in \text{Mod}_A$ is flat iff $t$ is injective on $M$.

Proof: Because valuation ring is Bézout (10.3.2.8), we can use (4.4.1.11). \hfill \qed

Cor. (4.4.1.13) [Flat Module over a Dedekind Domain]. If $A$ is a Dedekind domain, then an $A$-module is flat iff it is torsion-free.

Proof: Because flatness and torsion-freeness is stalkwise (4.1.4.2), so it suffices to prove for its localization, which is DVR (4.2.7.2), so the result follows from (4.4.1.12). \hfill \qed

Prop. (4.4.1.14) [Finite Flat is Locally Free]. Finitely presented flat module is equivalent to finite projective and equivalent to finite locally free. (Immediate from (4.3.1.7)).
Prop. (4.4.1.15). if $M$ is a flat $R$-module, then $IM \cap JM = (I \cap J)M$ for ideals of $A$.

Proof: Tensoring the exact sequence $0 \to I \cap J \to I \oplus J \to J \cup J \to 0$ with $M$. □

Prop. (4.4.1.16) [Local & Infinitesimal Criterion of Flatness]. Let $(A, \mathfrak{m}) \to (B, \mathfrak{n})$ be a local homomorphism of Noetherian local rings, and $M$ is a finite $B$-module, then the following are equivalent:

- $M$ is flat over $A$.
- $\text{Tor}_1^A(M, A/\mathfrak{m}) = 0$.
- $M/\mathfrak{m}^nM$ is flat over $A/\mathfrak{m}^n$ for sufficiently large $n$.

Proof: 1 $\to$ 2, 1 $\to$ 3 is trivial. For the converse, we need to prove $\text{Tor}_1^A(M, A/I) = 0$ for any ideal $I \subset A$, or $I \otimes M \to M$ is injective.

If 2 holds, then $\text{Tor}_1^A(M, N) = 0$ for any $A$-module of finite length, because by devissage we can reduce $N$ to $A/\mathfrak{m}$.

Tensoring the exact sequence $0 \to \mathfrak{m}^n \cap I \to I \to I/I \cap \mathfrak{m}^n \to 0$ with $M$, we get

$$\mathfrak{m}^n \cap I \otimes M \to I \otimes M \to (I/I \cap \mathfrak{m}^n) \otimes M \to 0$$

and also the exact sequence $0 \to I/I \cap \mathfrak{m}^n \to R/\mathfrak{m}^n \to R/(I + \mathfrak{m}^n) \to 0$ gives

$$0 \to (I/I \cap \mathfrak{m}^n) \otimes M \to M/\mathfrak{m}^nM \to M/(I + \mathfrak{m}^n)M \to 0$$

by the fact $R/(I + \mathfrak{m}^n)$ has finite length in case 2 or the fact they are all $R/\mathfrak{m}^nM$ modules in case 3.

Thus the kernel of $I \otimes M \to M$ is contained in $(\mathfrak{m}^n \cap I) \otimes M$ for any $n$, which means it is contained in $\mathfrak{m}^n(I \cap M)$ for any $n$ by Artin-Rees (4.2.2.13). Thus the kernel is trivial by Krull’s intersection theorem (4.2.2.14) as $I \otimes M$ is finite over $S$. □

Prop. (4.4.1.17).

Flat ring extension

Prop. (4.4.1.18) [Flatness is Local]. Flatness is stalkwise both on the target and source, thus flatness is local both on the target and the source (4.1.4.2).

Cor. (4.4.1.19) [Going-down]. Going-down holds for flat ring map.

Proof: The ring map $R_{p'} \to S_{q'}$ is flat by (4.4.1.18), thus it is f.f. by (4.4.1.23). Then (4.4.1.21) says $p \subset p'$ is in the image. □

Prop. (4.4.1.20). if rings $A \subset B \subset C$ and $C/A, C/B$ is flat, then $B/A$ is flat.

Proof: Cf. [GAGA Serre P26]. □

Prop. (4.4.1.21). The following are equivalent:

- $A \to B$ is f.f.
- It is flat and $\text{Spec} B \to \text{Spec} A$ is surjective.
- It is flat and $\text{Spec}$ map contains all the closed pts.
Proof: This follows form (4.4.1.5) as we see that \( p \) is in the image of Spec map iff \( k(p) \otimes_A B \neq 0 \).

\[ \square \]

Cor. (4.4.1.22). Integral flat injective ring extension is f.f., by (4.2.1.5).

Cor. (4.4.1.23). Flat local ring map of local rings is f.f.

Cor. (4.4.1.24). Filtered colimits of f.f. rings over \( R \) is f.f.

Proof: If is flat by (4.4.1.6), and for a maximal ideal \( m \) of \( R \), \( S_i/mS_i \) is non-zero, hence there direct limit is non-zero because 1 is contained. So \( m \) is in the image, hence it is f.f. by (4.4.1.21).

\[ \square \]

Cor. (4.4.1.25) [Filtered Colimit of Flat Ring Maps]. If \( I \) is filtered and \( R_i \to S_i \) are (faithfully) flat ring maps, then \( \text{colim}_I R_i \to \text{colim}_I S_i \) is (faithfully) flat.

Proof: For any \( \text{colim}_I R_i \)-module \( M \), \( (\text{colim}_I S_i) \otimes_{\text{colim}_I R_i} M = \text{colim}(S_i \otimes_{R_i} M) \), so it is flat, because colim is exact. For the faithfully flatness, for any maximal ideal \( m \) of colim \( R_i \), let \( m_i = m \cap R_i \), then \( S_i/m_i S_i \neq 0 \), thus the direct limit is also \( \neq 0 \), so \( m \) is in the image, hence it is f.f. by (4.4.1.21).

\[ \square \]

Prop. (4.4.1.26). If \( R \to S \) is (faithfully) flat ring map and \( M \) is a (faithfully) flat \( S \)-module, then \( M \) is a (faithfully) flat \( R \)-module. In particular, (faithfully) flatness is stable under composition. Also (faithfully) flatness is stable under base change.

Prop. (4.4.1.27). If \( B \) is flat over \( A \), then

\[
\text{Tor}_i^A(M, N) \otimes B = \text{Tor}_i^B(M(B), N(B)), \quad \text{Ext}_i^A(M, N) \otimes B = \text{Ext}_i^B(M(B), N(B)).
\]

Prop. (4.4.1.28) [Faithfully Flat Ring Map is Injective]. A f.f. ring map \( R \to S \) is universally injective. In particular, tensoring with \( R/I \), we get \( R \cap IS = I \) for an ideal \( I \) of \( R \).

Proof: Because \( R \to S \) is f.f., we only need to show that \( N \otimes_R S \to N \otimes_R S \otimes_R S \) is injective for any \( N \), but this is true because it has a left inverse.

\[ \square \]

Prop. (4.4.1.29). A f.f. map between valuation rings is equivalent to an injective local homomorphism.

Prop. (4.4.1.30). A flat ring map maps a non-zero-divisor to a non-zero-divisor, because if we consider the principal ideal generated by it, then (4.4.1.2) shows the ideal in \( M \) is also injective, so it is not a zero-divisor.

Prop. (4.4.1.31) [Noetherian Completion is Flat]. If \( A \) is Noetherian and \( I \) is an ideal, then the \( I \)-adic completion \( A^\wedge \) is flat over \( A \) by (4.2.3.14).

Prop. (4.4.1.32) [Flat Map is Open]. The Spec map of a ring map \( R \to S \) of f.p. that satisfies going-down (e.g. flat), is open.

Proof: \( S \to S_f \) satisfies going-down and is of f.p, so we see that \( R \to S_f \) satisfies going down. It suffice to prove the image of this map is open. By Chevalley, the image is constructible, and it is stable under generalization. So it is open by (3.8.4.8).

\[ \square \]

Cor. (4.4.1.33). The Spec map \( f \) of a f.f. ring map is an quotient map.
Prop. (4.4.1.34) [Generic Freeness + F.P.]. Let $R$ be a reduced ring, $S$ a f.g. $R$-algebra, $M$ a finite $S$-module, and $R$ is reduced, then there exists an open dense subset $U \subset \text{Spec } R$ that there is a covering of $U$ by standard opens $D(f)$ s.t.
- $M_f$ and $S_f$ are free over $R_f$.
- $S_f$ is a f.p. $R_f$-algebra.
- $M_f$ is a f.p. $S_f$-module.
In particular, it is generically flat.

Proof: Cf. [Sta]051Z. □

Prop. (4.4.1.35) [Miracle Flatness]. Let $f : A \to B$ be a local map of local Noetherian rings s.t.
- $A$ is regular.
- $B$ is Cohen-Macauley.
- $\dim B = \dim A + \dim(A/f(\mathfrak{m}_A)B)$.
Then $f$ is flat.

Proof: Cf. [Sta]00R4. □

Prop. (4.4.1.36) [Slicing Criterion for Flat Modules on the Target]. Let $R \to S$ be a local homomorphism of local rings s.t.
- $S$ is essentially of f.p. over $R$,
- $M$ is of f.p. over $S$,
- $\text{Tor}_1^R(M, R/I) = 0$.
- $M/IM$ is flat over $R/I$.
Then $M$ is flat over $R$.

Proof: Cf. [Sta]0471. □

Prop. (4.4.1.37) [Slicing Criterion for Flatness on the Source]. Let $(R, \mathfrak{m}) \to (S, \mathfrak{n})$ be a local homomorphism of local rings s.t.
- $S$ is essentially of f.p. over $R$,
- $S$ is flat over $R$,
- $\mathfrak{t}$ is a non-zero divisor of $S/\mathfrak{m}S$.
Then $S/\mathfrak{t}S$ is flat over $R$, and $\mathfrak{t}$ is a non-zero divisor in $S$.

Proof: Cf. [Sta]046Z. □

Prop. (4.4.1.38) [Fibral Criterion of Flat Modules]. Let $R \to S \to S'$ be local homomorphisms of local rings and $\mathfrak{m}$ is the maximal ideal of $R$. If
- $R \to S'$ is essentially of f.p.
- $R \to S$ is essentially of f.t.
- $M \neq 0 \in \text{Mod}(S')$ is of f.p. over $S$.
- $M/\mathfrak{m}M$ is flat over $S/\mathfrak{m}S$.
- $M$ is flat over $R$.
Then $S$ is essentially of f.p. and flat over $R$ and $M$ is flat over $S$.

Proof: [Sta]05UV. □
2 Faithfully Flat Descent

Prop. (4.4.2.1) [Faithfully Flat Descent]. List of properties that descent through faithfully flat morphism. Let \( R \to R' \) be a f.f. ring map.

1. Finiteness for modules over a ring.
2. F.p. for modules over a ring.
3. Flatness for modules over a ring.
4. Finite locally freeness and invertibility for modules over a ring.
5. Mittag-Leffler for modules over a ring.
6. Projectiveness for modules over a ring.
7. F.g. for ring maps.
8. F.p. for ring maps, both on the target and source.
9. (Formal) Smoothness for ring maps.
11. Reducedness for rings.
13. Regular for rings.
14. Being Noetherian and has property \((R_k)\) for rings.
15. Local Complete Intersection ring maps.

Proof:

3. Let \( M \) be a \( R \)-module, and \( M' = M \otimes_R R' \), if \( M' \) is \( R \)-flat, then for any \( R \)-module \( N \),
   \( (N \otimes_R M) \otimes_R S = (N \otimes_R S) \otimes_S M' \), so as \( \cdot \otimes_R S \) is exact and reflects exactness, \( \cdot \otimes_R M \) is
   exact, so \( M \) is \( R \)-flat.
4. This follows from f.f. descent for f.p. and flatness and (4.3.1.7).
5. Cf. [Sta]05A5.
7. Cf. [Sta]00QP.
8. Cf. [Sta]00QQ, 00EP.
9. Use criterion (4.4.5.3), we see by flatness that the sequence \( I/I^2 \to \Omega_{P/R} \otimes_P S \to \Omega_{S/R} \to 0 \) commutes with flat base change, and when it is f.f., then use (4.4.3.6) and descent for projectiveness (4.4.2.1) that \( \Omega_{S/R} \) is projective, so it is a split exact sequence. The smooth case follows from definition (4.4.5.12) as f.p. can descend.
10. Because for \( S \to S' \) faithfully flat and a chain of ideals \( I_k \) in \( S \), \( I_kS' = I_k \otimes_S S' \), and \( I_kS' \) is
    stable if \( S' \) is Noetherian, so also \( I_k \) is stable because it is faithfully flat.
11. \( S \to S' \) is f.f. hence injective (4.4.1.28).
12. Normality is stalkwise, so it suffices to assume $R \rightarrow S$ is f.f. and $R, S$ are both local. Then $S$ is normal integral thus by (4.4.1.28), $R$ is also normal integral. Now if $a/b \in R$, then $a/b \in S$, $a \in bS$, thus $a \in bS \cap R = bR$ by (4.4.1.28), so $a/b \in R$.

13. Cf. [Sta]07NG.?


15. flatness and f.p. both satisfies f.f. descent, so it suffices to show that if $\mathfrak{p}' \subset R'$ is a prime lying over $\mathfrak{p} \subset R$, then $S \otimes_R k(\mathfrak{p})$ is a local complete intersection iff $S' \otimes_{R'} k(\mathfrak{p}') = S \otimes_R k(\mathfrak{p}) \otimes_{k(\mathfrak{p})} k(\mathfrak{p}')$ is a local complete intersection, and this follows from [Sta]00SI.

\[\square\]

\textbf{Prop. (4.4.2.2)[fpqc-Poincaré Lemma].} If a ring map $A \rightarrow B$, either has a section $B \rightarrow A$, or it is faithfully flat, then the Amitsur complex $s(M)$ for the canonical descent datum (with augmentation):

\[0 \rightarrow M \rightarrow B \otimes_A M \rightarrow B \otimes_A B \otimes_A M \rightarrow \ldots\]

with Čech-like maps, is exact.

\textit{Proof:} In the case $A \rightarrow B$ has a section $s$, It suffices to construct a nullhomotopy of the case $M = A$. Then we can just let $h(e_0 \otimes e_1 \otimes \ldots \otimes e_r) = s(e_0) e_1 \otimes \ldots \otimes e_r$.

The f.f. case can be reduced to the first case by tensoring $B$ to consider $B \rightarrow B \otimes_A B$, because it has a section. \[\square\]

\textbf{Cor. (4.4.2.3)[Glueing Functions].} Let $R$ be a commutative ring, $M$ a $R$-module, and $(f_1, \ldots, f_n) = (1)$, then there is an exact sequence

\[0 \rightarrow M \rightarrow \prod M_{f_i} \Rightarrow \prod M_{f_i f_j}.\]

In particular this holds for $M = R$.

\textit{Proof:} This is just (4.4.2.2) applied to $A \rightarrow \prod_i A_{f_i}$, which is faithfully flat. \[\square\]

\section*{Formal Glueing of Modules}

Main references are [Sta]Chap15.80 and 15.81.

\textbf{Lemma (4.4.2.4).} Let $R \rightarrow S$ be a ring map and $I = (f_1, \ldots, f_r) \subset R$ be an ideal, then for any $R$-module $M$ we can define a complex

\[0 \rightarrow M \otimes_R S \times \prod M_{f_i} \xrightarrow{\beta} \prod (M \otimes_R S)_{f_i} \times \prod M_{f_i f_j}\]

where $\alpha(m) = (m \otimes 1, m, \ldots, m)$, $\beta(m', m_1, \ldots, m_t) = (m' - m_1 \otimes 1, m' - m_2 \otimes 1, \ldots, m' - m_t \otimes 1, m_1 - m_2, \ldots, m_{t-1} - m_t)$.

Assume that $R \rightarrow S$ is flat and $R/I \rightarrow S/IS$ is an isomorphism, then this complex is exact.

\textit{Proof:} Cf. [Sta]05EK. \[\square\]

\textbf{Def. (4.4.2.5)[Category of Glueing Data].} Let $R \rightarrow S$ be a ring map and $I = (f_1, \ldots, f_r) \subset R$ be an ideal, then we define the category $\text{Glue}(R \rightarrow S, f_1, \ldots, f_r)$ of glueing data $\text{Glue}(R \rightarrow S, f_1, \ldots, f_i)$ consisting of objects $M = (M', M_i, \alpha_i, \alpha_{ij})$ where $M'$ is a $S$-module, $M_i$ are $R_{f_i}$-modules, $\alpha_i : (M')_{f_i} \rightarrow M_i \otimes_R S$ and $\alpha_{ij} : (M_i)_{f_j} \rightarrow (M_j)_{f_i}$ are isomorphisms that
• $\alpha_{ij} \circ \alpha_i = (\alpha_j)_{f_i}$.
• $\alpha_{jk} \circ \alpha_{ij} = \alpha_{ik}$.

There is a canonical functor $\text{Can} : \text{Mod}_R \rightarrow \text{Glue}(R \rightarrow S, f_1, \ldots, f_r)$ and also a morphism $H^0 : \text{Glue}(R \rightarrow S, f_1, \ldots, f_r) \rightarrow \text{Mod}_R$ where

$$H^0(M) = \ker(M' \times \prod M_i \rightarrow \prod M'_{f_i} \times \prod(M_i)_{f_j}).$$

$H^0$ is a left inverse of Can, by (4.4.2.4).

**Lemma (4.4.2.6).** If $R \rightarrow S$ is flat, then $\text{Glue}(R \rightarrow S, f_1, \ldots, f_r)$ is an Abelian category, and Can is an exact functor that commutes with arbitrary colimits.

If moreover $(f_1, \ldots, f_r) = R$, then Can and $H^0$ induces an equivalence of categories.

**Proof:** The kernels and cokernels can be constructed because $- \otimes_R S$ is exact, and Can is exact because $R_{f_i}$ and $S$ are flat over $R$, and also tensoring commutes with taking colimits.

For the last assertion, by (4.4.2.5) it suffices to show that Can is essentially surjective. For this, just use (4.4.2.3) on both $R$ and $S$. \qed

**Prop. (4.4.2.7).** In the setting of (4.4.2.5), if $R/I \rightarrow S/IS$ is an isomorphism, then Can and $H^0$ induces an equivalence of categories.

**Proof:** Cf. [Sta]05ER. \qed

**Cor. (4.4.2.8).** If $R \rightarrow S$ is a flat ring map and $f \in R$ that $R/fR \cong S/fS$ is an isomorphism, then there is a pullback diagram of categories:

$$
\begin{array}{ccc}
\text{Mod}_R & \longrightarrow & \text{Mod}_{R_f} \\
\downarrow & & \downarrow \\
\text{Mod}_S & \longrightarrow & \text{Mod}_{S_f}
\end{array}
$$

and we can also restrict to the category of f.g./f.p/flat/projective(any property satisfying f.f. descent) modules.

**Proof:** For the last assertion, notice $R \rightarrow R^{\wedge} \times \prod R_{f_i}$ is f.f. by (4.2.3.7), then use f.f. descent (4.4.2.1). \qed

**Cor. (4.4.2.9).** If $R$ is a Noetherian ring, $f \in R$ and $R^{\wedge}$ the $f$-adic completion of $R$, then there is a pullback of categories:

$$
\begin{array}{ccc}
\text{Mod}_R & \longrightarrow & \text{Mod}_{R_f} \\
\downarrow & & \downarrow \\
\text{Mod}_{R^{\wedge}} & \longrightarrow & \text{Mod}_{R_{f}^{\wedge}}
\end{array}
$$

and we can also restrict to the category of f.g./f.p/flat/projective(any property satisfying f.f. descent) modules.

**Proof:** This satisfies the hypothesis of (4.4.2.7) by (4.2.3.14). \qed
Def. (4.4.2.10) [Gluing Pairs]. Let $R \to R'$ be a ring map and $f \in R$ that induces an isomorphism $R/f^n R \cong R'/f^n R'$ for any $n > 0$, then $(R \to R', f)$ is called a gluing pair if the sequence

$$0 \to R \to R' \oplus R_f \to R'_f \to 0$$

is exact. The pair $(R, f)$ is called a gluing pair if $(R \to \hat{R}, f)$ is a gluing pair (This makes sense by (4.2.3.6)).

This is equivalent to $R[f^\infty] \to R'[f^\infty]$ is bijective.

Let $M$ be an $R$-module, then $M$ is called a glueable module for $(R \to \hat{R}, f)$ if the sequence

$$0 \to M \to M_{R'} \oplus M_{R_f} \to M_{R'_f} \to 0$$

is exact.

This is equivalent to $M[f^\infty] \to M_{R'}[f^\infty]$ is a bijection. And when $(R \to R', f)$ is a gluing pair, this is equivalent to $M[f^\infty] \to M_{R'}[f^\infty]$ is injective.

Proof: Cf. [Sta]0BNR, 0BNW.

Prop. (4.4.2.11) [Flatness and Gluing]. $(R \to R', f)$ is a gluing pair when $R \to R^\wedge$ is flat. In particular $(R, f)$ is a gluing pair then $R$ is Noetherian or $f$ is a nonzero-divisor (4.2.3.10), Cf. [Sta]0BNT.

If $(R \to R', f)$ is gluing, then $M$ is glueable if $\text{Tor}_1^R(M, R')$ is $f$-power torsion, or equivalently $\text{Tor}_1^R(M, R'_f) = 0$. In particular this is the case when $M$ is flat $R$-module or $f$ is not a zero-divisor. And when $R \to R'$ is flat, any $R$-module $M$ is glueable, in particular this is the case for $(R, f)$ when $R$ is Noetherian. Cf. [Sta]0BNX.

Prop. (4.4.2.12) [Beauville-Laszlo]. Let $A$ be a commutative ring and $f \in A$ is a nonzero-divisor, let $\hat{A}$ be the $f$-adic completion, then there is a pullback diagram of categories:

\[
\begin{array}{ccc}
\text{Mod}_A & \longrightarrow & \text{Mod}_{\hat{A}}[1/f] \\
\downarrow & & \downarrow \\
\text{Mod}_{\hat{A}} & \longrightarrow & \text{Mod}_{\hat{A}}[1/f] \\
\end{array}
\]

Proof: Cf. [Sta]Ch15.81.

3 Kähler Differentials

Def. (4.4.3.1) [Derivations]. A derivation over $S$ from an $S$-algebra $R$ to an $S$-module $M$ is a morphism of $S$-modules $\delta: R \to M$ that $\delta(ab) = a\delta(b) + b\delta(a)$. The set of all derivatives from $R$ to $M$ is denoted by $\text{Der}_S(R, M)$

Def. (4.4.3.2) [$A \times_R M$]. For any $R$-algebra $A$, there is a functor $A \times -$ from $\text{Mod}_R$ to $(\text{Alg}_R)_A$ that $A \times_R M = A \otimes_R M$ with the algebra given by

$$(a, x)(b, y) = (ab, ay + bx).$$

Then there is a bijection of sets

$$\text{Der}_R(X, A \times_R M) \cong \text{Der}_R(X, M).$$
Def. (4.4.3.3) [Kähler Differential]. Let \( S \to R \) a ring map, then the **Kähler Differential** \( \Omega_{R/S} \) is defined as a \( R \)-module that \( \operatorname{Der}_S(R, M) \cong \operatorname{Hom}_S(\Omega_{R/S}, M) \). In particular, \( \operatorname{Der}_S(R, R) \) is the \( R \)-dual of \( \Omega_{R/S} \).

**Prop. (4.4.3.4).** One construction is by the free group generated by elements of \( R \) module some relations. It can also be constructed as follows: there are two ring maps \( \lambda_i \) from \( S \) to \( R \otimes_R S \), and one map \( \varepsilon \) from \( S \otimes_R S \) to \( S \). Let \( I = \ker \varepsilon \) as a \( R \)-module by \( \lambda_1 \), then \( I \triangleleft I^2 \cong \Omega_S \otimes_R S \otimes_R S \otimes_R S \cong \Omega_{S/R} \) by (4.4.3.8).

So \( I \otimes \Omega_I^2 = \Omega_S \otimes_R S \otimes_R S \otimes_R S \cong \Omega_{S/R} \). And it can be verified that \( a \otimes 1 - 1 \otimes a \) corresponds to \( da \).

**Prop. (4.4.3.5) [Adjointness].** The functor \( X \to A \otimes_X \Omega_{X/R} \) is left adjoint to the functor \( A \leftarrow_R R \) defined in (4.4.3.2) as a functor from \( (\mathbb{C}_{\operatorname{Alg}}_R)_A \to \operatorname{Mod}_A \).

**Proof:** Because they are both equivalent to \( \operatorname{Der}_R(X, M) \).

**Cor. (4.4.3.6) [Functoriality].** From the first construction, we can see directly that for a family of morphisms \( R_i \to S_i \),

\[
\Omega_{\operatorname{colim} S_i/\operatorname{colim} R_i} = \operatorname{colim} \Omega_{S_i/R_i}.
\]

In particular, we have:

\[
T^{-1} \Omega_{B/A} = \Omega_{T^{-1} B/A}, \quad \Omega_{S^{-1} B/S^{-1} A} = S^{-1} \Omega_{B/A}.
\]

Moreover, we have

\[
\Omega_{S/R} \otimes_R R' = \Omega_{S \otimes_R R' \otimes R'}, \quad (S \otimes_R \Omega_{T/R}) \oplus (T \otimes_R \Omega_{S/R}) \cong \Omega_{S \otimes_R T/R}
\]

by universal properties.

**Proof:** We prove for the localization: it suffices to show the following two assertions:

1. \( S^{-1} \Omega_{A/B} \cong \Omega_{S^{-1} A/B} \).
2. If \( T \subset B \) is a multiplicatively closed subset that \( i(t) \) are all invertible in \( A \), then \( \Omega_{A/T^{-1} B} \cong \Omega_{A/B} \).

We check the universal properties: For any \( S^{-1} A \)-module \( M \),

\[
\operatorname{Hom}_{S^{-1} A}(S^{-1} \Omega_{A/B}, M) \cong \operatorname{Hom}_{S^{-1} A}(S^{-1} A \otimes_A S^{-1} A, M) \cong \operatorname{Hom}_A(\Omega_{A/B}, M) \cong \operatorname{Der}_B(A, M),
\]

\[
\operatorname{Hom}_{S^{-1} A}(\Omega_{S^{-1} A/B}, M) \cong \operatorname{Der}_B(S^{-1} A, M)
\]

There is a map \( \operatorname{Der}_B(S^{-1} A, M) \to \operatorname{Der}_B(A, M) \) by restriction, and the converse is given by

\[
d \mapsto d \left( \frac{a}{s} \right) = \frac{sd a - ads}{s^2},
\]

This is well-defined as

\[
d \left( \frac{at}{st} \right) = \frac{std(at) - atds}{s^2 t^2} = \frac{sd a - ads}{s^2},
\]
and it satisfies
\[
d\left(\frac{a_1}{t_1} + \frac{a_2}{t_2}\right) = d\left(\frac{a_1 t_2 + a_2 t_1}{t_1 t_2}\right) = \left(\frac{(a_1d(t_2) + t_2d(a_1) + a_2d(t_1) + t_1d(a_2))t_1 t_2 - (a_1 t_2 + a_2 t_1)(t_1 d(t_2) - t_2 d(t_1))}{t_1^2 t_2^2}\right)
= \frac{t_1^2 t_2^2 d(a_1) + t_1^2 t_2^2 d(a_2) - a_2 t_2^2 d(t_2) + a_1 t_2^2 d(t_1)}{t_1^2 t_2^2}
= d\left(\frac{a_1}{t_1}\right) + d\left(\frac{a_2}{t_2}\right)
\]
\[
d\left(\frac{a_1 a_2}{t_1 t_2}\right) = \frac{(a_1 d(a_2) + a_2 d(a_1)) t_1 t_2 - a_1 a_2 (t_1 d(t_2) + t_2 d(t_1))}{t_1^2 t_2^2}
= \frac{a_1 (t_2 d(a_1) - a_2 d(t_2))}{t_1 t_2^2} + \frac{a_2 (t_1 d(a_2) - a_1 d(t_1))}{t_2 t_1^2}
= \frac{a_1}{t_1} d\left(\frac{a_2}{t_2}\right) + \frac{a_2}{t_2} d\left(\frac{a_1}{t_1}\right)
\]

Thus this \(d\) is an extension of the derivative to \(S^{-1}A\). Thus we get the desired isomorphism by Yoneda lemma. \(\square\)

**Prop. (4.4.3.7) [Jacobi-Zariski Sequences].** For a sequence of commutative rings: \(A \to B \to C\), there is an exact sequence
\[
C \otimes_B \Omega_{B/A} \to \Omega_{C/A} \to \Omega_{C/B} \to 0
\]
of \(C\)-modules. It has a left inverse and splits iff any derivation over \(A\) from \(B\) to a \(C\)-module can be extended to a derivation over \(A\) from \(C\) to \(M\). This is trivially true when \(B \to C\) has a retraction, and true when \(C/B\) is formally smooth by (4.4.5.5).

**Proof:** Taking Hom with an arbitrary \(C\)-module \(M\), by universal property, we need to check the exactness of \(0 \to \text{Der}_B(C, M) \to \text{Der}_A(C, M) \to \text{Der}_A(B, M)\), which is easy. \(\square\)

**Prop. (4.4.3.8) [Second Exact Sequence].** (This is a special case of (8.2.1.5)). If \(S' = S/I\), then there is an exact sequence of \(R'\)-modules:
\[
I/I^2 \to \Omega_{S/R} \otimes_S S' \to \Omega_{S'/R} \to 0.
\]
Where \(f \in I\) is mapped to \(df \otimes 1\) and it has a left inverse and splits iff \(S/I^2 \to S'\) has a right inverse.

And in fact \(\Omega_{S/R} \otimes S' \cong \Omega_{(S/I^2)/R} \otimes S'\).

**Proof:** For a \(S/I\)-module \(M\), we check:
\[
0 \to \text{Der}_R(S/I, M) \to \text{Der}_R(S, M) \to \text{Hom}_{S/I}(I/I^2, M)
\]
To prove \(\Omega_{S/R} \otimes S' \cong \Omega_{(S/I^2)/R} \otimes S'\), we apply Hom for a \(S'\)-module \(M\).

So to prove the left exactness, we may assume \(I^2 = 0\). If we have an inverse \(\Omega_{S/R} \otimes S' \to I\), then it gives a derivation \(D : A \to I\) that is identity on \(I\), so \(a - D(a)\) gives a \(R\)-ring map \(S \to S\) that is trivial on \(I\) (because \(I^2 = 0\)). Hence it gives a \(S/I \to S\) that is inverse to the projection.

For the converse, if \(d : S/I \to S\) is a right inverse, then \(a - d(\pi)\) is a derivation \(S \to I\), which is identity on \(I\), so it gives a inverse map \(\Omega_{S/R} \otimes S' \to I\) by universal property. \(\square\)
Cor. (4.4.3.9). If \( R \to S \) is of f.p., then \( \Omega_{S/R} \) is of f.p. over \( S \). If \( R \to S \) is of f.t., then \( \Omega_{S/R} \) is of f.t. over \( S \). (Follows from the second exact sequence (4.4.3.8) and (4.4.3.10)).

Cor. (4.4.3.10) [Examples].
1. \( \Omega_{A[X_1, \ldots, X_n]/A} = A[X_1, \ldots, X_n]\{dX_1, \ldots, dX_n\} \).
2. If \( S = A[X_i]/\langle f_j \rangle \), then \( \Omega_{S/A} = S[dX_i]/\langle df_j \rangle \).
3. \( \Omega_{A[X_i]/k} = \Omega_{A/k} \otimes_A A[X_i] \oplus A[X_i]\{dX_1, \ldots, dX_n\} \).
4. (Standard Étale Algebra) For \( A = R[x]/(f) \), where \( f' \) has image invertible in \( A, \Omega_{A/R} = 0 \).
5. The differential for the inclusion \( k[y^2, y^3] \to k[y] \) is \( k[y]/(2y, 3y^2)\{dy\} \).

Cor. (4.4.3.11). 1: Use the differential operator and universal property.
2: Use item 1 and (4.4.3.8).
3: Use item 1 and the fact (4.4.3.8) splits because any derivative of \( A/k \) can be extended to derivative of \( B/k \) by acting on the coefficients.
4:
5: Use definition.

Cor. (4.4.3.12). If \( S/I \) is a field \( k \) that embeds in \( S \), then \( I/I^2 \cong \Omega_{S/k} \otimes_S k \).

Prop. (4.4.3.13). Let \( k \subset K \subset L \) be fields, and \( L/K \) f.g., then
\[
\dim_L \Omega_{L/k} \geq \dim_K \Omega_{K/k} + \deg(L/K).
\]
Equality holds if \( L/K \) is separably generated, i.e. separable over a transcendental basis. If \( K = k \), then the equality hold iff \( L/k \) is separably generated. In particular, \( L/k \) is separable algebraic extension iff \( \Omega_{L/k} = 0 \).

Proof: Take a subfield \( K \subset K(t_1, \ldots, t_n) \subset L \) that \( L \) is separable algebra over \( K(t_1, \ldots, t_n) \). Then it suffices to add one element a time, so we may assume \( L = K(\alpha) \).
1: If \( \alpha \) is transcendental over \( K \), then \( \Omega_{K(\alpha)/t} \cong \Omega_{K(\alpha)} \otimes K[\alpha] /\alpha dt \) by (4.4.3.10), and by localization (4.4.3.6) we get \( \Omega_{L/K} \cong \Omega_{K/k} \otimes K L \oplus Ld\alpha \), thus \( \text{rank} \, \Omega_{L/k} = \text{rank} \, \Omega_{K/k} + 1 \).
2: If \( \alpha \) is separable over \( K \), then there is a monic polynomial \( f \in K[X] \) such that \( K[\alpha] \cong K[X]/(f) \). Then \( f' \) is invertible in \( K[\alpha] \), and by (4.4.3.10) \( \Omega_{K[\alpha]/k} = \Omega_{K/k} \otimes K L \oplus LdX/(d(f) + f'dX) \cong \Omega_{K/k} \otimes K L \). Thus \( \text{rank} \, \Omega_{L/k} = \text{rank} \, \Omega_{K/k} \).
3: If \( K \) has characteristic \( p \) and \( L = K[X]/(X^p - a) \) and \( d_{K/k}(a) = 0 \), then \( \Omega_{K[a]/k} = \Omega_{K/k} \otimes K L \oplus LdX/(d(a)) \cong \Omega_{K/k} \otimes K L \oplus LdX/(d(a)) \). Thus \( \text{rank} \, \Omega_{L/k} = \text{rank} \, \Omega_{K/k} + 1 \).
4: If \( K \) has characteristic \( p \) and \( L = K[X]/(X^p - a) \) and \( d_{K/k}(a) \neq 0 \), then \( \Omega_{K[a]/k} = \Omega_{K/k} \otimes K L \oplus LdX/(d(a)) \) has rank \( \text{rank} \, \Omega_{K/k} \).
Thus the assertion is clear.

Prop. (4.4.3.14) [Differential and Regularity]. Let \( B \) be a Noetherian local ring containing its residue field \( k \) and \( k \) is perfect, then \( \Omega_{B/k} \) is a free \( B \)-module of rank \( \dim B \) iff \( B \) is regular. [Hartshorne Ex.2.8.1] has a generalization of this fact.

Proof: One way is by (4.4.3.12). Conversely, if \( B \) is regular, then it is integral (4.3.5.19), so \( \Omega_{B/k} \otimes B K = \Omega_{K/k}(4.4.3.6) \) is of \( K \)-dimension \( \text{deg} \, K/k = \dim B \), where \( K \) is the quotient field of \( B \), and \( \Omega_{B/k} \otimes k \cong m/m^2 \) is of \( k \)-dimension \( \dim B \) once again. These two facts shows that \( \Omega_{B/k} \) is free \( B \)-module of rank \( \dim B \) by (4.4.8.1).

Prop. (4.4.3.15). The Kähler differential \( \Omega_{O_L/O_K} \) for an extension of number fields is cyclic.

Proof: Because it is locally cyclic (4.2.7.30).
4 Complete Intersections

Koszul Complex

**Prop. (4.4.4.1) [Koszul Complex].** The complex of $\mathbb{Z}[X_1, \ldots, X_n]$-modules $K_\bullet$, where

$$K_r = \wedge^{r+1} \mathbb{Z}[dX_1, \ldots, dX_n] \otimes_{\mathbb{Z} A, f_1, \ldots, f_n} \mathbb{Z}[X_1, \ldots, X_n]$$

and the morphism is given linearly by

$$\iota : dX_i \wedge dX_{i_1} \wedge \ldots \wedge dX_i \mapsto \sum_k X_{i_k}dX_{i_0} \wedge \ldots \wedge dX_{i_{k-1}} \wedge dX_{i_{k+1}} \wedge \ldots \wedge dX_i$$

Then this is a free resolution of $\mathbb{Z}$ over $\mathbb{Z}[X_1, \ldots, X_n]$.

**Proof:** We can use induction. If $r = 1$, then this is clear. For the induction process, if $\iota(dX_1 \wedge \alpha + \beta) = 0$, and $\beta \in K_i$, where $\beta, \alpha$ has no $dX_1$ involved. Notice if $dX_1 \wedge \alpha \in K_0$, then we may assume $\alpha$ has no constant coefficient, because this is impossible.

then $X_1\alpha - dX_1 \wedge \iota(\alpha) + \iota(\beta) = 0$. Then we see that $\iota(\alpha) = 0$. We can write $\alpha = \alpha_0 + X_1\alpha_1 + X_2\alpha_2 + \ldots$, where $\alpha_i$ has no $X_1$ involved, then we see that $\iota(\alpha_i) = 0$, then by induction hypothesis $\alpha = \iota(\alpha')(notice \, \alpha_0 \, has \, no \, constant \, coefficient)$, and $\iota(\beta) + X_1\iota(\alpha') = 0$. If $\beta = X_1\beta_1 + \beta_2$, where $\beta_2$ has no $X_1$ involved, then $\iota(\beta_2) = 0$, so $\beta_2 = \iota(\beta_2')$, and $\iota(\beta_1 + \alpha') = 0$, so $\beta_1 + \alpha' = \iota(\beta')$. So

$$dX_1 \wedge \alpha + \beta = dX_1 \wedge \iota(\alpha') + \iota(X_1\beta'_1 + \beta'_2) - X_1\alpha' = \iota(X_1\beta'_1 + \beta'_2 - dX_1 \wedge \alpha').$$

And in degree 0, this is clear. \qed

**Def. (4.4.4.2) [Koszul Complex].** Let $A$ be a ring and $I = (f_1, \ldots, f_n) \subseteq A$ is an ideal, then the Koszul complex for $Kos(A, f_1, \ldots, f_n)$ is an object in $D(A)$ defined by

$$Kos(A, f_1, \ldots, f_n) = A \otimes_{\mathbb{Z}[X_1, \ldots, X_n]} \mathbb{Z},$$

where $A$ is a $\mathbb{Z}[X_1, \ldots, X_n]$-algebra by mapping $X_i \mapsto f_i$. If $M$ is an $A$-module, then we define $Kos(M, f_1, \ldots, f_n) = M \otimes_{\mathbb{Z}} Kos(A, f_1, \ldots, f_n)$.

**Prop. (4.4.4.3).** If $f_1, \ldots, f_n \in R$, then $I = (f_1, \ldots, f_n)$ annihilates $H^*(K(f_1, \ldots, f_n))$. In particular, $Kos(A, f_1, \ldots, f_n)$ is in the image of $D(A/I) \subset D(A)$.

**Proof:** This is because every $H^i(A \otimes_{\mathbb{Z}[X_1, \ldots, X_n]} \mathbb{Z})$ is an $H^0(A \otimes_{\mathbb{Z}[X_1, \ldots, X_n]} \mathbb{Z}) = A/I$-algebra, because it is a simplicial algebra. \qed

**Prop. (4.4.4.4).** $K(A, f_1, \ldots, f_n, g_1, \ldots, g_m) = K(A, f_1, \ldots, f_n) \otimes_A K(A, g_1, \ldots, g_m)$. (Easy).

**Prop. (4.4.4.5).** The cone of the map

$$f_n : K(f_1, \ldots, f_{n-1}) \to K(f_1, \ldots, f_{n-1})$$

is isomorphic to $K(f_1, \ldots, f_n)$.

**Proof:** This is because $\mathbb{Z}[X] \xrightarrow{X} \mathbb{Z}[X] \to \mathbb{Z}$ is an exact triangle, so $A \xrightarrow{f_n} A \to A \otimes_{\mathbb{Z}[X]} \mathbb{Z}$ is an exact triangle, so $Kos(A, f_1, \ldots, f_{n-1}) \xrightarrow{f_n} K(A, f_1, \ldots, f_{n-1}) \to K(A, f_1, \ldots, f_n)$ is an exact triangle. \qed
Prop. (4.4.4.6). Let $A$ be a ring and $M$ be an $A$-module. Let $f_1, \ldots, f_{r-1}, f, g$ be elements of $A$, then there is a natural distinguished triangle

$$Kos(M, f_1, \ldots, f_{r-1}, f) \rightarrow Kos(M, f_1, \ldots, f_{r-1}, fg) \rightarrow Kos(M, f_1, \ldots, g).$$

Proof: We use (4.4.4.5) to consider $Kos(M, f_1, \ldots, f_{r-1}, f)$ as a cone of $f_n : Kos(M, f_1, \ldots, f_{r-1}) \rightarrow Kos(M, f_1, \ldots, f_{r-1})$. Then this distinguished triangle is given by (3.4.1.15) applied to the diagram

$$
\begin{array}{ccc}
Kos(M, f_1, \ldots, f_{r-1}) & \rightarrow & Kos(M, f_1, \ldots, f_{r-1}) \\
f & \downarrow & fg \\
Kos(M, f_1, \ldots, f_{r-1}) & \rightarrow & Kos(M, f_1, \ldots, f_{r-1}) \\
\end{array}
$$

□

Prop. (4.4.4.7) [Koszul Complex and Čech Complex]. Let $A$ be a commutative ring and $I = (f_1, \ldots, f_n) \subset A$, $K_n^\bullet = Kos(A, f_1^n, \ldots, f_n^n) = A \otimes_{\mathbb{Z}[X_1, \ldots, X_r]} \mathbb{Z}$. Then there are natural maps

$$\ldots \rightarrow K_n^0 \rightarrow K_n^1 \rightarrow K_n^2 \rightarrow \ldots$$

compatible with the inverse system $H^0(K_n^\bullet) = A/(f_1^n, \ldots, f_n^n)$. Then there is a description of $R \colim K_n^\bullet$ (4.6.5.6) as the alternating Čech complex

$$R \rightarrow \bigoplus_{i_0} R_{f_{i_0}} \rightarrow \bigoplus_{i_0 < i_1} R_{f_{i_0}f_{i_1}} \rightarrow \ldots \rightarrow R_{f_1f_2...f_r}$$

where $R$ sits in degree 0.

Proof: Cf. [Sta]0913, which is not hard. □

Def. (4.4.4.8) [Koszul-Regular Sequence]. Let $A$ be a ring and $(f_1, \ldots, f_n) \in A$ be a sequence, then $f_1, \ldots, f_n$ is called $M$-Koszul-regular iff $Kos(M, f_1, \ldots, f_n) = 0$. It is called Koszul-regular iff $Kos(A, f_1, \ldots, f_n) = 0$.

Prop. (4.4.4.9). If $(f_1, \ldots, f_r)$ is (M-Koszul)regular and $n_i > 0$, then $(f_1^{n_1}, \ldots, f_r^{n_r})$ is also (M-Koszul)regular.

Proof: This follows from (4.4.4.6). □

Prop. (4.4.4.10) [Regular and Koszul-Regular]. A $M$-regular sequence (4.3.4.1) is $M$-Koszul-regular. A regular sequence is Koszul-regular.

Proof: Let $(f_1, \ldots, f_r)$ be a regular sequence. The assertion is clear when $r = 1$. For the induction:

$$Kos(M, f_1, \ldots, f_n) = Kos(M, f_2, \ldots, f_n) \otimes_{\mathbb{Z}[X]} \mathbb{Z} = Kos(A, f_2, \ldots, f_n) \otimes_A M \otimes_{\mathbb{Z}[X]} \mathbb{Z}$$

$$= Kos(A/f_1, f_2, \ldots, f_n) \otimes_{A/f_1 M/f_1 M} M/f_1 M = Kos(M/f_1 M, f_2, \ldots, f_n)$$

so we can use induction. □
Complete Intersections

Def.(4.4.4.11)[Global Complete Intersections]. A ring map \( R \to S \) is called global intersection if \( S = R[x_1, \ldots, x_n]/(f_1, \ldots, f_c) \) that every non-empty fiber of \( \text{Spec} \, S \to \text{Spec} \, R \) has dimension \( n - c \).

Prop.(4.4.4.12). Global intersection is stable under base change and composition. And \( S \to S_f \) a global intersection, so it is stable under localization.

Proof: Base change: this is because flatness, f.p. is stable under base change, and the fibers are the same.
Composition: It suffices to assume \( R \) is a field and calculate the dimension of the fibers, which is true by dimension formula (4.2.4.13).

Prop.(4.4.4.13)[Noetherian Approximation]. Let \( R \) be a ring and \( S = R[X_1, \ldots, X_n]/(f_1, \ldots, f_c) \) be a global complete intersection, then there is a f.g. \( \mathbb{Z} \)-algebra \( R_0 \subset R \) that \( f_i \in R_0[X_1, \ldots, X_n] \), and \( S_0 = R_0[X_1, \ldots, X_n]/(f_1, \ldots, f_c) \) is a global intersection over \( R \).

Proof: Cf.[Sta]00SU.

Prop.(4.4.4.14) [Complete Intersection is Regular]. Let \( R \) be a ring and \( S = R[X_1, \ldots, X_n]/(f_1, \ldots, f_c) \) be a complete intersection, then \( \text{Spec} \, S \to \text{Spec} \, R[X_1, \ldots, X_n] \) is a regular embedding (5.6.8.1), and \( S \) is flat over \( R \).

Proof: Cf.[Sta]00SV.

Local Complete Intersections

Def.(4.4.4.15)[Local Complete Intersections]. Let \( S \) be a \( R \)-algebra, then \( S \) is a local complete intersection over \( R \) iff \( S \) is locally a global complete intersection over \( R \). Local complete intersection is flat, by (4.4.4.14).

Prop.(4.4.4.16). Local complete intersection is local on the source and target. In fact satisfies f.f. descent (4.4.2.1).

Lemma(4.4.4.17). If \( S \) is a f.t. \( k \)-algebra and \( K/k \) is a field extension, then \( S \) is a local complete intersection iff \( S_K \) is a local complete intersection.

Prop.(4.4.4.18)[Global Intersections and Fibers]. Let \( R \to S \) be a ring map and \( q \subset S \) be a prime lying over \( p \subset R \), then the following are equivalent:
- \( R \to S \) is a global complete intersection around \( q \).
- \( R \to S \) is a f.p. around \( q \), \( S_q/R_p \) is flat, and (the fiber) \( S_q/pS_q \) is a local complete intersection ring over \( k(p) \).

Proof: 1 \( \to \) 2 follows from (4.4.4.14). For 2 \( \to \) 1, Cf.[Sta]00SY.

Prop.(4.4.4.19)[Local Complete Intersection over Fields is Stalkwise]. For a f.g. \( k \)-algebra \( S \), \( S \) is a local complete intersection iff all localization at (maximal)primes are complete intersection local rings over \( k \). In particular, being local complete intersection is a stalkwise property.
Proof: This is because over field everything is f.p. and flat, and use (4.4.4.18). □

Prop. (4.4.4.20). If $S$ is a f.g. local complete intersection over a field $k$, then it is a CM ring.

Proof: Cf. [Sta]00SB. □

Def. (4.4.4.21) [Complete Intersection Local Rings]. Let $A$ be a local ring essentially of f.t. over a field $k$, then $A$ is called a complete intersection local ring over $k$ if there exists a surjection $R \to A$ from a regular local ring essentially of f.t. over $k$ that the kernel is generated by a regular sequence.

Prop. (4.4.4.22). When $A$ is f.g. local ring over a field $k$, then $A$ is a complete intersection local ring iff $A$ is local complete intersection over $k$ (4.4.4.11).

Proof: Cf. [Sta]00SC. See more in [Sta] Chap 23.8.

5 Smoothness

Formally Smoothness

Def. (4.4.5.1). A ring map $R \to S$ is called formally smooth if has right lifting property w.r.t all ring maps $A \to A/I$ where $I^2 = 0$.

Formal smooth is stable under base change and composition, by universal arguments. A polynomial algebra is formally smooth.

Prop. (4.4.5.2). Giving a presentation $S = P/J$ where $P$ is formally smooth (e.g. polynomial algebra), $S$ is formally smooth iff there is a map $S \to P/J^2$ that is right converse to the obvious projection.

Proof: One way is from the definition of formally smooth applied to $P/J^2$ and $J$. Conversely, for any $A$ and $I$, we notice the map $P \to S \to A/I$ can be lifted to $P \to A$, and $J$ is mapped to $I$, so $J^2$ is mapped to 0, so we have a map $P/J^2 \to A$. Then $S \to P/J^2 \to A$ is the lifting. □

Cor. (4.4.5.3). If $P \to S$ is a presentation of $S/R$ by polynomial algebra with kernel $I$, then $S/R$ is formal smooth iff

$$0 \to I/I^2 \to \Omega_{P/R} \otimes_P S \to \Omega_{S/R} \to 0$$

is split exact as in (4.4.3.8).

Proof: This sequence is split exact iff $P/J^2 \to S$ has a right converse, by (4.4.3.8). □

Now we consider the relation of Formal Smoothness and Kahler Differentials.

Cor. (4.4.5.4) [Equivalence Definition]. $S/R$ is formally smooth iff $NL_{S/R}$ is quasi-isomorphic to a projective $S$-module at degree 0.

Proof: If $S/R$ is formally smooth, then choose a presentation will suffice by (4.4.5.3). The converse is also true by projectiveness and (4.4.5.3).

Cor. (4.4.5.5). If $C/B$ is formally smooth, then the Jacobi-Zariski sequence

$$0 \to C \otimes_B \Omega_{B/A} \to \Omega_{C/A} \to \Omega_{C/B} \to 0$$

as in (4.4.3.7) is split exact, by (8.2.1.5). In particular, any derivation of $B$ to a $C$-module can be extended to a derivation $C$ to a $C$-module.
Cor. (4.4.5.6). If $A \to B \to C$ with $A \to C$ formally smooth and $B \to C$ surjective with kernel $I$, then there is a split sequence

$$0 \to I/I^2 \to \Omega_{B/A} \otimes_B C \to \Omega_{C/A} \to 0$$

by (8.2.2.6).

Standard Smooth Algebra

Def. (4.4.5.7). A standard smooth algebra over $R$ is a algebra $S = R[X_1, \ldots, X_n]/(f_1, \ldots, f_c)$, where $c \leq n$ and $J(f_1, \ldots, f_c)$ is invertible in $S$.

Prop. (4.4.5.8) [Standard Smooth Localization]. If $R \to S$ is standard smooth, then $R \to S_g$ is standard smooth, and $R_f \to S_f$ is standard smooth (because stable under base change (4.4.5.9)).

Proof: For localization at $g \in S$, let $h$ be an inverse image of $g$ in $R[X_1, \ldots, X_n]$, then $S_g = R[X_1, \ldots, X_n, X_{n+1}]/(f_1, \ldots, f_c, X_{n+1}h - 1)$, and it is standard smooth. □

Prop. (4.4.5.9). Standard smoothness is stable under base change and composition.

Proof: For base change, notice the Jacobi matrix is the base change of the Jacobi matrix, so it is also invertible. For composition, write out the presentation, the determinant is the product of the presentation. □

Lemma (4.4.5.10) [Kähler Differential of Smooth Algebra is Free]. The Kähler differential of a standard smooth algebra $S$ over a field $k$ is free of rank $\dim S$, and $(f_1, \ldots, f_c)/(f_1, \ldots, f_c)^2$ is free over $S$ with basis $f_1, \ldots, f_c$. Moreover, $S$ is pure dimensional.

Proof: The naive cotangent complex for $S/R$ is

$$d : (f_1, \ldots, f_c)/(f_1, \ldots, f_c)^2 \to S[dX_1, \ldots, dX_n].$$

By hypothesis and linear algebra it is a split injection, and $\Omega_{S/R} = S[dX_{c+1}, \ldots, dX_n]$, so it is free of rank $n - c = \dim S$, because $S$ is a global complete intersection (4.4.5.11). □

Prop. (4.4.5.11) [Standard Smooth and Complete Intersection]. A standard smooth algebra $S = R[X_1, \ldots, X_n]/(f_1, \ldots, f_c)$ is a global complete intersection (4.4.4.11).

Proof: It suffices to show any fiber of $S$ has dimension $n - c$. For this, notice $S \otimes_R k(p)$ is also standard smooth, then we reduce to the field case. Now $I = (f_1, \ldots, f_c)$ satisfies $I/I^2 \to \oplus Sdx_i$ is a split injection. For any maximal ideal $m$ containing $I$, tensoring $k(m)$, we get an injection $I/mI \to \oplus k(m)dx_i$. Notice there is a commutative diagram

$$I \xrightarrow{d} S/m \otimes I \cong I/mI$$

$$\oplus Sdx_i \xrightarrow{dx_i \mapsto 1 \otimes x_i} S/m \otimes m \cong m/m^2$$

And the lower horizontal map is an isomorphism by Hilbert’s Nullstellensatz, so the image of $f_i$ in $m_i/m_i^2$ are linearly independent over $k(m)$, thus we can use (4.3.5.22) to show that $\dim S = n - c$. □
Smoothness

Def. (4.4.5.12)[Smooth Ring Map]. A ring map $R \rightarrow S$ is called smooth if it satisfies the following equivalent conditions:

- It is of f.p. and the naive cotangent complex $NL_{S/R}$ is quasi-isomorphic to a finite locally free $S$-module placed at degree 0. In other words,
  $$0 \rightarrow I/I^2 \rightarrow \Omega_{P/R} \otimes_P S \rightarrow \Omega_{S/R} \rightarrow 0$$
  is exact and $\Omega_{S/R}$ is finite locally free. By (8.2.1.1), we only need to prove for a single presentation of $S$.
- It is locally standard smooth.
- It is formally smooth and of f.p.

We say $S$ is smooth at $x$ if it is smooth on a nbhd of $x$.

Proof: 1 $\rightarrow$ 3: by (4.4.5.4). 3 $\rightarrow$ 1: By (4.4.5.4), $\Omega_{S/R}$ is f.p. and projective, so it is finite projective.

At this point we already know that the first definition is stable under base change and composition, because f.p. and formally smoothness both do (4.4.5.1)(4.3.7.9).

And also the first definition is local on source because f.p. does (4.1.4.4) and $NL$ commutes with localization (8.2.1.6) so we can use the local properties of triviality (4.1.4.2) and finite projectiveness (4.3.1.7).

Now it is also local on the source because it is stable under base change and composition and $R \rightarrow R_f$ does by locality on the source.

2 $\rightarrow$ 1: Now the property are all local on source. It suffices to prove a standard smooth map is smooth. This follows from (4.4.5.10).

1 $\rightarrow$ 2: We need to prove, assuming the first definition, it is locally standard smooth. For this, Cf.[Sta]00TA?

Cor. (4.4.5.13). Smoothness is stable under composition and base change. Smoothness is local on the source and target (In particular, $R \rightarrow R_f$ is smooth). (Already proved in the proof of (4.4.5.12)).

Prop. (4.4.5.14). A smooth map is a local complete intersection (4.4.4.15), hence flat.

Proof: Clear from (4.4.5.12).

Prop. (4.4.5.15)[Noetherian Descent]. A smooth ring map $R \rightarrow S$ is a base change of smooth ring map over a ring f.g. over $\mathbb{Z}$.

Proof: Use the equivalence definition (4.4.5.2), we know that there is a map

$$S = R[X_1, \ldots, X_n]/(f_1, \ldots, f_c) \rightarrow R[X_1, \ldots, X_n]/(f_1, \ldots, f_c)^2,$$

which if we write $\sigma(X_i) = h_i$, then must satisfy

$$f_i(h_1, \ldots, h_n) = \sum a_{ijk} f_j f_k.$$

Then we consider the subalgebra generated by $f_i, h_i, a_{ijk}$, then by the same reason, they form a smooth algebra over $\mathbb{Z}$, and its tensor with $R$ gives out $S$.

Cor. (4.4.5.16)[Strong Lifting Property]. For a smooth ring map, the lifting property is true for $A \rightarrow A/I$, where $I$ is locally nilpotent.
Lemma (4.4.5.19). Let $S$ be f.g. over a alg. closed field $k$ and $m$ a maximal ideal, then the following are equivalent:

- $S_m$ is regular.
- $\dim_k \Omega_{S/k} \otimes_S k \leq \dim S_m$
- $\dim_k \Omega_{S/k} \otimes_S k = \dim S_m$

Smooth over Fields

Lemma (4.4.5.22). Let $S$ be f.g. over a alg. closed field $k$ and $m$ a maximal ideal, then the following are equivalent:

- $S_m$ is regular.
- $\dim_k \Omega_{S/k} \otimes_S k \leq \dim S_m$
- $\dim_k \Omega_{S/k} \otimes_S k = \dim S_m$
• $S/k$ is smooth at $m$.

Proof: Cf.[Sta]00TS.

Prop.(4.4.5.23) [Differential Criterion of Smoothness]. For a ring $S$ f.g. over a field $k$, $S$ is smooth in a nbhd of $q$ iff \( \dim_{k(q)} \Omega_{S/k} \otimes k(q) \leq \dim_q(S) \).

And in this case, equality hold, and $S_q$ is regular.

Proof: Cf.[Sta]00TT.

If $S$ is smooth at $x$, then $\Omega_{S/R}$ is finite free on a nbhd of $x$ of rank equals to the dimension(4.4.5.10), so the equation holds.

Conversely, if $\dim_{k(x)} \Omega_{S/k} \otimes k(x) \leq \dim_x(X)$, then

Cor.(4.4.5.24) [Jacobian Criterion of Smoothness]. For a f.p. ring $S = R[X_1, \ldots, X_n]/(f_1, \ldots, f_c)$ and $q \subset S$, $S$ is smooth at $q$ iff the Jacobian has rank $\leq n - \dim_q(S)$ at $q$ iff the Jacobian has rank $\leq n - \dim_q(S)$ at $q$.

Lemma(4.4.5.25). Let $k$ be a field and $(R, m, \kappa)$ be a Noetherian local ring containing $k$. If the residue field of $R$ is a f.g. field extension of $k$, then the derivation map

\[
m/m^2 \to \Omega_{R/k} \otimes_R \kappa
\]

is injective.

Proof: Cf.[Sta]00TU.

Prop.(4.4.5.26) [Smooth and Regular at Geometric Points]. Let $S$ be f.g. over a field $k$, if $k(q)/k$ is separable(e.g. char 0) for $q$ a prime of $S$, then $S$ is smooth at $q$ iff it is regular at $q$.

Proof: Let $R = S_q$ with maximal ideal $m$. By(4.4.5.25) and(4.4.3.8) there is an exact sequence\[
0 \to m/m^2 \to \Omega_{R/k} \otimes_R k(q) \to \Omega_{k(q)/k} \to 0.
\]

Since $k(q)/k$ is separable, $\dim_{k(q)} \Omega_{k(q)/k} = \text{tr} \cdot \deg(k(q)/k)$. So

\[
\dim_{k(q)}(\Omega_{R/k} \otimes_R k(q)) = \dim_{k(q)} m/m^2 + \text{tr} \cdot \deg(k(q)/k) \geq \dim R + \text{tr} \cdot \deg(k(q)/k) = \dim_q(S)
\]

with identity iff $R$ is regular(The last identity comes from(5.6.3.7)). So we are done by differential criterion of smoothness(4.4.5.23).

Prop.(4.4.5.27) [Smooth over Fields and Geo.Regular]. Let $S$ be f.g. over a field $k$, then $S$ is smooth over $k$ iff $S$ is geo.regular(4.3.6.1).

Proof: If $S$ is smooth at $x$, then all its base change is smooth at $x$(4.4.5.13), and the stalk is regular by(4.4.5.23), so it is geometrically regular at $x$.

Conversely, if $X$ is geometrically regular, then for any point $x \in X$, $k(x)$ is f.g. over $k$, so by(4.3.9.3) there is a finite purely inseparable extension $k'/k$ that the compositum $k'k(x)$ is separable over $k'$. Then by(4.1.7.26), Spec $A \otimes_k k'$ is homeomorphic to Spec $A$, so there is a unique prime $p'$ of $X_{k'}$ over $X$, and its residue field is $k'k(x)$. So by(4.4.5.26), as $k'k(x)/k'$ is separable, $X_{k'}$ is smooth over $k'$ at $p'$. And f.f. descent for smoothness(4.4.2.1) says $X$ is also smooth over $k$ at $p$. □
Cor. (4.4.5.28) [Differential and Smoothness]. Let $k$ be a field of characteristic 0 and $S$ a f.g. algebra over $k$, and $q$ a prime ideal of $S$, if $\Omega_{S/k,q}$ is free over $S_q$, then $S$ is smooth in a nbhd of $q$.

Proof: Cf.[Sta]00TX.

Prop. (4.4.5.29) [Generic Smoothness]. Let $R \to S$ be an injective ring map of f.t. with $R,S$ domains, then it is smooth at $(0)$ iff the quotient field map is separable.

Proof: If $S$ is smooth at 0, then replacing $S$ by $S_g$ for some $g$, we can assume $R \to S$ is smooth. Then $K \to S \otimes_R K$ is also smooth(4.4.5.13), and also for any field extension $K'$ of $K$. Then $S \otimes_R K'$ is regular, by(4.4.5.23), a priori reduced(5.4.1.5). Thus $S \otimes_R K$ is geometrically reduced. Hence also $L$ is geometrically reduced over $K$, thus separable, by(4.3.9.4).

Conversely, by(4.4.1.34), we may assume $R \to S$ is of f.p., thus to show it is smooth at $(0)$, it suffices to show $S \otimes_R K$ is smooth at $(0)$, by(4.4.5.20). Then this follows from(4.4.5.26).

□

6 Unramified

Formally Unramified

Def. (4.4.6.1). A ring map $R \to S$ is called formally unramified if for every $R$-ring $A$ and an ideal $I$ of $A$ that $I^2 = 0$, a map $S \to A/I$ has at most one extension to a map $S \to A$.

Formally unramified is equivalent to $\Omega_{S/R} = 0$. So it is stable under composition by Jacobi-Zariski sequence(4.4.3.7).

Proof: Let $J = \ker(S \otimes_R S \to S)$, let $A_{univ} = S \otimes_R S/J^2$, then $J/J^2 \cong \Omega_{S/R}(4.4.3.4)$, so we have two natural maps from $S$ to $A_{univ}$, they differ by the universal differential $S \to \Omega_{S/R}$. If $S/R$ is unramified, then $ds = 0$ for all $s \in S$, so $\Omega_{S/R} = 0$.

Conversely, if there is a $A$ and $A/J$ that there are two liftings $\tau_1, \tau_2$, then we let $A_{univ} \to A$ defined by $s_1 \otimes s_2 \to \tau_1(s_1)\tau_2(s_2)$, this is well-defined, and because $A_{univ} \cong S$, this map descends to $S$, so $\tau_1(s_1s_2) = \tau_2(s_1s_2)$.

□

Prop. (4.4.6.2) [Formally Unramified Stalkwise]. Formally unramified is stalkwise both on the source and target(4.1.4.2).

Prop. (4.4.6.3). Colimits of formally unramified rings over $R$ is formally unramified. (Trivial as one renders on the diagram in the definition of formally unramified).

Unramified Map

Def. (4.4.6.4) [Unramified Maps]. A ring map is called unramified iff it is formally unramified and f.g..

A ring map is called $G$-unramified iff it is formally unramified and of f.p.. In particular, an étale map is $G$-unramified.

These two notions are stable under composition and base change. These two notions are local on the source and target. $R \to R_f$ is $G$-unramified.(4.4.6.1)(4.1.4.2)
Prop. (4.4.6.5). $R \to R/I$ is unramified, and if $I$ is f.g., then it is $G$-unramified. (Trivial).

Prop. (4.4.6.6) [Stalkwise and Fiberwise]. If $R \to S$ is of f.t.(f.p.), then it is unramified ($G$-unramified) at a prime $q$ of $S$ iff $(\Omega_{S/R})_q = 0$ iff $\Omega_{S/R} \otimes_S k(q) = 0$ iff $\Omega_{S \otimes k(p)/k(p)} \otimes k(q) = 0$.

Proof: By Nakayama, two pair of them are equivalent, and if $\Omega_{S/R,q} = 0$, then $\Omega_{S/R,g} = 0$ for some $g \notin q$ (because support of finite module is open), so $R \to S_g$ is ($G$-)unramified. And notice in fact $\Omega_{S/R} \otimes_S k(q) = \Omega_{S \otimes k(p)/k(p)} \otimes k(p) k(q)$.

Prop. (4.4.6.7) [Equivalent Definition of Unramifiedness]. A f.g. ring map $R \to S$ is unramified at a prime $q$ of $S$ over $p$ iff $pS_q = qS_q$ and $k(q)/k(p)$ is finite separable.

Proof: Suppose $R \to S_g$ is unramified, then $S \otimes k(p)$ is unramified over $k(p)$, hence by (4.4.5.23), it is also smooth, so it is étale, and (4.4.7.9) gives the result.

For the converse, Cf[Sta][02FM].

Prop. (4.4.6.8). A ring map is unramified iff it is locally a quotient of a standard étale map.

Proof: Cf.[Sta][0395].

Prop. (4.4.6.9). Any $G$-unramified map is a base change of a $G$-unramified map over a ring $R_0$ f.g. over $\mathbb{Z}$. And similarly any unramified map is a quotient of a base change of a $G$-unramified map over a ring $R_0$ f.g. over $\mathbb{Z}$.

Proof: Let $S = R[X_1,\ldots, X_n]/(g_1,\ldots, g_c)$, then we have $dX_i = \sum a_{ij}dg_j + a_{ijk}g_jdX_k$, so we let $R_0$ be generated by $g_i, a_{ij}, a_{ijk}$, so $S_0 = R_0[X_1,\ldots, X_n]/(g_1,\ldots, g_c)$ is $G$-unramified. (Trivial).

Prop. (4.4.6.10) [Unramifiedness and Idempotent]. If $R \to S$ is of f.t., then it is unramified iff $S \times_R S \to S$ is isomorphic to $S \otimes_R S \to (S \otimes_R S)_e$ for some diagonal idempotent $e \in S \otimes_R S$ that $e \ker(\mu) = 0$, i.e. $S \otimes_R S \cong S \times S'$.

Proof: If it is $G$-unramified, the kernel $I$ satisfies $I/I^2 = 0$, and $I$ is f.g. (by $x_i \otimes 1 - 1 \otimes x_i$) so we can use (4.1.7.7).

Conversely, the existence of the diagonal idempotent $e$ implies that $I = I^2$. (Trivial).

7 Étale

Formally Étale

Def. (4.4.7.1). A ring map $R \to S$ is called formally étale iff it is formally smooth and formally unramified.

Prop. (4.4.7.2). Colimits of formally étale rings over $R$ is formally étale. (The lifting are compatible because of uniqueness).

Prop. (4.4.7.3). $R \to S^{-1}R$ is formally étale.

Proof: It suffice to prove that if $\varphi(s)$ is invertible modulo $I$, then $\varphi(s)$ is invertible, but this is true because $I$ is nilpotent.
Étale Map

**Def. (4.4.7.4).** A ring map \( R \to S \) is called \( \text{étale} \) if it is of f.p. and the naive cotangent complex is exact, i.e. \( I/I^2 \cong \Omega_{P/R} \otimes_R S \).

In particular, \( \text{étale} \) is equivalent to smooth+formally unramified (\( \Omega_{R/S} = 0 \)).

**Cor. (4.4.7.5) [Properties of Étale].**
1. Étale map is stable under base change and composition.
2. Étale map is local on the source and target. In particular, \( R \to R_f \) is étale.
3. If \( R \to S \) is of f.p. and \( R \to R' \) is flat. Then the set of primes in \( S' = S \otimes_R R' \) that has a nbhd that is étale over \( R' \) is the inverse image of set of primes in \( S \) that has a nbhd that is étale over \( R \). (The same as (4.4.5.18)).
4. Étale map is syntomic, hence flat.
5. Any Étale map is a base change of an étale map over a ring \( R_0 \) f.g. over \( 
\mathbb{Z} \). (Cf. [Sta]00U2).

**Cor. (4.4.7.6) [Étale Localness of Differential].** For ring morphisms \( A \to R \to S \), if \( R \to S \) is étale, then \( \Omega_{S/A} = \Omega_{R/A} \otimes_R S \).

**Proof:** This follows from (4.4.7.4) and (4.4.5.5). \( \square \)

**Prop. (4.4.7.7) [Jacobson Criterion].** Any étale map is equivalent to a standard smooth ring map \( S = R[X_1, \ldots, X_n]/(f_1, \ldots, f_n) \) that \( J(f_1, \ldots, f_n) \) is invertible in \( S \).

**Proof:** \( I/I^2 \cong \Omega_{P/R} \otimes_R S \), so \( I/I^2 \) is free, so by (4.3.7.12), there is a presentation of \( S \) that \( f_1, \ldots, f_c \) freely generate \( I/I^2 \), then obviously \( c = n \) and \( J(f_1, \ldots, f_n) \) is invertible in \( S \), i.e. \( S \) is standard smooth. \( \square \)

**Cor. (4.4.7.8) [Example of Étale Maps].** The ring
\[
S = R[X_1, \ldots, X_n, X_{n+1}]/(f_1, \ldots, f_n, X_{n+1} \det(\frac{f_1, \ldots, f_n}{X_1, \ldots, X_n}) - 1)
\]
is étale over \( R \).

**Prop. (4.4.7.9).** If \( R \to S \) is étale at a nbhd of a prime \( q \) of \( S \) over \( p \), then \( pS_q = qS_q \), and \( k(q)/k(p) \) is finite separable.

**Proof:** We can replace \( S \) by \( S_q \) so \( S_q/R \) is étale. Then \( S \otimes k(p)/k(p) \) is étale, that is \( S_p/pS_p \) is a finite product of finite separable fields, so \( S_q/pS_q = (S_p/pS_p)_q = \text{some separable closed field}. \) \( \square \)

**Lemma (4.4.7.10).** If \( R \to S \) is an étale map and \( q \) is a prime of \( S \) over \( p \), then \( S/R \) is étale in a nbhd of \( q \) if
- \( R \to S \) is of f.p.
- \( R_p \to S_q \) is flat.
- \( pS_q = qS_q \).
- \( k(q)/k(p) \) is a finite separable field extension.

**Proof:** Cf. [Sta]00U6. \( \square \)
Prop. (4.4.7.11) [Equivalent Definition of Étale]. A ring map $R \to S$ is étale iff it is flat, of f.p. and $\Omega_{S/R}$ vanishes.

Proof: One direction is by definition, and the converse is by (4.4.7.10) and (4.4.6.7). □

Prop. (4.4.7.12). A ring map of f.p. is formally étale iff it is étale. (Because in this case, formally smooth is equivalent to smooth (4.4.5.12).)

Prop. (4.4.7.13). If $S/R$ and $S'/R$ are étale, then any $R$-algebra map $S \to S'$ is étale.

Proof: $S \to S'$ is of f.p. by (4.3.7.11), the rest Cf.[Sta]00UE.

Prop. (4.4.7.14) [Étale Algebra seen explicitly as Finite Projective Modules]. Étale algebras are finite projective, by (4.3.1.7). And we can see this clearly as follows: There is a diagonal idempotent as it is unramified (4.4.6.10), if $e = \sum a_i \otimes b_i$, then we can realize $S$ as a direct command of $R^n$ through maps

$$S \xrightarrow{\alpha} R^n \xrightarrow{\beta} S$$

where $\alpha(f) = (\text{tr}_{S/R}(fa_i))$, and $\beta(g_i) = \sum g_i b_i$.

Proof: We check that $\beta \circ \alpha = \text{id}$: Notice first that $\text{tr}_{S/S}(e) = \text{tr}_{S/S}(1) = 1$, following from the decomposition above, so $\sum \text{tr}_{S/R}(a_i)b_i = 1$, thus shows that $\beta \alpha(1) = 1$.

Now for general $f$, using the formula $(f \otimes 1)e = (1 \otimes f)e$, we get $\sum \text{tr}(fa_i)b_i = \sum \text{tr}(a_i)b_i f = f$. □

Prop. (4.4.7.15). If $R$ is a ring and $I$ is an ideal, then any étale ring map $R/I \to \overline{S}$ comes from an étale ring map $R \to S$.

Proof: Use (4.4.7.7), an étale map is of the form $\overline{S} = R/I[X_1, \ldots, X_n]/(J_1, \ldots, J_n)$ that $\delta = J(\frac{f_1}{X_1}, \ldots, \frac{f_n}{X_n})$ is invertible in $S$, then we take $S = R[X_1, \ldots, X_n, X_{n+1}]/(f_1, \ldots, f_n, X_{n+1}\delta - 1)$, then it is étale by (4.4.7.8) and maps to $\overline{S}$. □

Standard Étale

Def. (4.4.7.16). A ring map $R \to R' = R[X]/g/f$ is called standard étale iff $f$ is monic and the derivative $f'$ is invertible in $R'$.

Standard étale is stable under base change and principal localization, but not stable under composition.

Prop. (4.4.7.17) [Étale and Standard Étale]. A ring map is étale iff it is locally standard étale.

Proof: For a standard étale algebra $R[X]/g/f = R[X, Y]/(f, gY - 1)$ which is standard smooth and $\Omega_{R'/R} = 0$ (4.4.3.10), so it is étale. To prove if it is locally standard étale then it is étale, Cf.[Sta]00UE.

Prop. (4.4.7.18). Giving any ring $R$ and a prime $p$, if there is a finite separable extension $L/k(p)$, then there is a standard étale map $R \to R'$ that for some $q'$, $k(q') \cong L$ over $k$.

Proof: $L = k(p)[\alpha]$ by primitive element theorem, so the minimal polynomial of $\alpha$ is separable, and if we change $\alpha$ to $c\alpha$ for some $c \in k(p)$, we can assume $f$ can be lifted to a $f \in R[X]$. Now $f'(\alpha)$ is invertible in $L$, so there is a map from $R[X]/f/(f)$ to $L$, whose kernel gives the desired prime $q$. □
Étale over Fields

Prop. (4.4.7.19) [Étale over Fields]. An algebra over a field \( k \) is étale iff it is a finite product of finite separable extensions of \( k \).

Proof: If \( k'/k \) is finite separable, then \( k' = k(\alpha) \) for some \( \alpha \) by primitive element theorem, thus \( k' = k[X]/(f) \) that \( f' \) is invertible in \( k' \), thus it is étale by (4.4.7.7).

Conversely, Cf. [Sta]00U3.

Cor. (4.4.7.20) [Étale over Perfect Fields]. Let \( k \) be a perfect field. If \( R \) is a \( k \)-algebra that is a finite as a \( k \)-module, then it is étale over \( k \) iff it is reduced.

Proof: If it is étale, then it is reduced, by (4.4.7.19). Conversely, if it is finite and reduced, then it is a reduced Artinian ring (4.1.3.4), so a product of fields over \( k \), so étale as \( k \) is perfect.

Prop. (4.4.7.21) [Étale and Trace Form]. Let \( A \) be a f.d. \( k \)-algebra, then \( A \) is étale over \( k \) iff the trace form: \( A \times A \to k : (a,b) \mapsto \text{tr}_{A/k}(ab) \) is non-degenerate.

Proof: If it is étale, then the trace form is non-degenerate by (4.4.7.19) and (2.2.5.32). Conversely, if the trace form is non-degenerate, then \( A \) is reduced, because if \( a \in A \) is nilpotent, then \( ab \) are nilpotent for any \( b \in A \), and \( \text{tr}_{A/k}(ab) = 0 \). Then as a reduced Artinian ring, \( A \) is isomorphic to a product of fields, then by (2.2.5.32), all the fields are separable over \( k \).

Prop. (4.4.7.22) [Étale and Unramified over Fields]. For \( k \in \text{Field} \), a f.g. \( k \)-algebra is étale iff it is \((G-)\)unramified over \( k \), by (4.4.5.23).

Prop. (4.4.7.23) [Maximal Étale Subalgebra]. Let \( A \) be an algebra of f.t. over a field \( k \), then there is a maximal étale \( k \)-subalgebra of \( A \). Also this subalgebra commutes with arbitrary field base change.

Proof: If \( R \) is an étale subalgebra of \( A \), then \( R_{\overline{k}} \) is étale over \( \overline{k} \), thus isomorphic to \((\overline{k})^n \) for some \( n \). Now \( n \) is smaller than the number of connected components of \( \text{Spec } A_{\overline{k}} \), which is finite. So it suffices to show the composite of two étale subalgebras of \( A \) is étale. For this, notice \( RR' \) is a quotient of \( R \otimes_k R' \), which is a finite product of finite separable fields over \( k \), thus its quotient is also a finite product of finite separable fields over \( k \), which is étale.

8 Local Algebras

Main references are [Local Algebra, Serre].

Prop. (4.4.8.1). If \( A \) is a Noetherian local integral domain with residue field \( k \) and quotient field \( K \), if \( M \) is a f.g. \( A \)-module that \( \dim_k M \otimes_A k = \dim_K M \otimes_A K = r \), then \( M \) is free of rank \( r \).

In other words, if the rank of \( M \) at the generic point and closed pt of \( B \) are the same, then \( M \) is free.

Proof: First \( M \) is generated by \( r \) elements by Nakayama and the kernel \( R \) of \( A^r \to M \) vanishes when tensoring \( K \), thus vanish because it is torsion-free.

Prop. (4.4.8.2). Let \( A \to B \) be a local ring map of local rings that

- \( B \) is finite as an \( A \)-module.
• $m_B$ is a f.g. ideal.
• $A/m_A \cong B/m_B$.
• $m_A/m_A^2 \cong m_B/m_B^2$.
Then $A \to B$ is surjective.

Proof: By Nakayama, to show it is surjective, it suffices to show $A/m_A \to B/m_A B$ is surjective, then it suffices to show $m_A \otimes_A B \to m_B$ is surjective. For this, use Nakayama again on $B$ to reduce to the fact $m_A \otimes_A B/m_B \to m_B \otimes B/m_B$ is surjective, which is satisfied because this is just $m_A/m_A^2 \to m_B/m_B^2$. □
4.5 \( p \)-adic Commutative Algebras

1 \( \mathbb{F}_p \)-Algebras

Def.(4.5.1.1)[relative Frobenius]. Let \( S \to R \) be a ring map, then the relative Frobenius \( \varphi_{R/S} \) is the map \( R \otimes_{S, \text{Frob}} S \to R \) induced by universal property.

Def.(4.5.1.2)[Perfect Rings]. A ring of characteristic \( p \) is called perfect iff the Frobenius \( \text{Frob}/\varphi : P \to P \) is an isomorphism. It is called semi-perfect iff Frob is surjective.

Prop.(4.5.1.3)[Perfection and Coperfection]. If \( R \) is of char \( p \), we define \( R_{\text{perf}} \) and \( R_{\text{coperf}} \) are perfect: for \( R_{\text{perf}} \) every element in \( R_{\text{perf}} \) is represented by an element \( a_n \in R_n \), and this element is equivalent to \( a_n^p \in R_{n+1} \), so its \( p \)-th root is \( a_n \in R_{n+1} \). For \( R_{\text{coperf}} \), an element \( (\ldots, x_n, \ldots, x_0) \) has \( p \)-th root \( (\ldots, x_{n+1}, \ldots, x_1) \).

In particular, the category of perfect rings admits limits and colimits, and it equals the limits and colimits in the category of rings.

Proof: First both \( R_{\text{perf}} \) and \( R_{\text{coperf}} \) are perfect: for \( R_{\text{perf}} \) every element in \( R_{\text{perf}} \) is represented by an element \( a_n \in R_n \), and this element is equivalent to \( a_n^p \in R_{n+1} \), so its \( p \)-th root is \( a_n \in R_{n+1} \). For \( R_{\text{coperf}} \), an element \( (\ldots, x_n, \ldots, x_0) \) has \( p \)-th root \( (\ldots, x_{n+1}, \ldots, x_1) \).

Second it is easily checked to be a functor because Frobenius is natural. The universal property is easy. □

Prop.(4.5.1.4)[Perfection Kills Nilextensions]. If \( f : R \to S \) is a map of rings of characteristic \( p \) that is surjective with nilpotent kernel, then \( R_{\text{perf}} \to S_{\text{perf}} \) and \( R_{\text{coperf}} \to S_{\text{coperf}} \) are both isomorphisms.

Proof: \( R_{\text{perf}} \) map is clearly surjective, and it is injective because if \( a \) maps to 0, then Frobenius \( \text{Frob}^k(a) \in \ker f \) for some \( k \), so it is nilpotent, so Frobenius \( \text{Frob}^{k+n}(a) = 0 \).

\( R_{\text{coperf}} \) is clearly injective, and it is surjective because: suppose \( \ker f^n = 0 \), then for \( a_n \in S \), let \( t_m \) be the inverse image of \( s_m \), for each \( m \), and let \( x = (x_n), x_{m-n} = \text{Frob}_m t_m \), then \( x \in R_{\text{coperf}} \) and \( x \) maps to \( s \).

Prop.(4.5.1.5)[Examples of Tilting].

- \( \mathbb{F}_p[[t]]_{\text{perf}} = \mathbb{F}_p[t^{1/p}] \), \( \mathbb{F}_p[[t]]_{\text{coperf}} = \mathbb{F}_p \).
- \( \mathbb{Z}_p^* \to \mathbb{Z}_p \).
- If \( R \) is a perfect ring of char \( p \) and \( f \in R \) is a non-zero divisor, then \( (R/f)_{\text{perf}} \) is the \( f \)-adic completion of \( R \). In particular, \( (\mathbb{F}_p[[t^{1/p}]]/(t))_{\text{perf}} \equiv \mathbb{F}_p[[t^{1/p}]] \).
- \( (\mathbb{Z}_p[[t^{1/p}]]_{\text{perf}} \equiv \mathbb{F}_p[[t^{1/p}]] \equiv \mathbb{F}_p[[t]_{\text{perf}}] \equiv (\mathbb{F}_p[[t]]/(t))_{\text{perf}} \).

Proof: The first two are trivial, for the third, notice \( \hat{R}_f = \lim_n R/f^n = \lim_n R/f^n \), and there are commutative diagram

\[
\begin{array}{ccc}
R/f & \xrightarrow{\varphi} & R/f \\
\downarrow{\varphi^{k+1}} & & \downarrow{\varphi^k} \\
R/fp^{k+1} & \xrightarrow{i} & R/fp^k
\end{array}
\]

so \( \lim_n R/f^n \equiv (R/f)_{\text{perf}} \).
For the fourth, only the first equivalence needs proving, the others are consequences of the first three items. Then notice

\[(\mathbb{Z}_p[p^{1/\infty}])^\flat \cong \lim_{\leftarrow}(\mathbb{Z}_p[p^{1/\infty}]/p^k)^{\text{perf}} \cong \left(\mathbb{Z}_p[p^{1/\infty}]/p\right)^{\text{perf}} \cong (F_p[t^{1/\infty}]/t)^{\text{perf}} \cong F_p[t^{1/\infty}].\]

The last isomorphism by item 3.

\[\square\]

Def. (4.5.1.6) [Perfectly Finitely Presented]. A map of perfect \(F_p\)-algebras \(B \to A\) are called perfectly finitely presented if \(A = (A_0)_{\text{per}}\) for some \(f.p.\ \)\(B\)-algebra \(A_0\).

Prop. (4.5.1.7) [Aberbach-Hochster]. Let \(R\) be a perfect \(F_p\)-algebra, \(f_1, \ldots, f_r \in R\), and consider the ideal \(I = \sqrt{(f_1, \ldots, f_r)} \in R\). Then \(R\downarrow I\) has flat dimension \(\leq r\) as an \(R\)-module.

Proof: We only prove for \(r = 1\).

We show \(I = \lim_{\leftarrow} f_1^{p^{n-1}/p^{n+1}} R\). The map is given by \((a_n) \mapsto f_1^{p^n} a_n\). This is injective because if \(f_1^{p^n} a = 0\), then \(f_1^{p^{n+1}} a = 0\) by perfectness, thus \(a\) is killed by the transition map \(f_1^{p^{n-1}/p^{n+1}}\).

\[\square\]

Prop. (4.5.1.8) [Perfect Algebras are Tor Independent]. For any two perfect \(A\)-algebras \(B, C\) where \(A\) is a perfect \(F_p\)-algebra, \(\text{Tor}_i^A(B, C) = 0\) for \(i > 0\).

Proof: \(A \to B\) can be written as a composition of a perfection of a free \(A\)-algebra and a quotient. The perfection of free algebra is flat, thus we can assume \(B = A/I\). By a filtered colimit argument again, we can assume \(I = (f_1^{1/\infty}, \ldots, f_r^{1/\infty})\) is perfectly f.p. By induction, we can assume \(r = 1\). Now the lemma (4.5.1.7) applied to \(R = C\) shows that \(IC = \lim_{\leftarrow} f_1^{p^n-1/p^{n+1}} C = I \otimes_A^L C\), so \(B \otimes_A^L C = C/IC\) is discrete.

\[\square\]

Prop. (4.5.1.9). If \(R\) is a perfect \(F_p\)-algebra, \(I\) is a radical ideal, and \(J = R[I] \subset R\), then \(J\) and \(I + J\) are both radical, and the square

\[
\begin{array}{ccc}
R & \longrightarrow & R/I \\
\downarrow & & \downarrow \\
R/J & \longrightarrow & R/I + J
\end{array}
\]

is both a fiber pullback and pushout square of commutative rings.

Proof: \(J\) is clearly a radical, and notice that \(I + J\) is the kernel of the map \(R \to R/I \otimes_R R/J = R/I + J\) (4.1.1.22), and the target is a colimit of perfect rings thus perfect, by (4.5.1.3). Thus \(I + J\) is also perfect, thus a radical ideal.

By (4.1.1.23), to show the map is a pullback square, it suffices to show that \(I \cap J = 0\). If \(x \in I \cap J\), then \(x^2 = 0\), thus \(x^p = 0\), so \(x = 0\).

\[\square\]

Tilting

Def. (4.5.1.10) [Tilting]. For any ring \(R\), let the tilting of \(R\) be defined to be \(R^\flat = (R/p)^{\text{perf}}\), endowed with the profinite topology.

Prop. (4.5.1.11). If \(R\) is a f.g. algebra over an alg. closed field \(k\) of char \(p\), then \(R^\flat \cong k^{\pi_0(\text{Spec } R)}\).
Proof: It suffice to prove for Spec $R$ connected and reduced, because by (4.5.1.4). We first prove the case Spec $R$ is irreducible, i.e. $R$ is integral:

In this case, choose a closed point $x$, then there is a map $R \to \hat{R}_x$, where $\hat{R}_x$ is the $\mathfrak{m}_x$-adic completion. By Krull(4.2.2.15) and the fact $R$ is integral, this map is injective, so it suffices to show that $0 = (\hat{R}_x)_{\text{perf}} = \lim_{\to}(R_x/\mathfrak{m}_x^n)_{\text{perf}}$. But $(-)_{\text{perf}}$ is a right adjoint so commutes with colimits and $\hat{R}_x = \lim_{\to} R_x/\mathfrak{m}_x^n$. But $(R_x/\mathfrak{m}_x^n)_{\text{perf}} = (R_x/\mathfrak{m}_x)_{\text{perf}} = k_{\text{perf}} = k$, by (4.5.1.4) again.

If $R$ is not irreducible,?

Prop.(4.5.1.12). If $R$ is a $p$-adically complete commutative ring, $\pi \in \text{rad}(p)$, then the map $R \to R/p$ induces an homeomorphism of monoids:

$$\lim_{\to} x \mapsto x^p \equiv \lim_{\to} R/\pi \equiv \lim_{\to} R/p(4.5.1.4) = R^p$$

Proof: Injectivity: if $(a_n), (b_n) \in \lim_{\to} x \mapsto x^p R$ satisfies $a_n \equiv b_n \mod \pi$ for all $n$, then applying power lifting(20.1.2.8), $a_n \equiv b_n \mod \pi^{n+k}$ for all $k$, so $a_n = b_n$.

Surjectivity: for $(\bar{a}_n) \in R^p$, choose arbitrary lifting $a_n$, then $a_n^{p+k} \equiv a_n+k \mod \pi$ for all $n+k$, so $k \mapsto a_n^{p+k}$ is a Cauchy sequence by power lifting(20.1.2.8) again, thus converging to some point $b_n$. then it’s easily checked that $b_n = (\lim_{\to} a_n^{p+k})^p = \lim_{\to} a_n^{p+k+1} = b_n$. so $(b_n)$ maps to $(\bar{a}_n)$.

For the topology: it is clearly continuous, and for the reverse, if $(a_i), (b_i)$ satisfies that $a_i \equiv b_i \mod \pi$ for $i < k$, then the image in $\lim_{\to} x \mapsto x^p R$ satisfies $x_i \equiv y_i \mod p^{k-i}$ for $i < k$, thus it is open.

Cor. (4.5.1.13)[Sharp Map]. From this proposition, we get a multiplicative sharp map: $\sharp: R^p \to R$, and its image is just the elements that has a compatible system of $p$-th roots $x^{1/p}$. These elements are also called perfect.

Cor. (4.5.1.14) [Addition in $R^p$]. From the isomorphism(4.5.1.12) above, we can read what the addition looks like in the presentation $\lim_{\to} x \mapsto x^p R$: if $(f_n), (g_n)$ are two elements, then their addition is given by $(h_n)$, where $h_n = \lim_{\to} (f_n + g_n)^{p^k}$.

Cor. (4.5.1.15) [Fontaine’s Map]. By (8.2.4.4), the natural map $R^p \to R/\pi$ induces a map $\theta_R : W(R^p) \to R$ of rings, called the Fontaine’s functor, which writes as $\sum [a_i] p^i \mapsto \sum a_i^\flat p^i$. And we denote $A_{\text{inf}}(R) = W(R^p)$ the Fontaine’s ring of $R$.

Prop. (4.5.1.16). Fontaine’s map $\theta_R$ is surjective iff $R/p$ is semiperfect.

Proof: By Nakayama, $\theta$ is surjective iff it is surjective modulo $o$. Because its reduction mod $p$ is $R^p \to R/p$ is surjective as $\varphi : R/p \to R/p$ does.

Prop.(4.5.1.17)[ Tilting as a Valuation Ring]. If $R$ is a domain or a valuation ring, then the same is true for $R^p$. In the valuation case, the valuation of $R^p$ can in fact be chosen to be $| \cdot | \circ \sharp$, so in particular, the rank of $R^p$ is no more than the rank of $R$.

Proof: Use the isomorphism $\lim_{\to} x \mapsto x^p R \equiv \lim_{\to} x \mapsto x^p R/p = R^p(4.5.1.12)$.

For the domain case, if $(a_n)(b_n) = 0$, then $a_nb_n = 0$, so $a_0 = 0$ or $b_0 = 0$, so $(a_n) = 0$ or $(b_n) = 0$. Similarly, if $R$ is a valuation ring, then $R^p$ is firstly a domain, and it suffices to prove that for any $(a_n), (b_n) \in R^p$, the quotient of one by another is in $R^p$, by (10.3.2.3). For this, because $R$ is
valuation ring, we may assume \( a_0/b_0 \in R \), so \( a_n/b_n \) is also in \( R \), because their power do, and \( R \) is normal\(^{\text{(10.3.2.6)}} \), thus \( (a_n)/(b_n) \in R^\flat \).

For the valuation given, notice in the above proof, \(|(a_n)| \leq |(b_n)|\) iff \(|a_0| \leq |b_0|\), so the valuation are equivalent to \(|\cdot| \circ \sharp\) by\(^{\text{(10.3.3.14)}} \), so it can be chosen to be so. \(\square\)

**Prop.(4.5.1.18)**[Tilting and Completion]. If \( R = A/I \) with \( A/p \) perfect, then \( R^\flat \) identifies with the \( I \)-adic completion of \( A/p \).

*Proof:* \( R^\flat = \varprojlim R/p = \varprojlim A/(p, I) \). But there are commutative diagrams

\[
\begin{array}{ccc}
A/(p, I) & \xrightarrow{\varphi} & A/(p, I) \\
\downarrow^{\varphi^{n+1}} & & \downarrow^{\varphi^n} \\
A/(p, I^{p^{n+1}}) & \xrightarrow{\phi^n} & A/(p, I^p)
\end{array}
\]

where the vertical arrows are isomorphisms because \( A/p \) is perfect. So the conclusion follows. \(\square\)

2 **\( p \)-Local Rings**

**Def.(4.5.2.1)**[\( p \)-Local Rings]. A commutative ring is called \( p \)-local if \( p \in \text{rad} \ A \).

**Prop.(4.5.2.2).** Let \( A \) be a \( p \)-adically complete ring, then \( A \) is \( p \)-local, by\(^{\text{(4.2.3.18)}} \).

**Prop.(4.5.2.3).** If \( A \) is \( p \)-adically complete and has bounded \( p \)-torsions, the \( p \)-completion of a smooth \( A \)-algebra is \( p \)-completely smooth.

*Proof:* This follows from\(^{\text{(4.6.7.4)}} \) and\(^{\text{(4.6.6.16)}} \). \(\square\)

**Def.(4.5.2.4)**[\( p \)-Normal Rings]. A \( p \)-torsion-free ring \( R \) is called \( p \)-normal if \( R \) is \( p \)-root closed in \( R[z]/z \).

**Complete Discrete Valuation Rings**

Structure of complete \( p \)-local DVRs will be studied in this subsubsection.

Main references are \([\text{Ser79}]\), [Integral \( p \)-adic Hodge, BMS].

**Def.(4.5.2.5)**[Strict \( p \)-Ring]. A \( p \)-ring \( A \) is a ring which is complete Hausdorff in the topology defined by the decreasing chain of ideals \( \alpha_1 \supset \alpha_2 \supset \cdots \) such that \( \alpha_m \alpha_n \subset \alpha_{m+n} \) that \( k = A/\alpha_1 \) is a perfect ring of characteristic \( p \).

It is called a **strict \( p \)-ring** if moreover \( \alpha_n = (p^n) \) and \( p \) is a non-zero divisor of \( A \).

**Prop.(4.5.2.6)**[Teichmüller Lifts]. For a \( p \)-ring, there exists a unique section map \( [\cdot] : k \rightarrow A \) that is multiplicative, called the **Teichmüller lifts**.

If char \( A = p \), then the Teichmüller lift is also additive (but not in general). And an element is in the image of \( f \) iff it is a \( p^n \)-th power for any \( n \).

*Proof:* For any \( \lambda \in k \), the \( \lambda^{p^n} - \lambda \) is unique in \( k \), and if we consider \( U_n \) the set of all \( x^{p^n} \) where \( x \) is a lift of \( \lambda^{p^n} - \lambda \), then \( U_n \) is a descending set. Moreover, the diameter converges to 0, because \( a \equiv b \mod \alpha_1 \) implies \( a^{p^n} \equiv b^{p^n} \mod \alpha_{n+1} \) as \( p \in \alpha_1 \). So it converges to a unique point \( f(\lambda) \) in \( A \). And we see that any other \( f' \) maps \( \lambda \) to a \( p^n \)-th root hence in \( U_n \) for any \( n \), hence it map be equal to \( f(\lambda) \). The rest is easy. \(\square\)
Cor. (4.5.2.7) [Equal Characteristic case]. If \( A \) is a complete discrete valuation ring with residue field \( k \). If \( k \) and \( A \) have the same characteristic and \( k \) is perfect, then \( A \cong k[[T]] \).

Def. (4.5.2.8) [(0, \( p \))-type case]. When \( A \) is a complete DVR with residue field \( k \) and quotient field \( K \). If \( \text{char}K = 0 \) and \( \text{char}k = p \), then \( p \) goes to 0 in \( k \), so \( e = v(p) \geq 1 \), called the absolute ramification index of \( A \). It is called absolutely unramified iff \( e = 1 \).

Remark (4.5.2.9) [Universal Strict \( p \)-Ring]. The canonical strict \( p \)-ring is the ring \( \hat{S} = \hat{\mathbb{Z}}[X_i^{p^{-n}}] \). Its residue ring is \( \mathbb{F}_p[X_i^{p^{-n}}] \) which is perfect. \( X_i \) are all Teichmüller lifts, as they all has \( p^i \) roots.

Now we consider the \( * = + - \times \) in \( \hat{S} \). Then there are elements \( Q_i^* \in \mathbb{F}_p[X_i^{p^{-n}}, Y_i^{p^{-n}}] \) that \( x * y = \sum f(Q_i^*)p^i \) where \( f \) is the Teichmüller lift.

Prop. (4.5.2.10) [Universal Law of \( p \)-Rings]. For any \( p \)-ring \( A \) with residue ring \( k \), the calculation in \( A \) is dominated by \( Q_i^* \) defined in (4.5.2.9), i.e.

\[
\left( \sum f(\alpha_i)p^i \right) * \left( \sum f(\beta_i)p^i \right) = \sum f(\gamma_i)p^i
\]

where \( \gamma_i = Q_i^*(\alpha_0, \alpha_1, \ldots, \beta_0, \beta_1, \ldots) \).

Proof: There is a map \( \theta \) from \( \hat{S} = \hat{\mathbb{Z}}[X_i^{p^{-n}}, Y_i^{p^{-n}}] \) to \( A \) induced by \( f(\alpha_i), f(\beta_i) \) as they all has \( p^{-n} \)-th roots. Then notice \( \theta \) induce a \( \bar{\theta} \) on residue ring and these two \( \theta \) commutes with Teichmüller lift, as seen by the definition of the latter. Then the theorem follows immediately.

Prop. (4.5.2.11) [Universal Properties of Strict \( p \)-Rings]. For two \( p \)-ring \( A, A' \) that \( A \) is strict, then any map \( \varphi \) of their residue ring induces a unique ring homomorphism \( A \to A' \). In particular, two strict \( p \)-ring with the same residue ring is canonically isomorphic.

Proof: We have already seen that ring homomorphism commutes with Teichmüller lift. Now we define

\[
g(a) = \sum g(f(\alpha_i))p^i = \sum f(\varphi(\alpha_i))p^i
\]

and this is the unique choice. It is a ring homomorphism by universal law of (4.5.2.10).

3 Witt Theory

References are [Michiel Hazewinkel, Formal Groups and Applications] and [Rab14].

Witt Vectors

Def. (4.5.3.1) [Divisor Stable Subsets]. A non-empty subset \( P \subset \mathbb{Z}_+ \) is called divisor-stable if it is stable under taking divisors.

For a divisor-stable subset \( P \) and \( n \in \mathbb{Z}_+ \), define \( P(n) = \{ m \in P | m \leq n \} \).

Def. (4.5.3.2) [Witt Polynomials]. For \( n \in \mathbb{N} \), the \( n \)-th Witt polynomial is defined to be

\[
W_n = \sum_{d|n} dX_d^{n/d} \in \mathbb{Z}[[X_d : d|n]].
\]

For example,

\[
W_{p^k} = X_1^{p^k} + pX_{p^{k-1}} + \ldots + p^nX_p.
\]
Prop. (4.5.3.3) [Commutative Coalgebra $\Delta_P$]. For a divisor-stable set $P$, let $\Delta_P = \mathbb{Z}[[X_n | n \in P]]$, then there is a unique commutative ring scheme structure on $\text{Spec} \Delta_P$ s.t. the map

$$W_* : \mathbb{Z}[X_P] \to \Delta_P : n \mapsto W_n \in \Delta_P$$

induces a homomorphism of ring schemes $\text{Spec} \Delta_P \to \text{Spec} \mathbb{Z}[X_P]$, where the ring structure on $\text{Spec} \mathbb{Z}[X_P]$ is given by

$$\times : \mathbb{Z}[X_P] \to \mathbb{Z}[X_P] \otimes \mathbb{Z}[Y_P] : X_n \mapsto X_n \otimes Y_n, \quad + : \mathbb{Z}[X_P] \to \mathbb{Z}[X_P] \otimes \mathbb{Z}[Y_P] : X_n \mapsto X_n \otimes 1 + 1 \otimes Y_n.$$

Then for another divisor-stable set $P' \subset P$, there is a natural map $\Delta_{P'} \to \Delta_P$ that induces a homomorphism of ring schemes.

If $P = \mathbb{Z}_+$, denote $\Delta_P = \Delta$, if $P = \{1, p, p^2, \ldots\}$, denote $\Delta_P = \Delta_p$, and if $P = \{1, p, \ldots, p^k\}$, denote $\Delta_P = \Delta_{p,k}$.

Proof:

Cor. (4.5.3.4). $S_n$ is of the form $S_n(X_P, Y_P) = X_n + Y_n + f_n(X_{P(n-1)}, Y_{P(n-1)})$.

Proof:

Def. (4.5.3.5) [Witt Vectors]. For a divisor-stable set $P$, consider the functor

$$W_P : \mathcal{C}_{\text{Alg}} \to \mathcal{C}_{\text{Alg}} : A \mapsto W_P(A) = \text{Hom}(\Delta_P, A),$$

then it is an exact functor, and by (4.5.3.3), there are natural ring homomorphism

$$W_* : W_P(A) \to \prod_P A : f \mapsto (f(W_n))_W$$

For $x \in W_P(A)$, $W_n(x)$ are called the ghost components of $x$, and $W_* (x)$ is called the Witt coordinate of $x$.

If $P = \mathbb{Z}_+$, $W_P(A)$ is denoted by $W(A)$, if $P = \{1, p, p^2, \ldots\}$, $W_P(A)$ is denoted by $W_p(A)$, and if $P = \{1, p, \ldots, p^k\}$, denote $W_P(A) = W_{p,k}(A)$.

Prop. (4.5.3.6) [Natural Coordinates]. There is another map

$$\varphi_* : W_P(A) \to \prod_P A : f \mapsto (f(X_i))$$

which is an isomorphism of sets, whose components are maps of sets $\varphi_n : W_P(A) \to A, n \in P$. WARNING: it is not an isomorphism of groups. For $x \in W_P(A)$, $\varphi_n(x)$ are called the ghost components of $x$, and $\varphi_*(x)$ is called the Witt coordinate of $x$. All coordinates of elements in $x$ will be assumed to be in the natural coordinates by default.

Then the map $W_* \varphi^{-1}_*$ is given by

$$W_* \varphi^{-1}_* : \prod_P A \to \prod_P A : (x_n)_\varphi \mapsto (W_n(\{x_P\}))_W.$$

Cor. (4.5.3.7) [Witt Coordinates are Injective]. $W_* : W_P(A) \to \prod_P A$ is injective if $A$ is $n$-torsion-free for any $n \in P$, and an isomorphism iff $n$ is invertible in $A$ for any $n \in P$.

This is very useful because it can prove equations by checking on each $W_n$. Also when checking universal equations, it is even not necessary that $A$ is $n$-torsion-free, because any ring $A$ is a quotient of a free $\mathbb{Z}$-algebra.
4.5. P-ADIC COMMUTATIVE ALGEBRAS

Proof: It suffices to prove for $W_s\varphi^{-1}_s$. Using the Witt polynomials and prove inductive on $n \in P$ s.t. if $x = (x_n)$ is mapped to 0, then $x_n = 0$ for any $n \in P$.

In case $n$ is invertible in $A$ for any $n \in P$, solve $x_n$ out of $W_s(x)$ inductively. 

**Def. (4.5.3.8) [Topology on $W_P(A)$].** Let $P$ be a divisor-stable set, then for any $A \in \mathcal{C}Alg$, the natural map

$$W_P(A) \to \lim_{n \in \mathbb{Z}^+} W_P(n)(A)$$

is an isomorphism of rings, so we can define the **natural topology** on $W_P(A)$ is as the profinite topology.

Then this topology makes $W_P(A)$ a topological ring, and it is discrete iff $\# P < \infty$, and $W_P$ is a functor from $\mathcal{C}Alg$ to the category of profinite rings.

**Prop. (4.5.3.9).** Let $P$ be a divisor-stable set and $A \in \mathcal{C}Alg$, then for $x = (x_n)$, $y = (y_n) \in W_P(A)$, if $x_n y_n = 0$ for any $n \in P$, then

$$x + y = (x_n + y_n) \in W_P(A).$$

**Proof:** It suffices to prove on $\Delta_P$. By (4.5.3.7), it suffices to prove $W_n((x_n + y_n)) = W_n(x) + W_n(y)$ for any $n \in P$. This is true because

$$W_n((x_n + y_n)) = \sum_{d|n} d(x_d + y_d)^{n/d} = \sum_{d|n} dx_d^{n/d} + \sum_{d|n} dy_d^{n/d} = W_n(x) + W_n(y).$$

**Prop. (4.5.3.10) [Teichmüller Lifts].** Let $P$ be a divisor-stable set and $A \in \mathcal{C}Alg$, for $a \in A$, denote $[a] = (a, 0, \ldots) \in W_P(A)$. Then for any $x = (x_n) \in W_P(A),$

$$[a]x = (a^n x_n).$$

In particular, $[\cdot] : A \to W_P(A)$ is multiplicative, called the **Teichmüller lifts** of $A$.

**Proof:** It suffices to prove on $\Delta_P$. By (4.5.3.7), it suffices to prove $W_n((a^n x_n)) = W_n([a]x)$ for any $n \in P$. This is because

$$W_n((a^n x_n)) = \sum_{d|n} d(a^d x_d)^{n/d} = a^n \sum_{d|n} dx_d^{n/d} = W_n([a]x) W_n(x) = W_n([a]x).$$

**Frobenius and Verschiebung Maps**

**Def. (4.5.3.11) [Verschiebung Maps].**

**Def. (4.5.3.12) [Frobenius Maps].**

**Prop. (4.5.3.13) [Frobenius and Verschiebung].** Let $n \in \mathbb{Z}_+$ and $P$ is a divisor-stable subset s.t. $nP \subset P$. Let $A \in \mathcal{C}Alg$, let $x, y \in W_P(A)$,

- $F_n \circ V_n = n \cdot \text{id}$,
- $V_n(F_n(x)y) = xV_n(y)$,
- If $(m, n) = 1$, then $V_m \circ F_n = F_n \circ V_m$,
- For $m \in \mathbb{Z}_+$, $(V_n(x))^m = n^{m-1}V_n(x^m)$.

**Proof:** Cf. [Rab14] P18.
\textbf{Prop.(4.5.3.14)[Structure of }\Delta_{p}\text{]}\text{. The ring structure on }\text{Spec }\Delta_{p}\text{ is given by}

\[\times : \Delta_{p} \rightarrow \Delta_{p} \otimes \Delta_{p} : X_{p}^{k} \mapsto S_{k}(X_{F}, Y_{P}), \quad + : \Delta_{p} \rightarrow \Delta_{p} \otimes \Delta_{p} : X_{p}^{k} \mapsto Z_{k}(X_{F}, Y_{P})\]

where

\[S_{1} = X_{1} + Y_{1}, \quad S_{2} = X_{p} + Y_{p} + \sum_{i=1}^{p-1} \frac{1}{p} \binom{p}{i} X_{1}^{i} Y_{1}^{p-i},\]
\[Z_{1} = X_{1} Y_{1}, \quad Z_{2} = X_{p}^{p} Y_{p} + X_{p} Y_{p}^{p} + p X_{p} Y_{p}.\]

\textit{Proof:} \[\] 

\textbf{Cor.(4.5.3.15)[W2]}\text{. Let }W_{2} = W_{P}\text{ where }P = \{1, p\}\text{, then }W_{2}(A)\text{ is the set }A \times A\text{(as the natural coordinates) with the addition and multiplication given by}

\[(x_{0}, x_{1}) + (y_{0}, y_{1}) = (x_{0} + y_{0}, x_{1} + y_{1} + \frac{x_{0}^{p} + y_{0}^{p} - (x_{0} + y_{0})^{p}}{p}), \quad (x_{0}, x_{1})(y_{0}, y_{1}) = (x_{0} y_{0}, x_{0}^{p} y_{1} + y_{0}^{p} x_{1} + p x_{1} y_{1})\]

There are two natural morphism of rings \(\varepsilon_{1}, \varepsilon_{2} : W_{2}(A) \rightarrow A:\)

\[\varepsilon_{1}((x_{0}, x_{1})) = x_{0}, \quad \varepsilon_{2}((x_{0}, x_{1})) = x_{0}^{p} + p x_{1}.\]

\textbf{Prop.(4.5.3.16). For }k \geq 1\text{ and }A \in \mathbb{C}Alg,\text{ the kernel of }W_{1} : W_{p,k}(A) \rightarrow A\text{ is a nilpotent ideal.}

\textit{Proof:} \[\text{Cf.[Basic Algebra 2, Jacobson]P508.}\]

\textbf{Cor.(4.5.3.17). An element }x \in W_{p,k}(A)\text{ is a unit iff }W_{1}(x) \in A\text{ is a unit.}

\textbf{Example(4.5.3.18)[}p\text{-Typical Witt Vectors].}

\begin{itemize}
  \item \(W_{p}(\mathbb{F}_{q})\text{ is the unramified extension of }\mathbb{Z}_{p}\text{ of degree }\log_{p} q.\)
  \item \(W_{p}(\mathbb{F}_{p})\text{ is the completion of the maximal unramified extension of }W_{p}(\mathbb{F}_{p}).\)
\end{itemize}

\textit{Proof:} \[\]

\textbf{Lemma(4.5.3.19)[Formula for }p\text{-Rings]. For }* = + \text{ or }\times\text{, there are integral polynomials }S_{*}(X_{i}, Y_{i})\text{ that}

\[\left(\sum f(\alpha_{i})p^{i}\right) * \left(\sum f(\beta_{i})p^{i}\right) = \sum f(\gamma_{i})p^{i}\]

where \(\gamma_{i} = Q_{i}^{*}(\alpha_{0}, \alpha_{1}, \ldots, \beta_{0}, \beta_{1}, \ldots).\) And for \(+\), when reduced to \(\mathbb{F}_{p}\), \(Q_{i}^{+}\) are polynomials in \(X_{i}^{p-n}, Y_{i}^{p-n}\) for \(i \leq n\) and homogenous of degree 1. And

\[Q_{i}^{+} = (X_{n} + Y_{n}) + (X_{n-1}^{p-1} + Y_{n-1}^{p-1}) R_{n,n-1} + \ldots + (X_{0}^{p-n} + Y_{0}^{p-n}) R_{n,0}.\]

\textit{Proof:} \[\text{We solve }S_{n}\text{ by induction. Notice for any lift }\tilde{S}_{i}\text{ of }S_{i},\]

\[f(S_{i}) \equiv \tilde{S}_{i}(X^{1/p^{n-i}}, Y^{1/p^{n-i}})p^{n-i} \mod p^{n-i+1}\]

so we mod \(p^{n+1}\) to solve \(S_{n}:\)

\[S_{n} \equiv 1/p^{n}(X_{0} + Y_{0} + \ldots + p^{n}X_{n} + p^{n}Y_{n} - \tilde{S}_{0}(X^{1/p^{n}}, Y^{1/p^{n}})p^{n} - \ldots - p^{n-1}\tilde{S}_{n-1}(X^{1/p}, Y^{1/p})p^{n}).\]

The rest follows by induction. \[\]
Lemma (4.5.3.20). If $k$ is a perfect field of characteristic $p$ and $R$ is a strict $p$-ring with residue field $k$, then the map

$$f : W_p(k) \to R : (x_1, x_2, x_3, \ldots) \mapsto \sum_{n=0}^{\infty} [x_{p^n}] p^n$$

is an isomorphism of topological rings.

*Proof:* We need to prove this is a ring homomorphism. That on $W(A)$ is to make $\varphi$ a ring homomorphism, and that on the right is usual. It suffice to prove for the canonical strict $p$-ring, as seen by the universal law (4.5.2.10).

For this, we let $(\sum X_i^{p^i} \cdot p^i) \ast (\sum Y_i^{p^i} \cdot p^i) = \sum f(\psi_i(X_i, Y_i)) p_i \cdot p^i$, and $W_n(a_i) \ast W_n(b_i) = W_n(\varphi_i)$, where $\psi_i \in F_p[X_i, Y_i]$ and $\varphi_i \in Z[X_i, Y_i]$, they both exist, the latter because of (4.5.4.7).

Then we mod $p^{n+1}$, and let $X_i = Y_i^{p^n}$, so $W_n(\varphi_i) = W_n(X_i) \ast W_n(Y_i) = \sum f(\psi_i(X_i^{p^n}, Y_i^{p^n})) p_i \cdot p^i = W_n(\psi_i)$ mod $p^{n+1}$

Now induction, $\varphi_i \equiv \psi_i$ mod $p$, then $p^n \varphi_n \equiv p^n \psi_n$ mod $p^{n+1}$ so this is true for $n$, too.

Cf. [Rab14] P8, 20. 

\[ \square \]

Prop. (4.5.3.21) [Witt $p$ For Perfect Rings]. For any perfect ring $k$ of char $p$, there exists uniquely a strict $p$-ring $W(k)$ that has residue ring $k$, which is just the ring of Witt vectors $W_p(k)$.

Then $W_p$ is a faithful functor from the category of perfect rings to the category of $p$-rings with perfect residue fields that is left adjoint to the functor mapping a $p$-ring with perfect residue fields to its residue field, by (4.5.2.11).

*Proof:* For a canonical ring $F_p[X_p^{-n}]$, $\tilde{Z}[X^{-n}]$ is a strict $p$-ring. Now arbitrary perfect $p$-ring is a quotient of $F_p[X_p^{-n}]$, so we can construct its strict $p$-ring $W(k)$ as the quotient of $\tilde{Z}[X^{-n}]$. Uniqueness is by (4.5.2.11).

Notice it is nothing mysterious, it is just the set of all formal sum $\sum f(x_i) p^i$ under the operation defined in (4.5.2.9). See also (4.5.3.20). 

\[ \square \]

Cor. (4.5.3.22). $W_{p,k}(F_p) \cong \mathbb{Z}/(p^k)$.

Def. (4.5.3.23) [Witt Vectors over Valued Rings]. If a perfect ring $R$ itself has a complete valuation $v$, then we can endow $W(R)$ with a finer topology: we let $w_k(x) = \inf_{i \leq k} v(x_i)$, where $x = \sum p^i f(x_i)$. Now $w_k(x + y) \geq \inf(w_k(x), w_k(y))$ by (4.5.3.19). The weak topology of $W(R)$ is defined by the semi-valuations $w_k$.

Prop. (4.5.3.24). If $a, b \in O_R + p^{n+1} W(R)$, then

$$p^n v(a_n - b_n) \geq w_n(a - b) \geq \inf_{k \leq n} p^{-k} v(a_{n-k} - b_{n-k}).$$

So we see that a sequence is Cauchy in $W(R)$ if each coordinate is Cauchy in $R$, so $W(R)$ is complete in the weak topology.

*Proof:* Firstly the last proposition follows from the first because we can always multiply by a $f(\alpha)$ to make the first $n$ coordinate in $O_R$.

The first is nearly an immediate consequence of (4.5.3.19). 

\[ \square \]
Prop. (4.5.3.25). $O_E = W(K^{1/p})$ is a complete ring with maximal ideal $pO_E$. And $O_E[1/p] = E$ is complete ring of character $p$. And the same construction of $K^{1/p}$ yields the completion of maximal unramified extension of $O_E$, and the Galois group is the same as $G_K$.

Prop. (4.5.3.26) [van Der Kallen]. If $A \to B$ is an étale morphism, then $W_r(A) \to W_r(B)$ is also étale. Moreover, if $A \to A'$ is any ring map with $B' = B \otimes_A A'$, then the natural map

$$W_r(A') \otimes_{W_r(A)} W_r(B) \to W_r(B')$$

is also an isomorphism.

Proof: Cf.[Integral $p$-adic Hodge, BMS]. \hfill \square

4 $\delta$-Rings

Def. (4.5.4.1) [$\delta$-Ring]. A $\delta$-ring structure on $R$ characterize the deficit in lifting the Frobenius action on $R/p$, i.e. $\varphi(x) = x^p + p\delta(x)$. A $\delta$-ring is a pair $(R, \delta)$ where $R$ is a commutative ring and $\delta : R \to R$ is a map that $\delta(0) = \delta(1) = 0$, and satisfies:

$$\delta(xy) = x^p\delta(y) + y^p\delta(x) + p\delta(x)\delta(y), \quad \delta(x + y) = \delta(x) + \delta(y) - \frac{(x + y)^p - x^p - y^p}{p}.$$}

$\delta$-rings naturally form a category, denoted by $CAlg^{\delta}$. And in case $A$ is $p$-torsionfree, a $\delta$-structure on $A$ is the same as a lifting of the Frobenius on $A/p$.

Def. (4.5.4.2) [$\delta$-Pairs]. The category of $\delta$-pairs consists of pairs $(A, I)$ where $A$ is a $\delta$-ring and $I$ is an ideal of $A$ that morphisms $\varphi : (A, I) \to (B, J)$ are $\delta$-ring maps $A \to B$ that $\varphi(I) \subset J$.

Prop. (4.5.4.3) [$\delta$-Rings and $W_2$]. A $\delta$-ring structure on $A$ is the same as a section of the map $W_1 : W_2(A) \to A$, and a morphism of $\delta$-rings is a commutative diagram of sections.

Proof: By the description of $W_2$ in (4.5.3.15), this is clear, the morphism is given by $A \to W_2(A) : x \mapsto (x, \delta(x))$. \hfill \square

Lemma (4.5.4.4) [Initial $\delta$-Algebra]. We usually work with $\delta$-algebras over $\mathbb{Z}_{(p)}$. Then there is an initial object in the category of $\delta$-rings, given by $Z_{(p)}$ with $\delta(x) = \frac{x - x^p}{p}$.

Prop. (4.5.4.5). For a $\delta$-ring $A$, $\varphi$ commutes with $\delta$.

Proof: We need to check $\delta(x^p + p\delta(x)) = \varphi(x)^p + p\delta(\varphi(x))$. This is hard to check, but we can check $\varphi(\frac{x^p}{p}) = \frac{x^p}{p}$, so the conclusion is true when $A$ is $p$-torsion-free. But by (4.5.4.10), every $\delta$-ring is a quotient of a free thus $p$-torsionfree ring, thus the equation is also true for arbitrary $A$. \hfill \square

Def. (4.5.4.6) [Commutative Coalgebra $\mathbb{Z}[\delta]$]. Denote $\mathbb{Z}[\delta] = \mathbb{Z}[\delta, \ldots, \delta_n, \ldots]$. Using the formulas in (4.5.4.1), we can write $\delta^n(xy)$ and $\delta^n(x + y)$ as functions of $\delta^i(x), \delta^i(y)$ for $0 \leq i \leq n$, i.e.

$$\delta^n(xy) = M_n(x, \delta(x), \delta^2(x), \ldots, \delta^n(x), y, \delta(y), \ldots, \delta^n(y))$$

$$\delta^n(x + y) = S_n(x, \delta(x), \delta^2(x), \ldots, \delta^n(x), y, \delta(y), \ldots, \delta^n(y))$$
Then we can change \( \delta^{on} \) to \( \delta_n \) to define a commutative ring scheme structure on \( \text{Spec} \, \mathbb{Z}[\delta] \):

\[
\times : \mathbb{Z}[\delta] \to \mathbb{Z}[\delta] \otimes \mathbb{Z}[\delta] : \delta_n \mapsto M_n, \quad + : \mathbb{Z}[\delta] \to \mathbb{Z}[\delta] \otimes \mathbb{Z}[\delta] : \delta_n \mapsto S_n.
\]

It is easily prove by induction that if we denote \( \mathbb{Z}[\varphi] = \mathbb{Z}[e, \varphi, \varphi_2, \ldots, \varphi_n, \ldots] \), and \( \text{Spec} \, \mathbb{Z}[\varphi] \) the commutative ring scheme with the ring structure given by

\[
\times : \mathbb{Z}[\varphi] \to \mathbb{Z}[\varphi] \otimes \mathbb{Z}[\varphi] : \varphi_n \mapsto \varphi_n \otimes \varphi_n, \quad + : \mathbb{Z}[\varphi] \to \mathbb{Z}[\varphi] \otimes \mathbb{Z}[\varphi] : \varphi_n \mapsto \varphi_n \otimes 1 + 1 \otimes \varphi_n,
\]

then the map

\[
\mathbb{Z}[\varphi] \to \mathbb{Z}[\delta] : \varphi_n \mapsto \text{expansion of } \varphi^{on} \in \mathbb{Z}[e, \delta_1, \ldots, \delta_n]
\]

induces a homomorphism of ring schemes \( \text{Spec} \, \mathbb{Z}[\delta] \to \text{Spec} \, \mathbb{Z}[\varphi] \).

There is a natural functor:

\[
[\delta] : \mathbb{Z}[\delta] \to \mathbb{Z}[\delta] : \delta_i \mapsto \delta_{i+1}
\]

**Lemma (4.5.4.7)**[\( \delta \)-Component]. Let \( \varphi = e^p + p\delta \) be a polynomial in \( e, \delta \), then there are polynomials \( \Theta_n \in \mathbb{Z}[e, \delta_1, \delta_2, \ldots, \delta_n] \) s.t.

\[
\varphi^{on} = \Theta_0^n + p\Theta_1^{p^n-1} + \cdots + p^n\Theta_n = W_{p^n}(\Theta_0, \ldots, \Theta_n), \forall n
\]

In particular, \( \Theta_0 = e, \Theta_1 = \delta \).

Moreover, \( \mathbb{Z}[\Theta_0, \Theta_1, \ldots, \Theta_n] = \mathbb{Z}[e, \delta_1, \delta_2, \ldots, \delta_n] \) for any \( n \).

**Proof:** Use equation \( \varphi \circ \varphi^n = \varphi^n \circ \varphi \) and module \( p^n\mathbb{Z}[\Theta_0, \Theta_1, \ldots, \Theta_n] \).

\( \square \)

**Prop. (4.5.4.8)**[Witt Vectors as \( \delta \)-Rings]. By (4.5.4.7), there is an isomorphism of algebras

\[
\Delta_p \cong \mathbb{Z}[\delta] : X_{p^n} \mapsto \Theta_n,
\]

but it is also an isomorphism of ring schemes because of the uniqueness property of (4.5.3.3).

Then for any \( A \in \mathcal{C} \text{Alg} \), every element of \( W_p(A) \) has a \( \delta \)-coordinates:

\[
f \in W_p(A) = \text{Hom}(\Delta_p, A) \mapsto (f(e), f(\delta_1), f(\delta_2), \ldots)_{\delta}.
\]

Let \( W_p(A) \) be defined as in (4.5.3.5), then \( [\delta] : \mathbb{Z}[\delta] \to \mathbb{Z}[\delta] \) induces a homomorphism \( \delta : W_p(A) \to W_p(A) \) that can be checked to be a \( \delta \)-functor from our definition of coalgebra structure on \( \mathbb{Z}[\delta] \).

Thus \( W_p \) is a functor \( \mathcal{C} \text{Alg} \to \mathcal{C} \text{Alg}^{\delta} \).

**Prop. (4.5.4.9)**[Witt Vectors as an Right Adjoins]. \( W_p \) is right adjoint to the forgetful functor \( \mathcal{C} \text{Alg}^{\delta} \to \mathcal{C} \text{Alg} \).

**Proof:** Given a ring homomorphism \( f : B \to A \), let

\[
f^\delta : B \to W_p(A) : x \mapsto (f(x), f(\delta(x)), f(\delta^2(x)), \ldots)_{\delta},
\]

Then \( f^\delta \) is a \( \delta \)-ring homomorphism: It is a homomorphism by our definition of the ring structure on \( \text{Spec} \, \mathbb{Z}[\delta] \) (4.5.4.6), and it is a \( \delta \)-ring homomorphism by our definition \( \delta \)-ring structure (4.5.4.8).

And it is easy to see \( f^\delta \) is the unique \( \delta \)-ring homomorphism \( B \to W(A) \) that restricts to \( f : B \to A \), thus

\[
\text{Hom}^\delta(B, W(A)) \cong \text{Hom}(B, A).
\]

\( \square \)
Prop. (4.5.4.10) [Free δ-Rings]. The ring \( \mathbb{Z}\{x_i\} \) is a ring on the free generators \( \{x, \delta(x), \delta^2(x), \ldots\} \) and the Frobenius morphism defined by asserting \( \varphi(\delta^i(x)) = \delta^i(x)p + p\delta^{i+1}(x) \).

Generally we can define the free δ-ring generated by \( \{x_i\} \) over a δ-ring \( A \) as the tensor \( A \otimes \mathbb{Z}\{x_i\} \), and it satisfies the universal property.

Then the Frobenius action is f.f.

Proof: It is easily verified that for any δ-ring \( R \) over \( A \) and a map of sets \( \{x_i\} \to R \), there is a unique morphism \( \mathbb{Z}\{p\}\{x_i\} \to R \) sending \( x \) to \( f \), thus verifying the universal property.

For the f.f., notice it is a colimit of \( \mathbb{Z}[x, \delta(x), \delta(x) \ldots, \delta(x)^n(x)] \to \mathbb{Z}[x, \delta(x), \delta(x) \ldots, \delta(x)^{n+1}(x)] \), so by (4.4.1.25), it suffices to show \( \varphi_n \) are all f.f.. We decompose this map as \( n \) maps:

\[
\mathbb{Z}[x, \delta(x), \ldots, \delta^n(x)] \cong \mathbb{Z}[x, \delta(x), \ldots, (\delta^i(x)p, \ldots, \delta^n(x)) \subset \mathbb{Z}[x, \delta(x), \ldots, \delta^n(x)]
\]

which are all f.f., so it is f.f. \( \square \)

Cor. (4.5.4.11) [Frobenius is Fpqc locally Surjective]. For a δ-ring \( A \) and an element \( x \in A \), there is a faithfully flat morphism of δ-rings \( A \to B \) that the image of \( x \) in \( B \) is of the form \( \varphi(y) \) for some \( y \in B \).

Cor. (4.5.4.12). Set \( B \) as the pushout of the diagram \( \mathbb{Z}\{p\}\{s\} \leftarrow \mathbb{Z}\{p\}\{t\} \to A \), where the arrows sends \( t \) to \( \varphi(s) \) and \( x \). \( B \) exists by (4.5.4.13) and the underlying ring is the same as the ring pushout, thus \( A \to B \) is faithfully flat by (4.5.4.10).

Prop. (4.5.4.13) [Limits and Colimits of δ-Rings]. \( \mathcal{C}\text{Alg}_\delta^\delta \) admits limits and colimits, and their underlying rings are just the ring-theoretical limit and colimit, as the forgetful functor \( \mathcal{C}\text{Alg}_\delta \to \mathcal{C}\text{Alg} \) has both left and right adjoints (4.5.4.9)(4.5.4.10).

Proof: Use (4.5.4.3), the construction of limits is straightforward, as \( W_2 \) commutes with limits.

To construct colimits, notice the morphisms \( A_i \to W_2(A_i) \) induces a morphism

\[
\lim A_i \to \lim W_2(A_i) \to W_2(\lim A_i)
\]

and clearly this map is a section of \( W_2(\lim A_i) \to \lim A_i \), thus given a δ-ring structure on \( \lim A_i \).

It is a colimit because any commutative diagrams \( \varphi_i : (A_i \to W_2(A_i)) \to (B \to W_2(B)) \) induces a unique commutative diagram

\[
\begin{array}{ccc}
\lim A_i & \xrightarrow{\varphi_i} & W_2(A_i) \\
\downarrow & & \downarrow \varphi_i \\
B & \xrightarrow{W_2(\varphi_i)} & W_2(B)
\end{array}
\]

Extension of δ-Structures

Lemma (4.5.4.14) [Quotients]. Let \( A \) be a δ-ring and \( I \) be an ideal, then if \( I \) is stable under δ, then there is a natural δ-structure on \( A/I \) compatible with \( A \). In general, if \( J \) is an ideal of \( A \), then there is a universal δ-A-algebra \( B = A/J \), where \( J = \cup_{n \geq 0} \delta^n(I) \). It is the universal δ-A-algebra that the image of \( I \) is 0.
Lemma (4.5.4.15) [Localization]. Let $A$ be a $\delta$-ring and $S$ be a multiplicative set of $A$ that $\varphi(S) \in S$, then there is a unique $\delta$-structure on $S^{-1}A$, and it satisfies the universal property.

Proof: Firstly if $A$ is $p$-torsionfree, in this case a $\delta$-structure is the same as a lifting of the Frobenius on $A/p$, thus the proposition is clear because $\varphi_{S^{-1}A} : S^{-1}A \to S^{-1}A$ is uniquely determined.

Generally, we choose a free $\delta$-ring $F$ and a surjection $\alpha : F \to A$, then $T = \alpha^{-1}S$ is multiplicative, and $T^{-1}F$ admits a unique $\delta$-structure. But now $S^{-1}A = T^{-1}F \otimes_F A$, so there is a $\delta$-structure on $S^{-1}A$ as the colimit, so compatible with that of $S^{-1}A$. Then it’s also the unique one (because if there is another one, the colimit properties gives a morphism of $\delta$-rings above $\text{id}_{S^{-1}A}$, which must by identity).

Lemma (4.5.4.16) [$p$-adic Localization]. If $A$ is a $\delta$-ring with $p \in \text{rad}(A)$, then the formula $\varphi(f) = f^p + p\delta(f)$ shows if $f$ is a unit, then $\varphi(f)$ is also a unit (2.4.2.2), so $S^{-1}A = T^{-1}A$, where $T = \{S, \varphi(S), \varphi^2(S), \ldots\}$.

Thus for any $\delta$-ring $A$ and a multiplicative set $S$, the $p$-localization (4.1.1.31) $(S^{-1}A)(p)$ is the same as the $p$-localization of $T^{-1}A$. Then (4.5.4.15) shows that $(S^{-1}A)(p)$ carries a unique $\delta$-structure compatible with that of $A$.

Lemma (4.5.4.17) [Completions]. For a $\delta$-ring $A$ and a f.g. ideal $I$, the $I$-adic completion of $A$ has a unique $\delta$-structure compatible with that of $A$.

Proof: Let $A \to W_2(A)$ corresponds to the $\delta$-structure by (4.5.4.3), then there is a natural map $A \to W_2(A) \to W_2(A)$, then by the universal property of complete, it extends to a map $\hat{A} \to W_2(A)$, which is a ring map and is a section, all by universal properties.

Lemma (4.5.4.18) [Derived Completion]. If $A$ is a $\delta$-ring and $I \subset A$ is an ideal containing $p$, then the derived $I$-completion ring $\hat{A}$ of $A$ admits a unique $\delta$-structure extending that of $A$.

Proof: The proof is similar as (4.5.4.17).

Prop. (4.5.4.19) [Étale Extension]. Let $A$ be a $\delta$-ring with a f.g. ideal $I$ containing $p$. Assume $B$ is a derived $I$-complete and $I$-completely étale $A$-algebra, then $B$ admits a unique $\delta$-structure compatible with that of $A$.

In particular, any $\delta$-structure on an algebra $A$ passes uniquely to its derived $I$-completion for any ideal $I \subset A$ containing $p$.

Proof: By Elkik’s algebraization (4.6.7.9), we can write $B$ as derived $I$-completion of some étale $A$-algebra $B'$. Then $W_2(A) \to W_2(B')$ is étale by van der Kallen’s theorem (4.5.3.26). Then $W_2(B)$ is the derived $I$-completion of $W_2(B')$, with the $A$-algebra structure given by $A \to W_2(A) \to W_2(B')$. For the rest, Cf. [Scholze, Prism, 2.18].

Distinguished Elements

Def. (4.5.4.20) [Distinguished Elements]. In a $\delta$-ring $A$, an element $d$ is called a distinguished element if $\delta(d)$ is a unit in $A$. A distinguished element is preserved by a $\delta$-ring map.

Lemma (4.5.4.21) [Distinguished up to units]. If $A$ is a $\delta$-ring, $d$ is distinguished and $u$ is a unit, then $ud$ is also distinguished, if $d, p \in \text{rad}(A)$.

Proof: $\delta(ud) = u^p\delta(d) + d^p\delta(u) + p\delta(u)\delta(d)$ is a unit.
Lemma (4.5.4.22) [Irreducibility of Distinguished Elements]. Let $A$ be a $\delta$-ring and $d$ be distinguished element in $A$. If $d = fh$ for some $f, h \in A$ that $f, p \in \text{rad}(A)$, then $f$ is also distinguished and $h$ is a unit.

Proof: Notice that $\delta(d) = f^p\delta(h) + h^p\delta(f) + p\delta(f)\delta(h)$, $\delta(d)$ is a unit, $f^p\delta(h) + p\delta(f)\delta(h) \in \text{rad}(A)$, thus $h^p\delta(f)$ is a unit, so we are done. $\square$

Prop. (4.5.4.23) [Characterization of Distinguished Elements]. Fix a $\delta$-ring $A$ and an element $d$ that $d, p \in \text{rad}(A)$, then $d$ is distinguished iff $p \in (d, \varphi(d))$. In particular, distinguished elements is stable under units.

Proof: If $d$ is distinguished, then $\delta(d)$ is a unit, thus $\varphi(d) = d^p + d^p + p\delta(d)$ shows immediately $p \in (d, \varphi(d))$. Conversely, if $p = ad + b\varphi(d)$, we show $\delta(d)$ is invertible. It suffices to show it is invertible modulo $(d, p)$ as $d, p \in \text{rad}(A)$, or equivalently $(p, d, \varphi(d)) = A$. If it is not the case, then we may take a $(p, d, \varphi(d))$-adic completion to assume $p, d, \varphi \in \text{rad}(A)$, thus the equation simplifies to $p(1 - b\delta(d)) = cd$. The left side is distinguished, by (4.5.4.21), and then $d$ is also distinguished, by (4.5.4.22), so truly $(p, d, \varphi(d)) = A$. $\square$

Prop. (4.5.4.24) [Examples of Distinguished Elements]. The element $d$ is distinguished in the following cases:

- (Crystalline cohomology) Take $A = \mathbb{Z}_{(p)}$ and $d = p$, then $\delta(p) = 1 - p^{p-1}$ is a unit.
- (q-de Rham cohomology) Take $A = \mathbb{Z}_p[[q - 1]]$ and $d = [p]_q = \sum_{i=0}^{p-1} q^i \in A$, with the $\delta$-structure determined by $\varphi(q) = q^p$.
- (Breuil-Kisin cohomology) Fix a discretely valued field $K/Q_p$ with uniformizer $\pi$, $W$ the maximal unramified subring of $O_K$. Take $A = W[[u]]$ with $\delta(u) = u^p$, then any generator of the kernel of the map of $A \to O_K : u \to \pi$ is distinguished.
- (Ainf-cohomology) Let $A$ be the $(p, q - 1)$-completion of $\mathbb{Z}_p[1/p^\infty]$. Then $A$ is $p$-torsion free and $\varphi(q) = q^p$ gives a $\delta$-structure. Then $d = [p]_q$ defined in item2 is also distinguished. And $\varphi^n(d)$ is distinguished for any $n \in \mathbb{Z}$ by (4.5.4.5).

Proof: It is clear $\varphi$ is continuous and $\delta$ stabilizes $(q - 1)$, and $d$ is distinguished because the image of $\delta(d)$ in $A/(q - 1) \cong \mathbb{Z}_q$ is $\delta(p) = 1 - p^{p-1}$ is a unit, thus it is also a unit in $A$. $\square$

Perfect $\delta$-Ring

Def. (4.5.4.25) [Perfect $\delta$-Ring]. A perfect $\delta$-ring is a $\delta$-ring that $\varphi$ is an isomorphism.

Prop. (4.5.4.26) [Perfections]. The inclusion of the category of perfect $\delta$-rings to the category of $\delta$-rings admits left and right adjoints, $A_{\text{perf}}$ and $A_{\text{perf}}^\text{perf}$ with definition similar to (4.5.1.10).

Proof: We use (4.5.4.3), the map $A \to W_2(A) \to W_2(A_{\text{perf}})$ extends uniquely to a map $A_{\text{perf}} \to W_2(A_{\text{perf}})$ lifting the $\delta$-action of $A$. Similarly, because $(-)^{\text{perf}}$ is a limit and $W_2(-)$ is a right adjoint, then $W_2(-)$ commutes with $(-)^{\text{perf}}$. In particular, there is a natural map $A_{\text{perf}} \to W_2(A_{\text{perf}})$. $\square$

Lemma (4.5.4.27) [Frobenius Kills $p$-Torsion]. If $A$ is a $\delta$-ring and $x \in A$ satisfies $px = 0$, then $\varphi(x) = 0$. In particular, if $A$ is perfect, then $A$ is $p$-torsionfree.

Proof: Applying $\delta$ to $px = 0$, we have $0 = p^\delta(x) + x^p\delta(p) + p\delta(x)\delta(p) = p^\delta(x) + \varphi(x)\delta(p)$. As $\delta(p)$ is a unit, and $p^\delta(x) = p^{p-1}(\varphi(x) - x^p) = \varphi(x)(p^{p-1}x) - p^{p-1}x^p = 0$, thus $\varphi(x) = 0$. $\square$
Prop. (4.5.4.28) [Perfect $p$-Complete $\delta$-Rings]. The following categories are equivalent:

- The category of perfect $p$-adically complete $\delta$-rings.
- The category $p$-adically complete and $p$-torsionfree rings $A$ with $A/p$ perfect.
- The perfect $F_p$-algebras.

In particular, every perfect $p$-complete $\delta$-ring is of the form $W(k)$ thus has Teichmuller expansions.

**Proof:** 2 and 3 are equivalent by Witt vector construction, by (8.2.4.3), noticing that there is a natural lifting on $W(k)$ lifting the Frobenius of $k/F_p$ that induces a $\delta$-functor. There is a forgetful functor from 1 to 2, by (4.5.4.27) (notice $A/p$ is also perfect because if $\varphi(x) \in (p)$, then $x \in \varphi^{-1}(p) = (p)$ as $\varphi(p) = p\varphi(1) = p$) and it is faithful. Now there is an equivalence from $3 \to 1 \to 2$, thus $1 \to 2$ is essentially surjective thus is an equivalence.

Prop. (4.5.4.29) [Perfect Element has Rank 1]. Fix a $\delta$-ring $A$ and an element $x \in A$, then $\delta(x^n) \in p^nA$ for any $n$. In particular, if $A$ is $p$-adically separated and $y$ is perfect in $A$, then $\delta(y) = 0$.

**Proof:** By formal calculation, it suffices to show that $p\delta(x^n) \equiv x^{pn+1} \mod p^{n+1}A$, which is true by (20.1.2.8).

Prop. (4.5.4.30) [Distinguished Element in Perfect $\delta$-Rings]. Let $A$ be a perfect $p$-complete $\delta$-ring (or perfect $F_p$-algebra by (4.5.4.28)), and $d \in A$, then $d$ is distinguished iff its coefficient of $p$ in the Teichmuller expansion (4.5.4.28) is a unit.

If $d$ is distinguished, then it is a nonzero-divisor, and $A/d[p^\infty] = A/d[p]$.

**Proof:** Let $d = \sum_{i \geq 0} [a_i]p^i$, then

$$\delta(d) = \frac{1}{p} \left( \sum_{i \geq 0} [a_i]p^i \right) \equiv [a_1] \mod pA$$

thus it is a unit iff $a_1$ is a unit, because $A$ is $p$-complete.

Now if $d$ is distinguished, and $fd = 0$. If $f \neq 0$, we may assume $p \nmid f$, because $A$ is $p$-torsionfree and $p$-adically complete (4.5.4.28). Now

$$\varphi(f)\delta(fd) = \varphi(f)(f^p\delta(d) + \delta(f)\varphi(d)) = \varphi(f)f^p\delta(d) = 0,$$

so $f^p\varphi(f) = 0$, and $f^{2p} \equiv 0 \mod p$. Hence $f \equiv 0 \mod p$, but then $p|f$, contradiction.

For the last assertion, it suffices to show that $A/d[p^2] = A/d[p]$. If $p^2f = dg$, then $\varphi(g)\delta(gd) = \varphi(g)(\delta(d)g^p + \varphi(d)\delta(g)) = \varphi(g)\delta(d)g^p + \varphi(dg)\delta(g) \in pA$, thus $\varphi(g)g^p \in pA$, hence $g^{2p} \in pA$, and hence $g \in pA$, showing $pf \in dA$. 

\[\square\]
4.6 Derived Commutative Algebras

Main references are [Sta].

[Sta] Chap15 contains many beautiful results working on the derived category of rings, and is used heavily in Scholze’s Thesis.

The basic construction of $R\text{tensor}$ and $R\text{Hom}$ should be redone at the level of ringed sites, Cf.[Sta] Chap21.

1 Basics

Prop.(4.6.1.1)[Product in $D(R)$]. Let $R$ be a ring and $K_n \in D(R)$, then the product in $D(R)$ of $K_n$ is given by $\prod I_n$, where $I_n$ are $K$-injective resolutions of $K_n$.

Proof: This is immediate from (3.4.3.7). □

Def.(4.6.1.2)[Homotopy Fiber Square]. A square of Abelian groups is called a homotopy fiber square if it is a homotopy fiber square in the derived category, or equivalently, the kernel of the two rows(or the two columns) are isomorphic.

This notion is identical to the notion of pullback square when the rows or the columns are surjective.?

Prop.(4.6.1.3)[Bockstein Differential]. Let $I$ be an invertible ideal of $A$, for any $M^\bullet \in D(A)$, we use the Breuil-Kisin Twist notation (6.7.5.1) and consider the exact triangle

$$M^\bullet \otimes^L _A A/I\{i+1\} \to M^\bullet \otimes^L _A I^i/I^{i+2} \to M^\bullet \otimes^L _A A/I\{i\}$$

obtained from the exact triangle

$$I^{n+1}/I^{n+2} \to I^n/I^{n+2} \to I^n/I^{n+1}$$

tensoring $\mathcal{O}_\Delta$. Then we get a Bockstein differential

$$\beta^n : H^n(M^\bullet \otimes^L _A A/I\{n\}) \to H^{n+1}(M^\bullet \otimes^L _A A/I\{n+1\})$$

Then these maps satisfy $\beta^{n+1} \circ \beta^n = 0$.

Proof: Consider the morphism of distinguished triangles:

$$\begin{array}{ccc}
I^{n+1}/I^{n+3} & \to & I^n/I^{n+3} \\
\downarrow & & \downarrow \\
I^{n+1}/I^{n+2} & \to & I^n/I^{n+2}
\end{array}$$

then we see for any $M^\bullet \in D(A)$, $\beta^n$ factors as

$$H^n(M^\bullet \otimes^L _A I^n/I^{n+1}) \to H^{n+1}(M^\bullet \otimes^L _A I^{n+1}/I^{n+3}) \to H^{n+1}(M^\bullet \otimes^L _A I^{n+1}/I^{n+2})$$

and also we consider the distinguished triangle

$$I^{n+2}/I^{n+3} \to I^{n+1}/I^{n+3} \to I^{n+1}/I^{n+2}$$

to see that the composition

$$H^{n+1}(M^\bullet \otimes^L _A I^{n+1}/I^{n+3}) \to H^{n+1}(M^\bullet \otimes^L _A I^{n+1}/I^{n+2}) \xrightarrow{\beta^{n+1}} H^{n+2}(M^\bullet \otimes^L _A I^{n+2}/I^{n+3})$$

is 0, and this two observation gives the result. □


**4.6. DERIVED COMMUTATIVE ALGEBRAS**

**Injective Amplitude**

**Prop.(4.6.1.4)[Injective Amplitude].** For $K \in D(A)$, the following are equivalent:

- $K$ has finite amplitude in $[a, b]$.
- $\text{Ext}^i(N, K) = 0$ for any $N \in D^0(A)$ and $i \notin [a, b]$.
- $\text{Ext}^i(A/I, K) = 0$ for any ideal $I$ of $A$.

**Proof:** $1 \to 2 \to 3$ is clear. For $3 \to 1$: Notice $\text{Ext}^n(A, K) = H^n(K), H^i(K) = 0$ for any $i \notin [a, b]$. Then $K$ is represented by a complex

$$0 \to I^a \to I^a \to I^a+1 \to \ldots \to I^b \to \ldots.$$  

Let $J = \text{ker}(I^b \to I^{b+1})$, then $K$ is also represented by

$$0 \to I^a \to I^a \to I^a+1 \to \ldots \to I^b \to J \to 0.$$  

Let $K' = (I^a \to \ldots \to I^b) \in D(A)$, then there is an distinguished triangle

$$J[-b] \to K \to K' \to J[1-b],$$

which induces an exact sequence $\text{Ext}^b(R/I, K') \to \text{Ext}^1(R/I, J) \to \text{Ext}^{b+1}(R/I, K)$ for any ideal $I \subset A$. Then by $1 \to 2$, $\text{Ext}^1(R/I, J) = 0$, implying $J$ is injective. $\square$

**Prop.(4.6.1.5)[Dedekind Domain].** Let $R$ be a Dedekind domain, then every ideal $I$ is finite torsion-free thus projective over $R$, so every $R$-module has injective dimension $\leq 1$. In particular, $\text{Ext}^i(M, N) = 0$ for any $i \geq 2$ and $M, N \in \text{Mod}_R$. In particular, by (3.4.4.26), any $K \in D^+(R)$ is isomorphic to a direct sum of their cohomology groups.

**Prop.(4.6.1.6).** Let $(R, m, k)$ be a Noetherian local ring and $K \in D^+(R)$ have finite cohomology modules, then $K$ has finite injective dimension iff $\text{Ext}^i_R(k, K) = 0$ for $i$ large.

**Proof:** Cf.[Sta]0AVJ. $\square$

**2 Derived Tensor and Tor**

**Prop.(4.6.2.1)[Differential Graded Structure].** If $K$ is a commutative $A$-algebra object in $D(A)$ in the monoidal structure defined in (5.3.3.8), then $\oplus_{n \geq 0} H^n(K^\bullet)$ carries a natural graded commutative $A$-algebra structure.

**Proof:** Compare with (8.1.2.4).

We may replace $K$ by a $K$-flat resolutions $L^1(5.3.3.3)$ that the algebra structure map for $K$ is represented by a morphism $L^1_1 \otimes_A L^1_1 \to L^2$ of complexes where $L^2$ is a complex quasi-isomorphic to $K$, hence the graded $A$-algebra structure is clear by (3.3.6.2), and it is commutative by (3.3.6.1). (How to check the structure is uniquely determined?). $\square$

**Tor**

**Def.(4.6.2.2)[Tor].** Let $M, N$ be $A$-module, then the torsion group $\text{Tor}^A_i(M, N)$ is defined to be $H^i(M \otimes_A L N)$, compatible with the definition in (5.3.3.11).
Def.(4.6.2.3) [Torsion Group]. Let \( A \) be a commutative ring, \( B \) an \( A \)-algebra and \( I \) be an ideal, then the \( I \)-torsion of \( B \) is defined to be \( \text{Tor}_I^1(A/I, B) \), denoted by \( B[I] \). In case \( I = (f) \), it can be checked that \( B[f] \) is the set of elements of \( B \) that killed by \( f \).

Also we denote \( B[I^n] = \text{colim}_{n \to \infty} B[I^n] \). And \( B \) is said to have bounded \( f \)-torsion iff \( B[f^n] = B[f^n] \) for some \( n \).

Prop.(4.6.2.4). If \( A \) is a commutative ring with bounded \( I \)-torsions and \( B \) is a flat \( A \)-module, then \( B \) also has bounded \( I \)-torsions. (Because tensoring \( B \) is exact).

Prop.(4.6.2.5) [Balancing Tor]. In the category of rings, \( \text{Tor}_n(A, B) = \text{Tor}_n(B, A) \). This can be seen using spectral sequence of the double complex of flat resolutions of \( A \) and \( B \). Similarly, we have two definitions of \( \text{Ext}^i(M, N) \) are compatible.

Proof:

Prop.(4.6.2.6) [Base Change]. For a ring extension \( R \to S \), using projective resolution and spectral sequence, there is a first quadrant homology spectral sequence:

\[
E^2_{pq} = \text{Tor}_p^S(\text{Tor}_q^R(A, S), B) \Rightarrow \text{Tor}_{p+q}^R(A, B).
\]

Similarly, for \( \text{Ext} \),

\[
E^2_{pq} = \text{Ext}_p^R(A, \text{Ext}_q^R(S, B)) \Rightarrow \text{Ext}_{p+q}^R(A, B).
\]

Prop.(4.6.2.7) [Universal Coefficient Theorem]. Let \( P \) be a free \( R \)-module so \( d(P_n) \) are all flat, then \( Z(P_n) \) are also flat and

\[
0 \to d(P_{n+1}) \to Z_n \to H_n \to 0
\]

is a free resolution. we have an exact sequence:

\[
0 \to H_n(P) \otimes_R M \to H_n(P \otimes_R M) \to \text{Tor}_1^R(H_{n-1}(P), M).
\]

and these exact sequences non-canonically split because \( Z_n \) is a direct summand of \( P_n \), thus \( Z_n \otimes M \) is a direct summand of \( P_n \otimes M \) and a fortiori \( Z_n(P_n \otimes M) \). so \( H_n(P) \otimes M \) is a direct summand of \( H_n(P \otimes_R M) \).

**Internal Hom and Derived Tensor**

Prop.(4.6.2.8). If \( R \) is a ring and \( K, L, M \in D(R) \), then

\[
R\text{Hom}_R(K, R\text{Hom}(L, M)) = R\text{Hom}_R(K \otimes^L_R L, M).
\]

Proof: This is a special case of(5.3.3.29).

Cor.(4.6.2.9).

\[
\text{Hom}_{D(R)}(K, R\text{Hom}(L, M)) = \text{Hom}_{D(R)}(K \otimes^L_R L, M),
\]

i.e., derived tensor is left adjoint to internal Hom.

Proof: This follows from taking \( H^0 \), by(3.4.4.18).

Prop.(4.6.2.10) [Derived Base Change Adjunction]. For a ring map \( R \to S \) and any \( L \subset D(R), M \subset D(S) \), there is an isomorphism

\[
\text{Hom}_R(L, M) \cong \text{Hom}_S(L \otimes^L_R S, M)
\]

Proof: This follows from(5.3.3.16).
3 Rlim

Def. (4.6.3.1) [Rlim]. Rlim is the derived limit (3.4.6.1) in $D(\text{Ab})$ restricted to the inverse systems consisting of discrete complexes.

Lemma (4.6.3.2). The set of Mittag-Leffler Complexes in $\text{Ab}(\mathbb{N})$ is adapted for $R\lim$.

Proof: Firstly, for any complex $(A_n)$, we can associate to it the complex $(B_n)$ where $B_n = A_n \oplus A_{n-1} \oplus \ldots \oplus A_1$, then $(B_n)$ is a Mittag-Leffler complex and $(A_n) \hookrightarrow (B_n)$. So ML complexes are sufficiently large.

Now for any exact sequence of complexes $0 \to (A_n) \to (B_n) \to (C_n) \to 0$, if $A_n$ is ML, then $\lim B_i \to \lim C_i$ is surjective: for an element $(c_i) \in \lim C_i$, let $E_i = \pi_i^{-1}(c_i) \in B_i$, then $(E_i)$ is an inverse system of nonempty sets, and it suffices to show $(E_i)$ is ML, because then (3.1.1.46) will show there is an element $(e_i) \in \lim E_i \subset \lim B_i$ that maps to $(c_i)$.

For this, Cf. [Sta]0598. □

Prop. (4.6.3.3) [Rlim].

- If $(A_n)$ is Mittag-Leffler, then $R^1\lim ((A_n)) = 0$.
- $R\lim ((A_n))$ is represented by the complex in degree 0,1:

$$\prod_n A_n \to \prod_n A_n : (x_n) \mapsto (x_n - f_{n+1}(x_{n+1}))$$

- for any $(A_n) \in \text{Ab}(\mathbb{N})$ we have $R^p \lim ((A_n)) = 0$ for $p > 1$.

Proof: 1 follows from (4.6.3.2) and (3.4.4.2).

2, 3: We use (3.4.4.2) again. Notice the complex $(B_n)$ where $B_n = A_n \oplus A_{n-1} \oplus \ldots \oplus A_1$ and the complex $(C_n)$ where $C_n = A_{n-1} \oplus A_{n-2} \oplus \ldots \oplus A_1$ form an exact sequence of complexes

$$0 \to (A_n) \to (B_n) \to (C_n) \to 0$$

where $B_n \to C_n : (x_i) \mapsto (x_i - f_{i+1}(x_{i+1}))$, and $(B_n), (C_n)$ are both ML, so we are done. □

4 Lifting Complexes

Prop. (4.6.4.1) [Lifting Projective Complex Along Thickening]. Let $R$ be a ring and $I$ be a nilpotent ideal, and $K \in D(R)$. Now if $K \otimes_R^L R/I$ is represented by a bounded above complex of projective $R/I$-modules, then there is a complex $P$ of bounded above complex of projective $R$-modules that $P \cong K \in D(R)$, and $P \otimes_R R/I \cong E$.

Proof: Cf. [[Sta]09AR]. □

5 Pseudo-Coherent and Perfect Modules

Def. (4.6.5.1) [Pseudo-Coherent Modules]. Let $R$ be a ring, $m \in \mathbb{Z}$, then $K \in D(R)$ is called an $m$-pseudo-coherent module iff there exists a complex $E^* \in K^b(R)$ and a morphism $\alpha : E^* \to K^*$ where $K^*$ represents $K$, s.t. $H^i(\alpha)$ is an isomorphism for $i > m$, and surjective for $i = m$.

$K \in D(R)$ is called a pseudo-coherent module if it is represented by a bounded above complex of finite free $R$-modules.
Prop.(4.6.5.2). If $A$ is Noetherian and $C^\bullet$ is a complex of $A$-modules bounded above that every cohomology group $H^i$ is a finite $A$-module, then there is a complex $L^\bullet$ of finite free $A$-modules, that $g : L^\bullet \to C^\bullet$ is a quasi-isomorphism.

Moreover, if $C^i$ are all flat $A$-modules, then $L^\bullet \otimes_A M \to C^\bullet \otimes_A M$ is quasi-isomorphism for every $M$.

Proof: $C^\bullet$ is bounded above so we choose $L^n = 0$, and use induction to construct $L^n$ that $H^i(L) \to H^i(C)$ is isomorphism for $i > n+1$ and surjection for $i = n+1$. For this, choose a generator $x_1, \ldots, x_r$ of $H^n(C)$ in $Z^n(C)$, and let $y_{r+1}, \ldots, y_s$ be a generator of $g^{-1}(B^{n+1}(C))$(Noetherian used), and let $g(y_i) = dx_i$ for $x_i \in C^n$.

Now let $L^n$ be freely generated by $e_1, \ldots, e_s$ and $de_i = 0$ for $i \leq r$ and $de_i = y_i$ for $i > r$, and let $g : L^n \to C^n$ be $ge_i = x_i$. Then it can be verified to be a quasi-isomorphism.

If $C^i$ are all flat, we check isomorphism for all f.g. modules $M$, because $\otimes$ and cohomology all commutes with direct limits. Use induction, for $n$ large, both are 0, and if we write $0 \to R \to F \to M \to 0$, for $F$ finite free, then there is a commutative diagram of long exact sequences, and for $F$, $H^i$ are obviously isomorphism, so I can use five lemma. □

Def.(4.6.5.3) [Perfect Complexes of Modules]. Let $R$ be a ring, then $K \in D(R)$ is called a perfect module if $K$ is quasi-isomorphic to a bounded complex of finite projective $R$-modules. An $R$-module $M$ is called perfect iff $M[0]$ is perfect.

Prop.(4.6.5.4) [Perfectness and Pseudo-Coherence]. An object $K \in D(R)$ is perfect iff it is pseudo-coherent and has finite Tor amplitude.

Proof: Cf.[Sta]0658. □

Prop.(4.6.5.5). If $R$ is a regular ring of finite dimension, then an object $K \in D(R)$ is perfect iff $K \in D^b(R)$ and each $H^i(K)$ is a finite $R$-module.

Proof: Cf.[Sta]066Z. □

Prop.(4.6.5.6) [Duality of Perfect Complexes]. Let $K$ be a perfect complex of $D(A)$, then the dual complex $K^\vee = R \text{Hom}(K,A)$ is also a perfect complex and $(K^\vee)^\vee \cong K$. Also, there is a functorial isomorphism

$$L \otimes^L_A K^\vee = R \text{Hom}_A(K,L)$$

Proof: Cf.[Sta]07VI. □

Prop.(4.6.5.7). If $A$ is a ring and $K_n$ is a system of perfect objects in $D(A)$, then for any $E \in D(A)$, there is an isomorphism

$$R \text{Hom}_A(\text{ho colim } K_n, E) \cong R \text{lim } E \otimes^L_A K_n$$

Proof: By(4.6.5.6), $R \text{lim } E \otimes^L_A K_n = R \text{lim } R \text{Hom}(K_n, E)$ which fits into a distinguished triangle

$$R \text{lim } R \text{Hom}(K_n, E) \to \prod \text{Hom}(K_n, E) \to \prod \text{Hom}(K_n, E)$$

. So it suffices to show that

$$\prod \text{Hom}(K_n, E) \cong R \text{Hom}_A(\oplus K_n, E).$$

This follows from Yoneda lemma and(5.3.3.28)(5.3.3.29). □
Prop. (4.6.5.8) [Perfectness and Thickening]. If $R$ is a ring, $I \subset R$ is a nilpotent ideal, and $K \in D(R)$. If $K \otimes_{R}^{} R/I$ is perfect in $D(R/I)$, then $K$ is perfect in $R$. Moreover, if $K \otimes_{R}^{} R/I = 0$, then $K = 0$.

Proof: Let $P^\bullet \cong K \otimes_{R}^{} R/I$ where $P$ is a complex of finite projective $R/I$-modules, then by (4.6.4.1) there is a complex of projective $R$-modules $P$ that $P/IP \cong P$. Then it follows from Nakayama that $P$ is bounded.

Pseudo-Coherent Modules

Def. (4.6.5.9) [Pseudo-Coherent Complexes of Modules]. Let $R \in \mathcal{C}_{\text{Alg}}$, $K \in D(R)$ is called an $m$-pseudo-coherent module if there exists a perfect object $E \in D(R)$ and a morphism $E \to K$ that induces isomorphisms on $H^i$ for $i > m$ and surjection on $H^m$.

$K \in D(R)$ is called a pseudo-coherent module if it is represented by a bounded above complex of finite free $R$-modules.

6 Derived Completeness

Cf. [Sta] Chap 15.90.

Def. (4.6.6.1). For a ring $A, f \in A$ and a complex $K \in D(A)$, we denote by $T(K, f)$ a derived limit of the system

$$\ldots \to K \xrightarrow{f} K \xrightarrow{f} K$$

Prop. (4.6.6.2) [Properties of $T(K, f)$]. For a ring $A, f \in A$ and $K \in D(A)$, the following are equivalent:

1. $T(K, f) = 0$.
2. $R\text{Hom}_A(A_f, K) = 0$.
3. $\text{Ext}^n_A(A_f, K) = 0$ for all $n$.
4. $\text{Hom}_{D(A)}(E, K) = 0$ for all $E \in D(A_f)$.
5. For any $p \in \mathbb{Z}$, $\text{Hom}_A(A_f, H^p(K)) = 0$ and $\text{Ext}^1_A(A_f, H^p(K)) = 0$.
6. For any $p \in \mathbb{Z}$, $T(H^p(K), f) = 0$.

Proof: 2, 3 is clearly equivalent.

4 $\to$ 3 is clear, and for 3 $\to$ 4: Let $I^\bullet$ be a complex representing $K$, then 3 says $\text{Hom}_A(A_f, I^\bullet)$ is acyclic, and $\text{Hom}_{D(A)}(E, K) = \text{Hom}_K(A_f)(E, \text{Hom}_A(A_f, I^\bullet))$. As $\text{Hom}_A(A_f, I^\bullet)$ is both acyclic and $K$-injective (3.3.6.6), we get it is homotopic to 0 by (3.4.3.1), thus we get 4.

1 $\iff$ 3: There is a free resolution of $A_f$ given by

$$0 \to \oplus_n A \to \oplus_n A \to A_f \to 0$$

where the first map is $(a_n) \mapsto (a_n - f a_{n-1})$, and the second map is $(a_n) \mapsto \sum a_i / f^i$. Applying $\text{Hom}_A(-, I^\bullet)$, we get a distinguished triangle

$$R\text{Hom}_A(A_f, K) \to \prod K \to \prod K.$$ 

So this shows $R\text{Hom}_A(A_f, K)$ is just $T(K, f)$, so we get 1 $\iff$ 3.
1 $\iff$ 5 $\iff$ 6: There is a spectral sequence convergence (choose a finite free resolution of $A_f$ then rotate and use (3.4.7.10)):

$$E_2^{p,q} = \text{Ext}_A^q(A_f, H^p(K)) \Rightarrow \text{Ext}_A^{p+q}(A_f, K)$$

This spectral sequence degenerates at $E_2$ because $A_f$ has a length 1 resolution by free $A$-modules hence the $E_2$ page has only 2 rows. So there is an exact sequence

$$0 \to \text{Ext}_A^1(A_f, H^{p-1}(K)) \to \text{Ext}_A^1(A_f, K) \to \text{Hom}_A(A_f, H^p(K)) \to 0.$$ 

Then we are done. $\square$

**Lemma (4.6.6.3).** Let $A$ be a ring, $K \in D(A)$, then the set $I$ of $f$ that $T(K, f) = 0$ is a radical ideal of $A$.

**Proof:** If $T(K, f) = 0$ and $g \in A$, then $A_{gf}$ is a $A_f$-module, then

$$\text{Ext}_A^n(A_{gf}, K) = \text{Hom}_{D(A)}(A_{gf}[-n], K)(5.3.3.32) = 0$$

by (4.6.6.2) item 4. Then $T(K, gf) = 0$ by (4.6.6.2) again. And if $f, g \in I$, there is an exact sequence

$$0 \to A_{f+g} \to A_{f(f+g)} \oplus A_{g(f+g)} \to A_{fg(f+g)} \to 0$$

by (4.4.2.3) and a easy check that the last term is surjective. Then from the long exact sequence of Ext, we get $\text{Ext}_A^n(A_{f+g}, K) = 0$ for any $n$. Finally if $f^n \in I$, then $f \in I$, because $A_f = A_{f^n}$. $\square$

**Def. (4.6.6.4) [Derived Completeness].** Let $A$ be a ring, $K \in D(A)$, $I$ is an ideal of $A$, then $K$ is said to be derived complete w.r.t $I$ if $T(K, f) = 0$ for any $f \in A$. Let $D_{\text{comp}}(A, I)$ denote the subcategory consisting of derived $I$-complete objects in $D(A)$.

Let $M$ be an $A$-module, then $M$ is called derived complete w.r.t $I$ if $M[0] \in D(A)$ is derived complete w.r.t $I$.

**Prop. (4.6.6.5).** A $\aleph_0$-filtered colimit of derived $I$-complete rings is also derived $I$-complete.

**Proof:** Cf. [Bhatt, Prism, 5.4.3]. $\square$

**Prop. (4.6.6.6) [Complete and Derived Complete].** Let $A$ be a ring and $I$ be an ideal, $M$ an $A$-module, then

- If $M$ is $I$-adically complete, then $T(M, f) = 0$ for any $f \in I$.
- If $T(M, f) = 0$ for all $f \in I$ and $I$ is f.g., then $M \to \lim M/I^n M$ is surjective.

In particular, if $I$ is f.g., $M$ is $I$-adically complete iff $M$ is derived $I$-adically complete and $\cap I^n M = 0$.

In particular, when $M$ is f.g., over a Noetherian and $I \subset \text{rad}(A)$, derived $I$-complete is equivalent to $I$-complete (4.2.2.14).

**Proof:** If $M$ is $I$-adically complete, by (4.6.6.2), it suffices to show that $\text{Hom}(A_f, M) = 0$ and $\text{Ext}_A^1(A_f, M) = 0$. But $M = \lim M/I^n M$, and $\text{Hom}(A_f, M/I^n M) = 0$, because $f \in I$. For Ext, use (3.4.4.24), for any extension

$$0 \to M \to E \to A_f \to 0,$$

chose arbitrary $e_n$ that maps to $1/f^n$. Then $\delta_n = fe_{n+1} - e_n \in M$. We consider

$$e'_n = e_n + \delta_n + f\delta_{n+1} + f^2\delta_{n+2} + \ldots.$$
which exist because $M$ is $I$-adically complete. Then $f e_{n+1}' = e_n'$, so this gives a splitting of the extension.

Conversely, if $I = (f_1, \ldots, f_r)$ and $T(M, f_i) = 0$ for any $i$, then by (4.2.3.16), we can assume $I = (f)$. Then consider the extension

$$0 \to M \to E \to A_f \to 0$$

where $E = (M \oplus \bigoplus A e_n)/(x_n - f e_{n+1} + e_n) \to A_f$ that maps $M$ to $0$ and $e_n$ to $1/f^n$. This extension splits by (4.6.6.2) and (3.4.4.24), thus there is an element $x + e_0$ that generate a copy of $A_f$ in $E$.

But then $x + e_0 = x - x_0 + f e_1 = x - x_0 - f x_1 + f^2 e_2 - \ldots - f^{n-1}x_{n-1} \in f^n E + A_f$ for any $n$. Then $x - x_0 - f x_1 + f^2 x_2 - \ldots - f^{n-1}x_{n-1} \in f^n M$, because $E = M \oplus A_f$. Then we are done.

**Prop. (4.6.6.7)**. If $M = D(A/I) \subset D(A)$, then $M$ is derived-$I$-complete. (This follows from the definition of $T(M, f)$).

**Prop. (4.6.6.8)** [Category of Derived Complete Modules]. Let $I$ be an ideal of $A$, then the derived $I$-complete $A$-modules form a weak Serre subcategory of $\text{Mod}_A$. In particular, $D_{comp}(A, I)$ is also a weak Serre subcategory.

**Proof**: If $f : M \to N$ is a map of derived $I$-complete $A$-modules, then we consider the complex $K = (M \to N)$, then there is an exact sequence $0 \to M[1] \to K \to N \to 0$, so we have $\text{Ext}^n(A_f, K) = 0$ for any $f \in I$, $n \in \mathbb{Z}$ because $M, N$ does (4.6.6.2), so $K$ is derived $I$-complete by (4.6.6.2) again. Then we have $\ker(f), \text{Coker}(f)$ are derived $I$-complete, by (4.6.6.2) again. Extension is also clear.

**Lemma (4.6.6.9)**. If $R$ is ring, $I$ is an ideal, and $K \in D(R)$ that $K \otimes_R^L R/I = 0$, then $K \otimes_R^L M$ for any $M \in D^b(R)$ with all the cohomology groups $I$-power torsions.

**Proof**: We use the truncation (3.3.3.6), then it suffices to prove for $M$ discrete. Now $M = \bigcup M[I^n]$, and we have $K \otimes_R^L M = \text{ho} \lim \colim K \otimes_R^L M[I^n]$, so we may assume $I^n M = 0$ for some $n$. Consider the $R$-algebra $R' = R/I^n \oplus M$, where $M^2 = 0$, then it suffices to show $K' = K \otimes_R^L R' = 0$. Now $0 = K \otimes_R^L R/I = K' \otimes_R^L R/I$, so by (4.6.6.8) $K' = 0$.

**Prop. (4.6.6.10)** [Derived Nakayama]. the derived tensor product $- \otimes_A^L A/I$ reflects isomorphism on $D_{comp}(A, I)$, i.e. if $M \otimes_A^L A/I = 0$, then $M = 0$.

**Proof**: Let $I = (f_1, \ldots, f_r)$, by (4.6.6.9), $M \otimes_A^L K_n = 0$ for any $K_n = K \otimes_A^L f_1^n, \ldots, f_r^n$, so $K = R \text{lim} K \otimes_A^L K_n = 0$.

**Cor. (4.6.6.11)**. If $I$ is f.g. and $M$ is a derived $I$-complete $A$-module that $M/IM = 0$, then $M = 0$.

**Proof**: ? This should be an immediate corollary.

Let $I = (f_1, \ldots, f_r)$, if $M \neq 0$, let $i$ be the largest integer that $M/(f_1, \ldots, f_i)M \neq 0$, then $N$ is also derived $I$-complete by (4.6.6.8). But $f_{i+1} : N \to N$ is surjective, so $T(N, f_{i+1}) \neq 0$, contradiction.

**Prop. (4.6.6.12)**. If $A$ is derived $I$-complete, then $(A, I)$ is a Henselian pair.

**Proof**: Cf. [Sta]0G3H?.
Prop. (4.6.6.13) [Derived I-Completion]. If \( I = (f_1, \ldots, f_n) \) is f.g. in \( A \), the inclusion of categories \( D_{\text{comp}}(A, I) \subset D(A) \) has a left adjoint, which maps \( K \) to

\[
\hat{K} = R\text{Hom}\left((A \to \prod_{i_0} A_{f_{i_0}} \to \prod_{i_0 < i_1} A_{f_{i_0}f_{i_1}} \to \cdots \to A_{f_1 \ldots f_r}), K\right).
\]

called the derived I-completion of \( K \).

Moreover, this construction is identical to \( K \mapsto K^{\bullet} = R\lim (K \otimes_A K^{\bullet}_n) \), by (4.6.5.7) and (4.4.4.7).

**Proof:** There is a map \( (A \to \prod_{i_0} A_{f_{i_0}} \to \prod_{i_0 < i_1} A_{f_{i_0}f_{i_1}} \to \cdots \to A_{f_1 \ldots f_r}) \to A \), which induces a morphism \( K \to \hat{K} \). Now by (5.3.3.28), \( R\text{Hom}(A_f, \hat{K}) \) is isomorphic to \( R\text{Hom}((A_f \to \prod_{i_0} A_{ff_{i_0}} \to \prod_{i_0 < i_1} A_{ff_{i_0}f_{i_1}} \to \cdots \to A_{ff_1 \ldots f_r}), K) \) as \( A_f \) is \( A \)-flat. Now this one is 0 for any \( f \in I \), by (4.4.4.7), so \( \hat{K} \) is derived I-complete.

Conversely, if \( \hat{K} \) is derived I-complete, then \( R\text{Hom}(A_f, K) = 0 \) for any \( f \in I \), thus \( K \to \hat{K} \) is an isomorphism is we inductively use the stupid truncation (3.3.3.6). \( \square \)

Cor. (4.6.6.14). If \( M \) is an \( A \)-module, then \( H^0(\hat{M}) \) is the derived-I-completion in the category of modules, by (3.4.2.12).

Cor. (4.6.6.15). (4.6.6.2) show the notion of derived I-complete and derived I-completion only depends on \( \text{rad} I \).

**Principal Ideal Case**

Prop. (4.6.6.16) [Bounded Torsion and Derived Completion]. Let \( A \) be a commutative ring and \( f \in A \). If \( M \) is an \( A \)-module that has bounded \( f^\infty \)-torsion, then the derived \( f \)-completion of \( M \) as a complex is a module and coincides with the classical \( f \)-adic completion.

**Proof:** The derived \( f \)-completion is defined to be

\[
\hat{M} = R\lim_n (M \otimes_{\mathbb{Z}[X]} \mathbb{Z}[X]/(x^n)) = R\lim_n (M \xrightarrow{f^n} M).
\]

So by (3.4.6.5), there are exact sequences

\[
R^1\lim_n M/f^n M \cong H^1(\hat{M})
\]

\[
0 \to R^1\lim_n M[f^n] \to H^0(\hat{M}) \to \lim_n M/f^n \to 0
\]

\[
H^{-1}(\hat{M}) \cong \lim_n M[f^n]
\]

Now the hypothesis implies that \( (M[f^n]) \) is Mittag-Leffler and \( \lim_n M[f^n] = 0 \), so we have the desired result. \( \square \)

Cor. (4.6.6.17). Let \( R \) be a perfect \( \mathbb{F}_p \)-algebra, then the derived \( p \)-completion and \( p \)-adic completion of \( R \) coincide.
7 Derived Completely Properties

Def. (4.6.7.1) [Derived Completely Properties]. Let $A$ be a commutative ring and $I$ is a f.g. ideal, then $M \subset D(A)$ is called $I$-completely (faithfully) flat/smooth/étale/… if $M \otimes^L_A A/I$ is discrete and is a (faithfully) flat $A/I$-module.

$M$ is said to have finite $I$-completely Tor amplitude if $M \otimes^L_A A/I$ is is a bounded complex in $D(A/I)$.

Clearly, any flat/smooth/étale $A$-module $M$ is $I$-completely flat/smooth/étale/… for any $I$. And $M$ has finite $I$-completely flatness if $M$ has a finite resolution of flat $A$-modules.

Prop. (4.6.7.2) [I-Completely F.F. Descent]. If $A \to B \to B'$ are ring maps and $I$ is an ideal of $A$,

1. If $C$ is a $B$-algebra and $B$ is $I$-completely f.f. over $A$, then $C$ is $I$-completely (f.)f. over $A$ iff $C$ is $I$-completely (f.)f. over $B$.

2. If $B \to B'$ is $I$-completely flat, $M$ is a $B$-module, then $M$ is $I$-completely flat over $A$ iff $M \otimes^L_B B'$ is $I$-completely flat over $A$.

Proof: 1: One direction is easy, for the other, if $C$ is $I$-completely (f.)f. over $A$, then

$$C \otimes^L_A A/I = C \otimes^L_B B \otimes^L_A A/I = (C \otimes^L_B B/I) \otimes_B/I (B \otimes^L_A A/I)$$

is a discrete and (f.)f. $C/I$-module iff $(C \otimes^L_B B/I)$ does, as $(B \otimes^L_A A/I)$ is f.f. over $B/I$.

2: This is because $(B' \otimes^L_B M) \otimes^L_A A/I \cong B' \otimes^L_B (M \otimes^L_A A/I)$. \hfill \Box

Prop. (4.6.7.3). If $I$ is generated by a Koszul-regular sequence, then any $A$-module $M$ has finite $I$-completely Tor amplitude.

Proof: This is because $A/i \cong A \otimes^L_{\mathbb{Z} \langle X_1, \ldots, X_n \rangle} \mathbb{Z}$ in this case, so $M \otimes^L_A A/I \cong M \otimes^L_{\mathbb{Z} \langle X_1, \ldots, X_i \rangle} \mathbb{Z}$, which has f.m. homology groups because $\mathbb{Z}$ has a finite free $\mathbb{Z}[X_1, \ldots, X_n]$-resolution (4.4.4.1). \hfill \Box

Prop. (4.6.7.4) [I-Completely Flatness and Derived Completion]. Let $A$ be a commutative ring and $I$ be f.g., then the derived $I$-completion of a $I$-completely (faithfully) flat/étale $M$ is $I$-completely (faithfully) flat/étale, both the complex and the module. In fact, $H^0(\hat{M}) \otimes^L_A A/I \cong \hat{M} \otimes^L_A A/I \cong M \otimes^L_A A/I$.

Proof: Because objects in the image of $D(A/I) \to D(A)$ are all derived $I$-complete, by (4.6.6.7), so there is an isomorphism $M \otimes^L_A A/I \cong \hat{M} \otimes^L_A A/I$ for any $M$, because they are both left adjoint to $\text{Mod}_{A/I} \subset D(A)$, by the definition of derived $I$-completion and (4.6.2.10). So $\hat{M} \otimes^L_A A/I \cong M \otimes^L_A A/I = M \otimes_A A/I$, which is a flat $A/I$-module. \hfill \Box

Prop. (4.6.7.5) [Flatness and Completed Derived Tensor]. The completed derived tensor of an $I$-completely flat/étale module is discrete and $I$-completely flat/étale.

Proof: If $M$ is an $I$-completely flat $A$-module, then $M \hat{\otimes}^L_A B$ is $I$-complete and $I$-completely flat by (4.6.7.4), and $(M \hat{\otimes}^L_A B) \otimes^L_B B/I = H^0(M \hat{\otimes}^L_A B) \otimes^L_B B/I = M \otimes^L_A B/I$, because they are both left adjoint of the forgetful functor $\text{Mod}_{B/I} \subset D(A)$. Then we have $M \hat{\otimes}^L_A B \cong H^0(M \hat{\otimes}^L_A B)$ is discrete, as they are both $I$-complete, by (4.6.6.2) and derived Nakayama. \hfill \Box

Prop. (4.6.7.6). $A$ is derived $I$-completely flat iff $A$ is $I^n$-completely flat for any $n > 0$. Moreover, in this case, $A$ is derived $J$-completely flat for any ideal $J$ that $I \subset \text{rad } J$. 

Proof: The exact sequence
\[ 0 \to I/I^2 \to A/I^2 \to A/I \to 0 \]
induces distinguished triangles
\[ (M \otimes^L_A A/I) \otimes^L_{A/I} I/I^2 \to M \otimes^L_A I/I^2 \to M \otimes^L_A A/I^2 \to M \otimes^L_A A/I \]
which shows \( M \otimes^L_A I/I^2 \) is discrete, \( = N \). Then \( N \) is an \( A/I^2 \)-module that \( N \otimes^L_{A/I^2} A/I = M/IM \) is \( A/I \)-flat. Then \( N \) is \( A/I^2 \)-flat: for any \( A/I^2 \)-module \( L \), let \( L' = IL \) and \( L'' = L/IL \) which are both \( A/I \)-modules, then there is a distinguished triangle
\[ N \otimes^L_{A/I^2} L' \to N \otimes^L_{A/I^2} L \to N \otimes^L_{A/I^2} L'' \]
and
\[ N \otimes^L_{A/I^2} L' = (N \otimes^L_{A/I^2} A/I) \otimes^L_{A/I} L' = (M/IM) \otimes^L_{A/I} L' \]
\[ N \otimes^L_{A/I^2} L'' = (N \otimes^L_{A/I^2} A/I) \otimes^L_{A/I} L'' = (M/IM) \otimes^L_{A/I} L'' \]
are both discrete, hence so does \( N \otimes^L_{A/I^2} L \), implying it is \( A/I^2 \)-flat.

In a similar fashion, we can show \( M \) is \( I/I^n \)-flat for any \( n \). And if \( I \subseteq \text{rad} J \), then \( I^n \subseteq J \), so \( M \otimes^L_A A/J = (M \otimes^L_A A/I^n) \otimes^L_{A/I^n} A/J \) is discrete and \( A/J \)-flat. \( \square \)

Prop. (4.6.7.7). Let \( A \) be a ring and \( I \) be an invertible ideal, then any derived \( (p, I) \)-complete and \( (p, I) \)-completely flat \( A \)-complex \( \mathcal{M} \in \mathcal{D}(A) \) is discrete and \( (p, I) \)-complete. Moreover, for any \( n \geq 0 \), we have \( M[I^n] = 0 \) and \( M/I^n M \) has bounded \( p^\infty \)-torsion.

Proof: \( M \) is \( (I^n, p) \)-completely flat by (4.6.7.6), so we have \( M \otimes^L_A A/I^n \) is \( p \)-completely flat in \( D(A/I^n) \). Notice that \( A/I^n \) has bounded \( p^\infty \)-torsion by induction (\( I \) invertible used), (4.6.7.11) says \( M \otimes^L_A A/I^n \) is discrete in \( D(A/I^n) \) and has bounded \( p^\infty \)-torsion, and is \( p \)-adically complete. In particular,
\[ M \otimes^L_A A/I^n = (M \otimes^L_A A/I^{n+1}) \otimes^L_{A/I^{n+1}} A/I^n \]
So if we denote \( M \otimes^L_A A/I^n = M_n \), then \( M_n = M_{n+1}/I^n M_{n+1} \), as \( M \) is derived \( I \)-complete, we have \( M = R \text{lim} (M \otimes^L_{A/I^n} A/I^n) \), so clearly \( M \) is discrete. And then we have \( M \otimes^L_{A/I^n} A/I^n = M/I^n M \), which means \( M[I^n] = 0 \), and \( M/I^n M \) has bounded \( p^\infty \)-torsion. Now because \( M \) is derived \( (p, I) \)-complete,
\[ M = R \text{lim}((M \otimes_{A/I^n} A/I^n \xrightarrow{p^n} A/I^n)) = R \text{lim}(M/I^n \xrightarrow{p^n} M/I^n) = R \text{lim}(M/(I^n, p^n)) \]
is \( (p, I) \)-complete. \( \square \)

Lemma (4.6.7.8). Let \( C \) be a commutative ring with a f.g. ideal \( J \), and \( D \) a \( C \)-algebra that has finite \( J \)-complete Tor amplitude, then the \( J \)-completed base change operator \( - \otimes^L_C D \) commutes with totalization in \( \mathcal{D}^{\geq 0}(C) \) and \( \mathcal{D}^{\geq 0}(D) \), i.e. \( M \) is a cosimplicial object with in \( \mathcal{D}^{\geq 0}(C) \) with totalization \( M \), then
\[ \text{Tot}(M^\bullet) \otimes^L_C D \cong \text{Tot}(M^\bullet \otimes^L_C D) \]
via the natural map.

Proof: Cf. [Scholze, Prism, 4.22]. \( \square \)
Prop. (4.6.7.9) [Elkik’s Algebrization Theorem]. Let $A$ be a commutative ring and $I$ is a f.g. ideal, then an $A$-algebras is derived $I$-completely étale/smooth iff it is the derived $I$-completion of some étale/smooth $A$-algebra.

Proof: if it is the derived $I$-completion of some étale/smooth algebra, then it is derived $I$-completely étale/smooth by (4.6.7.4). Converse, Cf. [A. Arabia, “Relèvements des algèbres lisses et de leurs morphismes”, Commentarii Mathematici Helvetici 76 (2001), 607–639.]. □

Lemma (4.6.7.10). Let $A$ be a ring, if $M$ is an $A$-module with bounded $f^\infty$-torsion, i.e. $M[f^\infty] = M[f^c]$ for some $c > 0$, then there are maps

$$(M \xrightarrow{f^n} M) \to M/f^n M, \quad M/f^{n+c} \to (M \xrightarrow{f^n} M)$$

in $D(A)$ inducing an equivalence between two pro-objects $\{M \xrightarrow{f^n} M\}$ and $\{M/f^n\}$.

Proof: The first map is obvious, for the second map, use the following commutative diagram:

$$
\begin{array}{ccc}
M/M[f^c] & \xrightarrow{f^{n+c}} & M \\
\downarrow{f^c} & & \downarrow \\
M & \xrightarrow{f^n} & M
\end{array}
$$

the upper row is injective thus isomorphic to $M/f^{n+c}M$, then this gives the map. It can be checked that this is an equivalence of pro-objects. □

Prop. (4.6.7.11). Let $A$ be a commutative ring that has bounded $f^\infty$-torsion, then for a $M \in D(A)$, the following is equivalent:

- $M$ is derived $f$-complete and $f$-completely flat.
- $M$ is discrete and is represented by a $f$-adically complete module that $M/f^n M$ is $A/f^n$-flat for any $n > 1$ and $M$ has bounded $f^\infty$-torsion.

Furthermore, in this case, $M \otimes_A A[f^\infty] = M[f^\infty]$.

Proof: By (4.6.7.10), $\{A/f^n A\}$ and $\{Kos(A, f^n)\}$ are two equivalence pro-objects in $D(A)$. So if 1 or 2 holds, then $M$ is derived $f$-complete, so

$$M = R\lim(M \otimes^L_A Kos(A, f^n)) = R\lim(M \otimes^L_A A/f^n A).$$

Now if 1 holds, then $M_n = M \otimes_A A/f^n A$ is discrete by (4.6.7.6), and $M_n = M_{n+1}/f^n M_{n+1}$ is surjective:

$$M \otimes^L A A/f^n A = (M \otimes^L_A A/f^{n+1} A) \otimes^L_{A/f^{n+1}} A/f^n.$$

So $M = R\lim(M \otimes^L_A A/f^n A)$ is discrete. Then $M \otimes_A A/f^n = M \otimes^L_A A/f^n$ is flat over $A/f^n$.

Next we prove $M \otimes_A A[f^\infty] = M[f^\infty]$: There is an exact sequence

$$0 \to (A[f^n])[1] \to Kos(A, f^n) \to A/f^n \to 0$$

Then tensoring $M \otimes^L_A$ gives a distinguished triangle

$$(M \otimes^L_A A[f^n])[1] \to Kos(M, f^n) \to M \otimes^L_A A/f^n.$$
Notice that
\[ M \otimes_A^L A[f^n] = (M \otimes_A^L A/f^n) \otimes_{A/f^n}^L A[f^n] = M \otimes_A^L A[f^n] \]
by flatness, so the distinguished triangle shows \( M \otimes_A^L A[f^n] \sim H^{-1}(Kos(M, f^n)) = M[f^n]. \)
Conversely, if 2 holds, then there are equivalences of pro-objects
\[ \{ M \otimes_A^L A[f^n] \} \sim \{ M \otimes_A^L Kos(A, f^n) \} = \{ Kos(M, f^n) \} \sim \{ M/f^nM \} \]
by (4.6.7.10) as \( M \) has bounded \( f^\infty \)-torsion. So
\[ \hat{M} = R\lim \{ M \otimes_A^L Kos(A, f^n) \} = R\lim \{ M/f^nM \} = M[0] \]
so \( M \) is derived \( p \)-complete. And the constant system
\[ \{ M \otimes_A^L A/f \} = \{ M \otimes_{A/f^n}^L A/f^n \otimes_{A/f^n}^L A/f \} \sim \{ M/f^nM \otimes_{A/f^n}^L A/f \} = \{ M/fM \} \]
where we used \( M/f^nM \) is \( A/f^n \)-flat. So \( M \otimes_A^L A/f \sim M/fM \) is flat over \( A/f \). \( \square \)

8 Duality

Def. (4.6.8.1) [Dualizing Complexes]. Let \( A \) be a Noetherian ring, then a dualizing complex for \( A \) is a complex \( \omega_A \in D(A) \) s.t.
- \( \omega_A \) has finite injective dimension.
- \( H^i(\omega_A) \) are all finite \( A \)-modules.
- \( A[0] \rightarrow \text{RHom}(\omega_A, \omega_A) \) is a quasi-isomorphism.

Prop. (4.6.8.2) [Dualizing Complex is Local]. Let \( A \) be a Noetherian ring,
- If \( B = S^{-1}A \) and \( \omega_A \in D(A) \) is a dualizing complex for \( A \), then \( \omega_A \otimes_A^L B \) is a dualizing complex for \( B \).
- If \( (f_1, \ldots, f_n) = (1) \in A \), and \( \omega_A \in D(A) \) satisfies \( (\omega_A)_{f_i} \) are dualizing complexes for \( A_{f_i} \) for any \( i \), then \( \omega_A \) is a dualizing complex for \( A \).

Proof: Cf. [Sta]0A7G, 0A7H. \( \square \)

Def. (4.6.8.3) [Dualizing Modules]. Let \( (A, \mathfrak{m}, k) \) be a Noetherian local ring and \( \omega_A \) a normalized dualizing complex for \( A \), then \( [\omega_A] = H^{-\dim A}(\omega_A) \) is called a dualizing module for \( A \).

Def. (4.6.8.4) [Relative Dualizing Complex]. Cf. [Sta]0E9M.

Quasi-Finite Case
Cf. [Sta]Chap49.4.

Prop. (4.6.8.5).
4.7 Divided Power Algebras

Basics

Def. (4.7.0.1) [PD-Structures]. Let \( I \) be an ideal of a commutative ring \( A \), a divided power structure or \( \text{pd-structure} \) on \( I \) is a collection of maps \( I_n : I \to A, n \geq 0 \) that

- \( \gamma_0(x) = 1, \gamma_1(x) = x, \gamma_n(x) \in I \forall n. \)
- \( \gamma_n(x + y) = \sum \gamma_{n-i}(x)\gamma_i(y). \)
- \( \gamma_n(\lambda x) = \lambda^n \gamma_n(x), \lambda \in A, x \in I. \)
- \( \gamma_n(x)\gamma_n(y) = \binom{m+n}{n} \gamma_{m+n}(x). \)
- \( \gamma_n(\gamma_m(x)) = \binom{m+n}{m}\gamma_{m+n}(x). \)

It is a simulation of the divided power \( \gamma_n(x) = x^n \) in case \( n! \) is definable.

A divided power ring is a triple \((A, I, \gamma)\) where \( I \) is an ideal of a commutative ring \( A \) and \( \gamma \) is a pd-structure on \( I \). A morphism of divided power rings is a morphism of pairs \((A, I)\) that preserves pd-structures.

For a pd-structure \((A, I)\), denote \( I[n] \) the ideal generated by \( \prod_i \gamma_n(x_i) \) where \( x_i \in I \) and \( \sum n_i \geq n \).

Prop. (4.7.0.2) [Limits and Colimits]. The category of divided power rings has all limits and colimits, the limits commute with forget functors but the colimits don’t. However, the colimit always commutes with the functor taking \((A, I)\) to \( A/I \). This can be seen from the universal property of colimit applied to the pd-structures that \( I = 0 \).

Proof: The construction of the limit is clear. For the colimits, we use representability criterion (3.1.1.28), Cf. [[Sta]07GX]?

Prop. (4.7.0.3). Let \( A \) be a ring and \( I \) an ideal of \( A \), then if \( \gamma \) is a pd-structure on \( I \), then \( n!\gamma(x) = x^n \).

Proof: If \( \gamma \) is a pd-structure, then we have \( n\gamma_n(x) = \gamma_1(x)\gamma_{n-1}(x) \), so we can use induction.

Prop. (4.7.0.4). If \( I, J \) are two ideals of \( A \) and \( \gamma \) a pd-structure on \( I \) and \( \delta \) a pd-structure on \( J \), then

- \( \gamma, \delta \) agree on \( IJ \).
- \( \gamma, \delta \) agree on \( I \cap J \), then they extends to a pd-structure on \( I + J \).

Proof: 1: for \( x \in I, y \in J, \gamma_n(xy) = y^n\gamma_n(x) = n!\delta_n(y)\gamma_n(x) = \delta(xy). \)

2: direct calculation.

Prop. (4.7.0.5) [p-Nilpotent and Thickening]. Let \( p \) be a prime and \((A, I, \gamma)\) a pd-structure. Assume \( p \) is nilpotent in \( A/I \), then \( I \) is locally nilpotent iff \( p \) is nilpotent in \( A \), equivalently \((A, I, \gamma)\) is a pd-thickening.

Proof: If \( p^N = 0 \in A \), then for any \( x \in I, x^{pN} = (pN)!\gamma_{pN}(x) = 0. \) Then converse is trivial.

Constructing PD-Structures

Prop. (4.7.0.6) [\( \mathbb{Z}_p \)-Algebras]. Cf. [[Sta]07GN].

Prop. (4.7.0.7). Let \( A \) be a \( \mathbb{Z}_p \)-algebra and \( I \) is an ideal, then two pd-structures \( \gamma, \gamma' \) on \( \gamma \) are equal iff \( \gamma_p = \gamma' \). Moreover, given a map \( \delta : I \to I \) that
\begin{itemize}
\item $p!\delta(x) = x^p$,
\item $\delta(ax) = a^p \delta(x)$ for any $a \in A, x \in I$,
\item $\delta(x + y) = \delta(x) + \delta(y) + \sum_{i+j=p,i,j>0} \frac{1}{i!j!} x^i y^j$.
\end{itemize}

Then there exists a unique pd-structure on $I$ that $\gamma_p = \delta$.

\textbf{Proof:} Just notice that $\gamma_n(x) = dx\gamma_{n-1}(x)$ for some $c$ invertible in $\mathbb{Z}_{(p)}$, and also $\gamma_{pm}(x) = c\gamma_m(\gamma_p(x))$ for some $c$ invertible in $\mathbb{Z}_{(p)}$, thus $\gamma$ is uniquely determined, and we can also define $\gamma_n$ inductively in this way, and the verification of axioms in in[[Sta]07GS].

\textbf{Prop. (4.7.0.8).} Let $A$ be a $\mathbb{Z}$-torsion-free ring and $I$ an ideal of $A$, then:
\begin{itemize}
\item $I$ has at most one pd-structure.
\item if $\gamma_n : I \to I$ are maps, then $\gamma$ is a pd-structure iff $n!\gamma_n(x) = x^n$.
\item $I$ has a pd-structure iff there is a set of generators $\{x_i\}$ of $I$ that $x_i^n \in n!I$.
\end{itemize}

\textbf{Proof:} 1 is clear from (4.7.0.3).
2: because $A \subset A \otimes_{\mathbb{Z}} \mathbb{Q}$, we can verify in $A \otimes_{\mathbb{Z}} \mathbb{Q}$, then the verifications are trivial.
3: Use the axioms to extend linearly and additively.

\textbf{Prop. (4.7.0.9) [DVR].} If $R$ is a DVR in char $0$ with residue field of char $p$ and ramification $p$ and maximal ideal $m$, then $m$ has a pd-structure iff $e \leq p - 1$.

\textbf{Proof:} As $R$ has char $0$, it has at most one pd-structure by (4.7.0.8), and we need to show that $x^n/n!$ is in $m$ for any $x \in m$. And using (20.1.2.2), we are done.

\textbf{Extending PD-Structure}

\textbf{Def. (4.7.0.10) [Extending PD-Structure].} Let $(A, I, \gamma)$ be a pd-structure and $B$ is an $A$-algebra, we say that $\gamma$ extends to $B$ if $A \to B$ extends to a morphism of pd-structures $(A, I, \gamma) \to (B, IB, \gamma')$.

Let $(A, I), (B, J)$ be two pd-structures and $B$ is an $A$-algebra, then these two pd-structures are said to be compatible iff the pd-structure on $A$ extends to $B$ and the pd-structure on $J$ and $IB$ coincides, or equivalently, there is a pd-structure on $IB + J$ compatible with $IB$ and $J$, by (4.7.0.4).

\textbf{Prop. (4.7.0.11) [Extendability].} Let $(A, I)$ is a pd-structure and $B$ an $A$-algebra, if any of the following holds:
\begin{itemize}
\item $IB = 0$,
\item $I$ is principal,
\item $B[I] = 0$, (e.g. $A \to B$ is flat).
\end{itemize}

then $\gamma$ extends to $B$.

\textbf{Proof:} 1 is trivial.
2: if $I = (x)$, we define $\gamma_n(bx) = b^n \gamma_n(x)$. This is well defined: if $(b - b')x = 0$, then $(b^n - (b')^n)\gamma_n(x) = 0$ because $\gamma_n(x) \in (x)$. Verifications of axioms is routine.
3: the condition shows $I \otimes_A B \cong IB$, thus it suffices to define $\gamma$ on $I \otimes_A B$. For this we define on $I \otimes B$ and descend: let $\gamma_n((x, b)) = b^n \gamma_n(x)$ and extend by freeness and axioms in (4.7.0.1), then it is easy to show it is bi-additive and $A$-linear, so descend to $I \otimes B$ by (2.2.4.13).
Prop. (4.7.0.12) [PD-Structure and Completions]. Let \((A, I, \gamma)\) be a pd-structure that \(p\) is nilpotent in \(A/I\), then each \(\gamma_n\) is continuous in the \(p\)-adic topology and extends to a pd-structure \(\hat{\gamma}\) on \(\hat{I}\).

If moreover \(A\) is a \(\mathbb{Z}(p)\)-algebra, then for \(e\) large, \(p^e A \in I\) is preserved by \(\gamma\) and

\[
(\hat{A}, \hat{I}, \hat{\gamma}) = \text{colim}_e (A/p^e A, I/p^e A, \gamma).
\]

**Proof:** Let \(p^t \in I\), then 1 follows from (4.2.3.8). \(\gamma_n\) is clearly continuous, and \(\gamma_n\) preserves \(p^e A\) because

\[
\gamma_n(p^e a) = p^n \gamma_n(p^{e-1} a) = \frac{p^n}{n!} p^{n(e-1)} a^n \in p^e A.
\]

The limit equation follows from (4.7.0.2). \(\square\)

Prop. (4.7.0.13) [Quotient]. Let \((A, I, \gamma)\) be a pd-structure and \(a \subset A\) is an ideal, and \(I' = I \cap a\), then the following are equivalent:

1. \(\delta\) extends to \(A/a\).
2. \(I'\) is preserved by \(\gamma\).
3. There is a set of generator \(x_i\) of \(I'\) that \(\gamma_n(x_i) \in I'\) for all \(n, i\).

**Proof:** \(1 \rightarrow 2 \rightarrow 3\) is clear. \(2 \rightarrow 1\): we can just define \(\gamma(x + I) = \gamma(x) + I\), which is well defined by axiom 2 of (4.7.0.1). \(3 \rightarrow 2\) is clear. \(\square\)

Def. (4.7.0.14) [Free PD-Algebra]. For a pd-structure \((A, I, \delta)\), the **free pd-algebra** \(A(t_1, \ldots, t_n)\) is defined to be the \(A\)-algebra generated by symbols \(t_i^{[n]}\), where \(n > 0\), modulo the algebraic relations \(t_i^{[m]} t_j^{[n]} = (m+n) t_i^{[m+n]}\). Denote by \(A(t_1, \ldots, t_n)_+\) the ideal generated by \(t_i^{[n]}\) where \(n > 0\).

Then the ideal \(J\) generated by \(I\) and \(A(t_1, \ldots, t_n)_+\), where \(n > 0\) has a unique pd-structure that \(\gamma_n(t_i) = t_i^{[n]}\) and \((A, I, \delta) \rightarrow (A(t_1, \ldots, t_n), J, \gamma)\) is a morphism of pd-structures.

It has a universal property that \(\text{Hom}((A(t_1, \ldots, t_n), J, \gamma), (C, K, \varepsilon))\) is the same as \(\text{Hom}((A, I, \delta), (C, K, \varepsilon))\) with specified \(n\) elements in \(K\).

**Proof:** Because \(IA(t_i) \cap A(t_1, \ldots, t_n)_+ = IA(t_i) + A(t_1, \ldots, t_n)_+,\) by (4.7.0.4), it suffices to construct pd-structures on \(IA(t_i)\) and \(A(t_1, \ldots, t_n)_+\). The former is by (4.7.0.11) and for the latter: if \(A\) is torsion-free, then we can use (4.7.0.8) because \(\gamma_m(x)^n = n! \gamma_n(\gamma_m(x)) = \frac{(mn)!}{(m!)^n} \gamma_{mn}(x) \in n! A(t_1, \ldots, t_n)_+\). In general, we write \(A = R/a\) where \(R\) is a torsion-free pd-structure (can choose \(\mathbb{Z}(A)\)), so there is a pd-structure on \(R(t_i)\), and \(\gamma(t_i)^+/a(t_i) = A(t_i)\), then we can use (4.7.0.13) to construct a pd-structure on \(A(t_i)\) compatible with that of \(A\).

The verification of universal property is omitted. \(\square\)

PD-Envelopes

Prop. (4.7.0.15) [PD-Envelope]. Let \((A, I, \gamma)\) be a pd-structure, then there is a **pd-envelope** functor \((B, J) \rightarrow (D_B(J), \overline{J}, J)\) from the the category of pairs over \((A, I)\) to the category of pd-structures over \((A, I, \gamma)\) that is left adjoint to the forgetful functor.

In particular, by the universal property of pd-envelope, there is a morphism \((B, J) \rightarrow (D_B(J), \overline{J}) \rightarrow (B/J, 0)\) of pairs, so in particular \(D/\overline{J} \rightarrow B/J\) is surjective.
Proposition (4.7.0.16) [PD-Envelope of Quotients]. Let \((A, I, \gamma)\) be a pd-structure and \(\varphi : B' \to B\) be a surjection of \(A\)-algebras with kernel \(K\). Let \(IB \subset J \subset B\) be an ideal and \(J' = \varphi^{-1}(J)\) and \(D_{B', \gamma}(J') = (D', \mathcal{J}', \gamma)\), then \(D_{B, \gamma}(J) = (D'/K', \mathcal{J}'/K', \gamma)\) where \(K'\) is the ideal generated by all \(\gamma(k)\) for \(n \geq 0\) and \(k \in K\).

Proof: There is a pd-structure on \((D'/K', \mathcal{J}'/K', \gamma)\) by (4.7.0.13). A map of pairs \((B', J') \to (T, I', \gamma)\) is equivalent to a map of pairs \((B', J') \to (T, I', \gamma)\) that vanishes on \(K\), or a map of pd-structures \((D', \mathcal{J}', \gamma) \to (T, I', \gamma)\) that vanishes on \(\gamma(k)\), thus this is clearly represented by \((D'/K', \mathcal{J}'/K', \gamma)\).

Proposition (4.7.0.17). If \((A, I)\) is a pd-structure and \((B, J)\) is a pair over \((A, I)\), then

\[D_{B[X_i], \gamma}(JB[X_i] + (X_i)) \cong D_{B, \gamma}(J)(X_i)\]

Proof: This follows from the universal property of free pd-structure (4.7.0.14).

PD-Structures and \(\delta\)-Rings

Lemma (4.7.0.18). If \(A\) is a \(p\)-torsionfree \(\mathbb{Z}_p\)-\(\delta\)-ring, denote \(\gamma_n(z) = \frac{z^n}{n!}\). If \(z \in A\) satisfies \(\gamma_p(z) \in A\), then \(\gamma_n(z) \in A\) for any \(n\).

Proof: WARNING: this is not an easy consequence of power counting. We first prove for \(n = p^2\); as \(A\) is a \(\delta\)-ring, \(\delta(\frac{z^p}{p}) \in A\)

\[\delta(\frac{z^p}{p}) = \frac{1}{p} (\frac{\varphi(z)^p}{p} - \frac{z^{p^2}}{p^2}) = \frac{(zp^p + p \delta(z))^p - z^{p^2}}{p^{p+1}} \in A.\]

The first term is \(A\) by assumption, thus the second term is also in \(A\), proving the case for \(n = p^2\).

Now for general \(n\), it suffices to prove for \(n = kp\). But it can be checked that \(\gamma_{nk}(z) = u\gamma_k(\gamma_p(z))\) where \(u\) is a unit. Now by what we just proved, we can use induction hypothesis for \(z = \gamma_p(z)\), and conclude that \(\gamma_{nk}(z) \in A\).

Proposition (4.7.0.19). The ring \(C = \mathbb{Z}_p\{x, \frac{\varphi(x)}{p}\}\) identifies with the pd-envelope \(D = D_{\mathbb{Z}_p\{x\}}(x) = \mathbb{Z}_p\{x\}[[\gamma_n(x)]]\) where \(\gamma_n(x) = \frac{x^n}{n!}\). Moreover, it also equals to \(\mathbb{Z}_p\{X_1, X_2, \ldots\}/(x, x^p, pX_2 - X_1, \ldots)\).

Proof: It suffices to show that the smallest \(\delta\)-ring of \(\mathbb{Z}_p\{x\}\) containing \(\mathbb{Z}_p\{x\}\) and \(\frac{\varphi(x)}{p}\) is the same as the smallest ring of \(\mathbb{Z}_p\{x\}\) containing \(\mathbb{Z}_p\{x\}\) and \(\frac{\varphi(x)}{p}\).

\(D \subset C\) is immediate from (4.7.0.18). To show \(C \subset D\), notice \(\frac{\varphi(x)}{p} \in D\), it suffices to show \(\varphi\) preserves \(D\), or equivalently, \(\varphi(y) - y^n \in pD\) for any \(y \in D\). Now

\[\varphi(x^n) = \frac{(x^p + p \delta(x))^n}{n!} = \sum_{i=0}^{n} \binom{n}{i} \frac{(p)^i (x^{n-i})}{n!}, \delta(x)^{n-i}\]
The coefficients
\[
\frac{\binom{n}{i}(p)^i}{n!}p^{n-i}
\]
are all in \(p\mathbb{Z}(p)\), thus \(\varphi\left(\frac{x^n}{m!}\right) \in pD\). On the other hand,
\[
\left(\frac{x^n}{n!}\right)^p = \gamma_p(\gamma_n(x)) = u\gamma_{pn}(x) \cdot p! \in pD
\]
where \(u\) is a unit in \(\mathbb{Z}(p)\) by (4.7.0.1), thus we are done. \(\square\)

**Lemma (4.7.0.20).** If \(A\) is a \(p\)-torsionfree (equivalently, flat) \(\mathbb{Z}(p)\)-algebra and \((a, p)\) is a regular sequence in \(A\), then \(D_A((a)) \cong A \otimes_{\mathbb{Z}(p)} D_{\mathbb{Z}(p)}((x)) = A[X_1, X_2, \ldots]/(pX_1 - a^p, pX_2 - X_1^p, \ldots)\).

**Proof:** By (4.7.0.19),
\[
A \otimes_{\mathbb{Z}(p)} D_{\mathbb{Z}(p)}((x)) = A \otimes_{\mathbb{Z}(p)} \{ [\gamma_n(x)] \} = A[X_1, X_2, \ldots]/(a^p - pX_1, X_1^p - pX_2, X_2^p - pX_3, \ldots)
\]
thus there is a natural map from \(A \otimes_{\mathbb{Z}(p)} D_{\mathbb{Z}(p)}((x))\) to \(D_A((a))\) given by
\[
X_k \mapsto \frac{a^p}{p^{\text{ord}_p(n)}} = \frac{a^p}{p^1 + p^2 + \cdots + p^{k-1}} \in D_A((a)).
\]
It is surjective, and it is an isomorphism when inverting \(p\). Thus the kernel are all \(p^\infty\)-torsions. Then to show it is an isomorphism, it suffices to show \(A[X_1, X_2, \ldots]/(a^p - pX_1, X_1^p - pX_2, X_2^p - pX_3, \ldots)\) is \(p\)-torsion-free. It is a filtered colimit, so it suffices to show \(A[X_1, \ldots, X_n]/(a^p - pX_1, X_1^p - pX_2, X_2^p - pX_3, \ldots, X_n^p - pX_n)\) is \(p\)-torsionfree.

For this, it suffices to prove \(A' = A[X_1, \ldots, X_k]/(px_1 - a^k, px_2 - x_1^k, \ldots, px_k - x_{k-1}^p)\) is \(p\)-torsionfree. If we denote \(K(R) = K(R[X_1, \ldots, X_n], px_1 - a^k, px_2 - x_1^k, \ldots, px_k - x_{k-1}^p)\) for any ring \(R\), then we have a distinguished triangle
\[
K(A) \xrightarrow{p} K(A) \rightarrow K(Kos(A[X_1, \ldots, X_k], p)) = K(A/p)
\]
as \(A\) is \(p\)-torsionfree. Now we can consider the spectral sequence associated to this distinguished triangle. Notice first that \((px_1 - a^k, px_2 - x_1^k, \ldots, px_k - x_{k-1}^p)\) is a regular sequence in \(A'/p\), which is clear. So the \(E_1\) page looks like
\[
\begin{array}{cccc}
A' & \overset{p}{\longrightarrow} & A' & \longrightarrow A'/p \\
\uparrow & & \uparrow & \\
* & \longrightarrow & * & \longrightarrow 0 \\
\uparrow & & \uparrow & \\
* & \longrightarrow & * & \longrightarrow 0 \\
\uparrow & & \uparrow & \\
\vdots & \longrightarrow & \cdots & \longrightarrow \cdots
\end{array}
\]
and the \(E_2\) page is of the form
\[
\begin{array}{cccc}
A'[p] & \overset{p}{\longrightarrow} & 0 & \longrightarrow 0 \\
\uparrow & & \uparrow & \\
* & \longrightarrow & * & \longrightarrow 0 \\
\uparrow & & \uparrow & \\
* & \longrightarrow & * & \longrightarrow 0 \\
\uparrow & & \uparrow & \\
\vdots & \longrightarrow & \cdots & \longrightarrow \cdots
\end{array}
\]
This spectral sequence converges to 0, so $A'[p] = 0$, we win. □

Prop.(4.7.0.21) [PD-Envelope for Regular Sequence]. Let $A$ be a $p$-torsionfree $\delta$-ring and $p, f_1, \ldots, f_r$ define a regular sequence in $A$, then $A\{\frac{\varphi(f_1)}{p}, \ldots, \frac{\varphi(f_r)}{p}\}$ identifies with the pd-envelope $D_A(I)$ of $I = (f_1, \ldots, f_r)$ as a subring of $A[\frac{1}{p}]$.

Proof: In case $r = 1$, $A\{\frac{\varphi(f_1)}{p}\} = A \otimes_{\mathbb{Z}(p)} \mathbb{Z}(p) \{x, \varphi(x)\} = A \otimes_{\mathbb{Z}(p)} \mathbb{Z}(p)((x)) \cong D_A((f_1))$ by (4.7.0.20).

The general case follows from this, by considering the tower

$$
(A, (f_1)) \to (A, (f_2)) = (A\{\frac{\varphi(f_1)}{p}\}, (f_2))
$$

$$
\to (D_A\{\frac{\varphi(f_1)}{p}\}(f_3)) = (A\{\frac{\varphi(f_1)}{p}, \frac{\varphi(f_2)}{p}\}, (f_3))
$$

$$
\to \ldots = A\{\frac{\varphi(f_1)}{p}, \ldots, \frac{\varphi(f_r)}{p}\}
$$

The equations are true because $(p, f_k)$ are regular in $A\{\frac{\varphi(f_1)}{p}, \ldots, \frac{\varphi(f_{k-1})}{p}\}$:

$$
A\{\frac{\varphi(f_1)}{p}, \ldots, \frac{\varphi(f_{k-1})}{p}\}/p = A/p[X_{11}, X_{12}, \ldots, X_{21}, X_{22}, \ldots, X_{k-1,1}, X_{k-1,2}, \ldots]
$$

and $f_k$ is a nonzero-divisor in it because it is a non-zero divisor in $A/(p, f_{k-1}^p)$, as $(p, f_{k-1}^p, \ldots, f_k^p)$ is also a regular sequence by (4.3.4.4). Then a map of pairs of rings $(A, I) \to (C, J)$ will lift through this tower uniquely by the universal property of pd-envelope.

then we see $A\{\varphi(f_1)/p, \ldots, \varphi(f_r)/p\}$ is just the pd-envelop of $(A, I)$, by the universal property. □

Lemma (4.7.0.22). Let $A$ be an $\mathbb{F}_p$-algebra and $B$ an $A$-algebra. If $(x_1, \ldots, x_n) \in B$ is regular w.r.t. $A(8.1.3.7)$, then $D_B((x_1, \ldots, x_n))$ is $A$-flat.

Proof: By (4.7.0.19) and base change, it is clear that $D_B(I)$ is a free $B/I^p$-algebra. Thus we need to show that $B/I^p$ is a flat $A$-module. And this is true as the sequence $x_1^p, \ldots, x_n^p$ is also regular w.r.t. $A(8.1.3.8)$.

Prop.(4.7.0.23) [Flatness of PD-Envelope]. If $A \to B$ is a map of simplicial rings, $A$ is naturally a simplicial pd-structure with $I_\bullet = pA_\bullet$, and $B$ is $p$-completely flat over $A(8.1.3.5)$, and $(x_1, \ldots, x_n) \in \pi_0(B)$ is $p$-completely regular w.r.t $A(8.1.3.7)$, then the completed pd-envelope $D = D_B((x_1, \ldots, x_n))$ is $p$-completely flat over $A$.

Proof: By definition (8.1.3.5), to check it is $p$-completely flat, it suffices to check

$$
Kos(A, p) \to Kos(A, p) \otimes_A^L D
$$

is flat. and by (8.1.3.4) it suffices to check that

$$
\pi_0(Kos(A, p)) \to \pi_0(Kos(A, p)) \otimes_A^L D
$$
is flat. The formation of pd-envelope commutes with derived base change by universal property, and tensor with $A/p$-algebra undoes the completions, so we are reduced to the the case $A' = \pi_0(\text{Kos}(A,p))$ and $B' = A' \otimes^L_A B$ is flat over $A'$ and to show that

$$A' \to D_{B'}((x_1, \ldots, x_n))$$

is flat. Notice $B'$ is a discrete flat $A'$-algebra by definition(8.1.3.5), and $(x_1, \ldots, x_n)$ is a sequence in $B'$ that $\text{Kos}(B, x_1, \ldots, x_n)$ is a sequence regular w.r.t. $A'$:

$$\text{Kos}(B, x_1, \ldots, x_n) = \text{Kos}(B' = A' \otimes^L_A B, x_1, \ldots, x_n) = A' \otimes^L_{\text{Kos}(A,p)} \text{Kos}(A, p) \otimes_A \text{Kos}(B, x_1, \ldots, x_n)$$

is flat because $\text{Kos}(A, p) \to \text{Kos}(B, p, x_1, \ldots, x_n)$ does by definition(8.1.3.7) and(8.1.3.3). So we are done by(4.7.0.22).

**Cor. (4.7.0.24).** If $A$ is a p-complete simplicial $\delta$-ring and $B$ is a p-completely flat simplicial $\delta$-$A$-algebra, and if $x_1, \ldots, x_r \in \pi_0(B)$ is p-completely regular w.r.t. $A$, then

$$C_* = B_*\{\frac{x_1}{p}, \ldots, \frac{x_r}{p}\}$$

is p-completely flat over $A$.

**Proof:** Let $C'_* = B_*\{\frac{\varphi(x_1)}{p}, \ldots, \frac{\varphi(x_r)}{p}\}$, then $C'_*$ is p-completely flat over $A$, by(4.7.0.21) (? why $B$ is p-torsionfree and $(p, x_1, \ldots, x_n)$ is regular sequence) and(4.7.0.23). Now there is a commutative diagram

$$
\begin{array}{c c c c c c c c c c}
A & \longrightarrow & A\{x_1, \ldots, x_r\} & \longrightarrow & B & \longrightarrow & B\{\frac{x_1}{p}, \ldots, \frac{x_r}{p}\} & \longrightarrow & C_* \\
\downarrow & & \downarrow\psi & & \downarrow\psi_B & & \downarrow\psi' & & \downarrow\psi_C \\
A & \longrightarrow & A\{\varphi(x_1), \ldots, \varphi(x_r)\} & \longrightarrow & B' & \longrightarrow & B'\{\frac{\varphi(x_1)}{p}, \ldots, \frac{\varphi(x_r)}{p}\} & \longrightarrow & C'_*
\end{array}
$$

where $\psi$ is the relative Frobenius and $\psi_B, \psi_C$ is the derived base change and completed derived base change. Then $\psi$ is f.f. as it is the base change of the Frobenius on the free $\delta$-ring $\mathbb{Z}\{x_1, \ldots, x_r\}$.(4.5.4.10), thus so does $\psi'$. Then $\psi_C$ is p-completely flat, because it is the completion(use(4.6.7.2)) (4.6.7.4). Now the conclusion follows, by completely f.f. descent(4.6.7.2).

#### 1 de Rham Complex

**Def. (4.7.1.1) PD-Differentials.** Let $B$ be an $A$-algebra and $(B, J, \delta)$ be a pd-structure and $M$ a $B$-module, then a **pd-$A$-derivation** from $B$ to $M$ is a an element $\theta$ of $\text{Der}_A(B, M)$ that $\theta(\delta_n(x)) = \delta_{n-1}(x)\theta(x)$ for $n \geq 1$ and $x \in J$.

As in(4.4.3.4), there is a **pd-differential** $\Omega_{B/A,\delta}$ that

$$\text{Hom}_B(\Omega_{B/A,\delta}, M)$$

is isomorphic to the set of pd-$A$-derivations of $B$ to $M$, functorially in $M$.

**Prop. (4.7.1.2) PD-Differential of PD-Envelope.** Let $(A, I, \gamma)$ be a pd-structure and $(B, J)$ be a pair over $(A, I)$, and let $D_{B/A,\gamma}(J) = (D, \overline{T}, \overline{\gamma})$ be the pd-envelope, then $\Omega_{D/A,\overline{\gamma}} = \Omega_{B/A} \otimes_B D$. 

Proof: It suffices to show that for any $D$-module $M$, the set of $A$-derivations $B \to M$ is isomorphic to the set of pd-$A$-derivations $D \to M$.

Let $D \otimes M$ be the ring that $M^2 = 0$ and a pd-structure on $J \oplus M$ is given by $\delta_n(x + m) = \delta_n(x) + \delta_{n-1}(xm)$. Then a pd-$A$-derivations $D \to M$ is equivalent to a pd-ring map $(D, J) \to (D \oplus M, J \oplus M)$, and an $A$-derivations $B \to M$ is also equivalent to a map of pairs $(B, J) \to (D \oplus M, J \oplus M)$, thus we are done by the universal property of $D$. □

**Prop. (4.7.1.2)**. Let $B$ be an $A$-algebra and $(B, J, \delta)$ be a pd-structure, then

- if $(B[X], JB[X], \delta')$ is the $\delta$-structure extended from that of $(B, J, \delta)$ as in (4.7.0.11), then
  \[ \Omega_{B[X]/A,\delta'} = \Omega_{B/A,\delta} \otimes_B B[X] \oplus B[X]dx. \]

- Let $B\langle x \rangle$ be the free pd-algebra over $B$ (4.7.0.14), then
  \[ \Omega_{B\langle x \rangle/A,\delta'} = \Omega_{B/A,\delta} \otimes_B B\langle x \rangle \oplus B\langle x \rangle dx. \]

- Let $K \subset J$ be an ideal preserved by $\delta$ and then consider the quotient $(B' = B/K, J = J/K, \delta)$, then $\Omega_{B'/A,\delta}$ is quotient of the module $\Omega_{B/A,\delta} \otimes_B B'$ by the $B'$-submodule generated by $dk$ where $k \in K$.

Proof: These are all somewhat trivial. □

**Prop. (4.7.1.3)**. Let $A$ be a $\mathbb{Z}(p)$-algebra, $B$ be an $A$-algebra and $(B, J, \delta)$ be a pd-structure, then

\[
\Omega^i_{B/A,\delta} = (\Omega^i_{B/A,\delta})^\wedge = (\Omega^i_{B/A,\delta}^\wedge).
\]

where $B_e = B/p^e$.

Proof: By (4.7.0.12), the terms make sense. Now by (4.7.1.3) and the observation $d(p^e) = 0$, we have $\Omega^i_{B_e/A,\delta} = \Omega^i_{B/A,\delta}/p^e = \Omega^i_{B/A,\delta}/p^e$, thus we are done. □

**Def. (4.7.1.4)**. Let $\Omega^i_{B/A,\delta} = \wedge^i \Omega_{B/A,\delta}$, then the surjection $\Omega_{B/A} \to \Omega^i_{B/A,\delta}$ satisfies the condition of (6.2.1.2), thus there is a **pd-de Rham complex** $\Omega^*_{B/A,\delta}$.

**PD-Poincaré Lemma**

**Lemma (4.7.1.6)**. Let $A$ be a ring, $P = A \langle X_i \rangle$ is the free PD-algebra over $A$, then for any $A$-module, the complex

\[
0 \to M \to M \otimes_A P \to M \otimes_A \Omega^\wedge_{P/A,\delta} \to \ldots
\]

is exact. And if $D = \widehat{P}$ and let $\Omega^n_D = \Omega^n_{P/A,\delta}$, then for any $p$-complete $A$-module $M$, the complex

\[
0 \to M \to M \widehat{\otimes}_A P \to M \widehat{\otimes}_A \Omega^\wedge_{P/A,\delta} \to \ldots
\]

is exact.
Proof: It suffices to show that $0 \to M \to M \otimes_A P \to M \otimes_A \Omega^1_{P/A,\delta} \to \ldots$ is homotopic to 0. For this, notice every element of $\Omega^n_{P/A,\delta}$ is of the form $\sum P \prod_{j=0}^n dx_{i_0} dx_{i_1} \ldots dx_{i_n}$, so we can let

$$f(\omega) = f(\gamma_{i_0}(x_{i_0}) dx_{i_0} \wedge \omega) = \gamma_{i_0+1}(x_{i_0}) \omega$$

where $\omega$ doesn’t divides $dx_k$ for $k < i_0$. Then it can be checked that $df + fd = \text{id}$, so we are done.

□

Prop. (4.7.1.7). If $A$ is a ring and $(B,J,\delta)$ is a pd-structure, and let $P = B\langle X_i \rangle$ be the free pd-structure. Let $M$ be a $B$-module endowed with an integrable connection $\nabla : M \to M \otimes_B \Omega^1_B\langle X_i \rangle$, then the map of de Rham complexes

$$M \otimes_B \Omega^*_{B/A,\delta} \to M \otimes_B \Omega^*_{P/A,\delta}$$

is a quasi-isomorphism. And if we denote $D, D'$ the $p$-adic completions of $B, P$, and $\Omega_D, \Omega_{D'}$ the $p$-adic completion of $\Omega_{B/A,\delta}, \Omega_{P/A,\delta}$, and $M$ is a $p$-complete $B$-module endowed with an integrable connection $\nabla : M \to M \otimes_D \Omega_D$, then the map of de Rham complexes

$$M \otimes_D \Omega^*_{D} \to M \otimes_{D'} \Omega^*_{D'}$$

is a quasi-isomorphism.

Proof: Consider the filtration $F^*$ on $\Omega^*_{B/A,\delta}$ given by the stupid truncation $\sigma_{\geq i} \Omega^*_{B/A,\delta}$, and consider the filtration on $\Omega^*_{P/A,\delta}$ given by

$$F^*(\Omega^*_{P/A,\delta}) = F^*(\Omega^*_{B/A,\delta}) \wedge \Omega^*_{P/A,\delta}.$$ 

Notice that we have a split exact sequence

$$0 \to \Omega^1_{B/A,\delta} \otimes_B P \to \Omega^1_{P/A,\delta} \to \Omega^1_{P/B,\delta} \to 0$$

and $\Omega^1_{P/B,\delta}$ is free on $X_i$ over $B$ (pondering the universal property, this is for the same reason as (4.4.3.7).

Then we see that $F^i(\Omega^*_{P/A,\delta}) \to \Omega^*_{P/A,\delta}$ is termwise split injection for any $i$, and the graded is $\Omega^i_{B/A,\delta} \otimes_B \Omega^i_{P/B,\delta}$. Thus if we let $F^i(M \otimes_B \Omega^*_{P/A,\delta}) = M \otimes F^i(\Omega^*_{P/A,\delta})$, then the graded is $M \otimes_B \Omega^i_{B/A,\delta} \otimes_B \Omega^i_{P/B,\delta}$, which is quasi-isomorphic to $M \otimes_B \Omega^i_{B/A,\delta}$ by (4.7.1.6). Then the original map is a filtered complexes that induces quasi-isomorphism on gradeds, so it induces a quasi-isomorphism, because it induces a morphism between two convergent spectral sequences, by (3.4.7.6) and (3.4.7.5). □
4.8 Almost Ring Theory

References are [Almost Ring Theory Gaber/Ramero] and [Almost Ring Theory Foundations Gaber/Ramero].

Def.(4.8.0.1). The setup of most mathematics is an flat ideal $I \subset R$, that $I^2 = I$. This implies that $I \otimes I \cong I^2 = I$.

Denote $i : R \to R/I$. Then there is a map $i_* : M \to MR$, which has a left adjoint $i^* : N \to N \otimes_R R/I$, and a right adjoint $i^!: N \to \text{Hom}(R/I, N)$.

1 Homological Theory

Almost Modules

Prop.(4.8.1.1)[Examples].

- If $K$ is a perfectoid field, $R = K^0, I = K^{00}$, then $I$ is flat over $R$, because if $\pi$ is a pseudo-uniformizer of $K(10.3.8.9)$, then $I = (\pi^{1/p^n})$, which is a colimit of free modules thus flat, and $I^2 = I$ clearly.

- Let $R$ be a ring and $f$ is an arbitrary element with compatible $p^n$-th roots, let $I = (f^{1/p^n})$, then $I^2 = I$. To show $I$ is flat, consider:

\[
\begin{align*}
M_0 &\xrightarrow{f^{1/p^n}} M_1 \xrightarrow{f^{1/p^n}} M_2 \to \ldots \to M_n \xrightarrow{f^{1/p^{n+1}}} M_{n+1} \to \ldots
\end{align*}
\]

where $M_i \cong R$, and $M = \text{colim} M_i$, then $M$ is flat, and there is a map $M \to I : 1 \in M_n \to f^{1/p^n}$, then this map is surjective, and it is injective: if $\alpha$ maps to 0, then $\alpha f^{1/p^n} = 0$, so $\alpha p^n f = 0$ for all $m \geq n$, and by perfectness of $R$, $\alpha f^{1/p^n} = 0$, so in particular, $\alpha = 0 \in M_{n+1}$.

Prop.(4.8.1.2)[The Category of Almost $R$-Modules in disguise]. Let $\mathcal{A} \subset \text{Mod}_R$ be the category of all $R$-modules $M$ that the action $I \otimes M \to M$ is an isomorphism(If $I \otimes I = I$ this is equivalent to $M = I \otimes N$ for some $N$) then:

- The inclusion $j_! : \mathcal{A} \to \text{Mod}_R$ is exact, i.e. the cokernel, kernel of objects in $\mathcal{A}$ are also in $\mathcal{A}$.

- $j_!$ has a right adjoint $j^* : M \to I \otimes M$, and the unit map $N \to j^* j_! N$ is an isomorphism on $\mathcal{A}$.

- $j^*$ has its right adjoint $j_*(M) = \text{Hom}(I, M)$, and the counit $j^* j_! M \to M$ is an isomorphism on $\mathcal{A}$.

Proof: 1: an easy consequence of five-lemma.

2: We need to show for $N \in \mathcal{A}$, $\text{Hom}(N, I \otimes M) \cong \text{Hom}(N, M)$. Notice there is a distinguished triangle

\[
I \otimes M \to M \to M \otimes R/I,
\]
as $- \otimes_R^L M$ is a derived functor and $I$ is flat. So it suffices to show

\[
R \text{Hom}_R(N, M \otimes_R^L R/I) = 0 = R \text{Hom}_{R/I}(N \otimes_R^L R/I, M \otimes_R^L R/I).
\]

And in fact $N \otimes_R^L R/I = 0$, because $N \otimes_R^L R/I = N \otimes_R^L I \otimes_R^L R/I$, and $I \otimes_R^L R/I = I \otimes_R R/I = I/I^2 = 0$ by flatness and hypothesis.

$N \cong j^* j_! N$ is an easy consequence of $I \otimes I = I$. 


Prop. (4.8.1.3) [Category of Almost \( R \)-modules].

- The image of the functor \( i_* : \text{Mod}_{R/I} \to \text{Mod}_R \) is a Serre subcategory of \( \text{Mod}_R \), so the quotient \( \text{Mod}^a_R = \text{Mod}_R / \text{Mod}_{R/I} \) exists by (3.3.2.14),
- The quotient \( q : \text{Mod}_R \to \text{Mod}^a_R \) admits fully faithful left and right adjoints. In particular, \( q \) preserves all limits and colimits.
- The image of \( i \) is a ‘tensor ideal’ of \( \text{Mod}_R \), so the quotient \( \text{Mod}^a_R \) inherits a natural symmetric monoidal \( \otimes \)-product structure.
- There is a functor \( \text{alHom} : (\text{Mod}^a_R)^{\text{op}} \times \text{Mod}^a_R \to \text{Mod}^a_R : (X,Y) \to \text{alHom}(X,Y) \) that \( \text{alHom}(X,-) \) is right adjoint to \( - \otimes X \):

\[
\text{Hom}(Z \otimes X, Y) \cong \text{Hom}(Z, \text{alHom}(X,Y)).
\]

Proof: 1: the image of \( i_* \) is just the category of modules killed by \( I \), if \( M \) is killed by \( I \), then subobjects and quotients of \( M \) is killed by \( I \), and if \( M \) is an extension of two elements killed by \( I \), then \( IM = I^2M = 0 \).

2: In fact we show that the category \( A \) in (4.8.1.2) and the functor \( j^* \) is just equivalent to \( \text{Mod}^a_R \):

First: \( j^*(\text{Mod}_{R/I}) = 0 \), because \( I \otimes M = I \otimes R/I \otimes R/I M = I/I^2 \otimes R/I M = 0 \) as \( I = I^2 \), and \( j^* \) is exact because \( I \) is flat.

And for any \( R \)-module \( M \), consider \( I \otimes M \to M \), it has kernels and cokernels, then tensoring \( I \), it becomes \( I \otimes M \to I \otimes M (4.8.0.1) \). as \( I \) is flat, the kernel and cokernels are killed by \( I \), so for any functor \( q \) to another category that kills \( \text{Mod}_{R/I} \), \( q(M) = q(I \otimes M) = qj_0j^*(M) \), so \( q \) factors through \( M \), uniquely, as \( j^* \) is surjective.

Now the left/right adjoints exist by (4.8.1.2).

3: if \( IM = 0 \), then \( IM \otimes N = 0 \), so the tensor products pass to the quotient, and \( j^* \) is a map between symmetric monoidal categories.

4: \( \text{alHom} \) is defined by \( \text{alHom}(j^*M, j^*N) = j^*(\text{Hom}(M,N)) = \text{Hom}(M,N)^a \). This is well defined, because if \( IM = 0 \) or \( IN = 1 \), then \( I \text{Hom}(M,N) = 0 \). □

Cor. (4.8.1.4).

- \( i^*j_! = 0 \).
- \( i^!j_* = 0 \).
- \( j^*i_* = 0 \), and the kernel of \( j^* \) is just \( i_*(\text{Mod}_{R/I}) \).

Proof: 1: \( R/I \otimes I \otimes M = 0 \), because \( I \otimes R/I = 0 \).

2: \( \text{Hom}(R/I, \text{Hom}(I, M)) = 0 \), because \( I \otimes R/I = 0 \).

3: This is by 2 of the proposition (4.8.1.3). □
**Remark (4.8.1.5).** The construction above can be summarized as the following diagram:

\[
\begin{array}{ccc}
\text{Mod}_{R/I} & \xrightarrow{i^*} & \text{Mod}_R \\
\downarrow{i_!} & & \downarrow{j_!} \\
\text{Mod}_R & \xrightarrow{j^*} & \text{Mod}_R^a
\end{array}
\]

with four adjoint pair and three vanishing. This should be seen as an analogy of the case of topology: \(X\) is a space and \(i: U \to X\) is open in \(X\), and \(j: Z \to X\) is closed, \(Z = X - U\), then the defined sheaf operations are the same as written above.

However, one should not consider \(\text{Mod}_R^a\) as the sheaf of modules on the open subscheme \(\text{Spec} R_f\) for some pseudo uniformizer, because the map \(M \to M \otimes R_f\) factors through \(\text{Mod}_R^a\) as it vanishes on \(\text{Mod}_{R/I}\), but it is not \(\text{Mod}_{R/I}^a\). For example, if \(k\) is a perfect field, and consider \(R = k[t^{1/p}]\), then the module \(M = R/(t)\) is also killed by \(\otimes R_f\), but it is not killed by \(I\).

Then one may consider it is the category of \(\text{Qco}\) sheaves on \(D(I)\), but first this is not an affine scheme, and second this is false, anyway. And we should imagine an non-existent open subscheme \(U\) bigger than \(U\), as it contains any affine opens of \(U\).

**Remark (4.8.1.6).** Notice \(j^*\) is both left exact and right exact, so it preserves both arbitrary limits and colimits, so almostification nearly loses anything. In particular, the category \(\text{Mod}_R^a\) has all colimits and limits.

**Def. (4.8.1.7) [Almost Commutative Algebras].** As \(\text{Mod}_R^a\) has a symmetric monoidal structure, it is possible to define the category of almost commutative algebras as the category of commutative unitary monids in \(\text{Mod}_R^a\), denoted by \(CAlg(\text{Mod}_R^a)\). Notice that its unit object is \(I = R^a\).

There is an obvious map

\((-)^a : \text{Alg}(\text{Mod}_R) \to \text{Alg}(\text{Mod}_R^a)\),

and yet another functor

\((-)_* : \text{Alg}(\text{Mod}_R^a) \to \text{Alg}(\text{Mod}_R),

because \(M \to M_*\) is lax symmetric monoidal, i.e. there are natural map \(M_* \otimes N_* \to (M \otimes N)_*\).

This is a right adjoint of \((-)^a\), as \(j^*\) and \(j_*\) is adjoint.

Finally there is a functor

\((-)!! : \text{Alg}(\text{Mod}_R^a) \to \text{Alg}(\text{Mod}_R),

whose construction is a little complicated, first notice the functor \((-)_!\) preserves multiplication but it has no units, so in order to give it a unit, consider the module pushout: \((A! \oplus V)/I\), which has a natural multiplicative structure that can be made into a \(R\)-module, and \((-)!!\) is left adjoint to \((-)^a\), Cf.[Almost Ring Theory P22].

**Prop. (4.8.1.8).** \((-)!!\) preserves faithfully flatness.

**Proof:** Cf.[Almost Ring theory P52]? \(\square\)

**Def. (4.8.1.9).** For an almost commutative algebra \(A\), a left module is an almost module \(M \subset \text{Mod}_R^a\) that has a left action \(A \otimes M \to M\) that has natural commutative diagrams as one expects. And for any \(R\)-algebra \(A\), there are natural maps \(\text{Mod}_A \to \text{Mod}_R^a A\).
Almost Homological Algebra

2 Almost Commutative Algebra

Def. (4.8.2.1) [Almost Notations]. Given a $R$-module $M$, an element $f \in M$ is called **almost zero** if $I \cdot f = 0$, and $M$ is called **almost zero** if all $f \in M$ is almost zero.

Denote

$$M^a = j^* M \in \text{Mod}^a_R, \quad M_s = j_s M^a = \text{Hom}(I, M), \quad M_t = j_t M^a = I \otimes M.$$  

Then there are morphisms $M_t \to M \to M_s$, which becomes isomorphisms after almostification.

Prop. (4.8.2.2). If $I = (f \frac{1}{f^n})$, then $M_s = \{x \in M[f^{-1}] | f^{\frac{1}{f^n}} x \in A\}$ for all $n$.

Prop. (4.8.2.3). If $M \to N$ is almost surjective maps of $K^0$-algebras that $M/I \to N/I$ is surjective, then $M \to N$ is surjective.

Proof: As $I$ is flat over $K^0$, if $M \to N \to Q \to 0$ is the cokernel, tensoring $A/I$, as $M/I \to N/I$ is surjective, $Q/IQ = 0$, but $Q$ is almost zero thus $IQ = 0$, so $Q = 0$. □

Def. (4.8.2.4) [Almost Properties]. Something is called **almost XXX** if it is XXX when passed to the category of almost $R$-modules. For example,

- elements of $M_s$ are called **almost elements** of $M$.
- $M$ is called **almost flat** iff $M^a \otimes -$ is exact on $\text{Mod}^a_R$, which is equivalent to $\text{Tor}^R_{>0}(M, N)$ is almost zero for all $N$.
- $M$ is called **almost projective** iff allHom$(M, -)$ is exact on $\text{Mod}^a_R$, which is equivalent to $\text{Ext}^R_{>0}(M, N)$ is almost zero for all $N$.

Notice this is not equivalent to projective in $\text{Mod}^a_R$, because $R$ is almost projective, but $\text{Hom}_{R^a}(R^a, M^a) = \text{Hom}(I, M)$ is not exact as $I$ is not projective: $\text{Ext}^1_R(R^a, M^a) = \text{Ext}^1_R(I, R) = \text{Ext}^2(k, R)$, which is not 0 if $R$ is the valuation ring of a non-spherically complete perfectoid field $K$, like $\widehat{Q_p}$?

- $M$ is called **almost finitely generated/ almost finitely presented** if for any $\varepsilon \in I$, there is a f.g./f.p. $M_\varepsilon \to M$ with $N_\varepsilon$ generators that the kernel and cokernel are killed by $\varepsilon$. It is called **uniformly almost finitely generated** iff $N_\varepsilon$ is independent of $\varepsilon$.

Notice this definition doesn’t depends on $M$ chosen?

- If $S$ is of charp, it is called **almost perfect** iff $S_\varepsilon$ is perfect.

Prop. (4.8.2.5) [Enough Almost Injectives]. The category $\text{mod}^a_R$ has enough injectives. In fact $j^*, j_s$ both preserves injectives, because they have exact left adjoints, so $I$ is injective $R$-module iff $I^a$ is injective $R^a$-module, and $J$ is injective $R^a$-module iff $J_s$ is injective $R$-module. So to construct an injective resolution in $R^a$, pass to $R$-modules using either $(-)_s$ or $(-)_t$; and find an injective resolution, then almostificate it.

Prop. (4.8.2.6) [Derived Functors of $(-)_s$]. Notice that $\text{Hom}_{R^a}(M^a, N^a) = \text{Hom}_R(I \otimes M, N)$ by adjointness, so using (4.8.2.5),

$$\text{Ext}^k_{R^a}(M^a, N^a) = \text{Ext}^k_R(M_s, N) = \text{Ext}^k_R(M, R \text{Hom}(I, N)),$$

then as $M_s = \text{Hom}(I, M)$, the derived functor of $(-)_s$ is just $\text{Ext}^k_R(I, M) = \text{Ext}^k_R(R^a, M^a)$.

Notice that $\text{Ext}^k_{R^a}(M, N)$ are all almost zero, as $j^a j_s = \text{id}$, and use trivial Grothendieck spectral sequence.
Prop. (4.8.2.7) [(Example) A Quadratic Extension of a Perfectoid Field]. If \( K = \hat{Q_p[p^{1/2}]} \) and \( L = K(\sqrt[p]{b}) \) with \( p \neq 2 \), then \( L^0 \) is a uniformly almost f.p. projective \( K^0 \)-module.

**Proof:** It suffices to find for each \( n \) a \( K^0 \)-module \( R_n \) of rank 2 that \( R_n \rightarrow L^0 \) is injective with cokernel annihilated by \( p^\frac{1}{2n+1} \). For this, consider \( R_n = K^0 \oplus K^0 p^\frac{1}{2n+1} \), then \( L^0 = \text{colim}_n R_n \).

Notice that the cokernel of \( R_n \rightarrow R_{n+1} \) is killed by \( p^{\frac{1}{2n+1}} \), because

\[
p^{\frac{1}{2n+1}} \cdot p^{\frac{1}{2n+1}} = p^{\frac{1}{2n+1} + \frac{1}{2n+1}} \subset R_n.
\]

So by killing one by one, the cokernel of \( R_n \rightarrow \text{colim}_n R_n \) is killed by any \( p \)-power with power larger than \( \sum \frac{1}{2n+1} \), in particular by \( p^{\frac{1}{2n+1}} \). So \( \text{colim}_n R_n \) is an extension of \( R_0 \) by a cokernel killed by \( p \), so it is also \( p \)-adically complete, and \( L^0 = \text{colim}_n R_n \). Now Consider \( 0 \rightarrow R_n \rightarrow \text{colim}_n R_n \rightarrow \text{Coker} \), then \( \text{Ext}^n(\text{colim}_n R_n, N) = \text{Ext}^n(\text{Coker}, N) \) is killed by \( p^{\frac{1}{2n+1}} \) for all \( n \), so it is killed by \( I \), thus \( \text{colim}_n R_n \) is almost projective.

**Completions and Closures**

Prop. (4.8.2.8) [\( \text{prc and Completion} \)]. If \( A \) is a ring with a non-zero-divisor \( f \) that \( A \subset A[f^{-1}] \) is \( p \)-root closed (prc), then:

- \( \hat{A} \subset \hat{A}[f^{-1}] \) is \( p \)-root closed.

- If \( f \) admits a compatible \( p \)-power roots, then \( A_s \subset A_s[f^{-1}] \) is \( p \)-root closed (where almost mathematics is performed w.r.t \( f^{\frac{1}{2n+1}} \)).

**Proof:** We first replace \( A \) with its maximal separated quotient \( A/(\cap_n f^n A = I) \): \( f \) is still non-zero-divisor, because if \( fg \in I \), then \( fg \in f^n A \) for all \( n \), so \( g \in f^{n-1} A \) as \( f \) is non-zero-divisor. And it is \( p \)-root closed, because if \( a^n \in A/I[f^{-1}] \), then \( a^n = b + f^{-c}d \) for \( c \) integer and \( d \in I \). Notice \( I = fI = f^c I \) by (4.2.2.16), so \( f^{-c}d \in I \) as well, so \( a \in A \).

Now \( \hat{A} \) is \( f \)-separated, in particular, \( A \hookrightarrow \hat{A} \).

1: If \( g \in \hat{A}[f^{-1}] \) and \( g^n \in \hat{A} \), then \( f^N g \in \hat{A} \) for some \( N \) and choose a \( m \geq N(p - 1) \), then by the density, \( g = g_0 + f^m g_1 \) for some \( g_0 \in A[f^{-1}] \), \( g_1 \in \hat{A} \). Notice \( f^N g_0 \in \hat{A} \), now

\[
g^n = g_0^n + p g_0^{n-1} f^m g_1 + \ldots + (f^m g_1)^n,
\]

By definition of \( m \), all terms except \( g_0^n \) are in \( \hat{A} \), so \( g_0 \in A \), so \( g_0 \in A \), and \( g \in \hat{A} \).

2: Use the convention (4.8.2.2), if \( g \in A_s[f^{-1}] \) that \( g^n \in A_s \), then \( f^{\frac{1}{2n}} g^n \in A \) for all \( n \), so \( (f^{\frac{1}{2n+1}} g)^n \in A, \) thus \( f^{\frac{1}{2n+1}} g \in \hat{A} \), hence \( g \in A_s \). \( \square \)

Prop. (4.8.2.9) [\( \text{ic and Completion} \)]. Let \( A \) be a ring with a non-zero-divisor \( f \), if \( A \subset A[f^{-1}] \) is integrally closed, then:

- \( \hat{A} \subset \hat{A}[f^{-1}] \) is integrally closed.

- If \( f \) admits a compatible \( p \)-power roots, then \( A_s \subset A_s[f^{-1}] \) is integrally closed (where almost mathematics is performed w.r.t \( f^{\frac{1}{2n+1}} \)).

**Proof:** We first replace \( A \) with its maximal separated quotient \( A/(\cap_n f^n A = I) \): \( f \) is still non-zero-divisor and \( I \) is \( f \)-divisible as in the proof of (4.8.2.8). And it is integrally closed, because if \( g \)
satisfies a monic polynomial \( h(X) \in A/I[f^{-1}][X] \), then choose a lifting, \( h(g) \in I[f^{-1}] = I \subset A \), so \( g \) is integral over \( A \) thus \( g \in A \), and \( g \in A/I \). Now \( A \) is \( f \)-separated and \( A \hookrightarrow \hat{A} \).

1. If \( g \in \hat{A}[f^{-1}] \) satisfies a polynomial \( H \in \hat{A}[X] \), then \( g = f^{-c}h \) for \( h \in \hat{A} \), and then \( h \) satisfies a polynomial \( H(f^c x) \), and choose an approximation of coefficients of \( H(x) \) and \( h_0 \) of \( h \) mod \( f^{cn} \), then it is clear that \( H(f^c h_0) \in f^{cn} \hat{A} \cap A = f^{cn} A \), so when dividing back, \( g_0 = f^{-c} h_0 \) is integral over \( A \) thus \( g_0 \in A \), thus \( h_0 \in f^c A \), and \( h \equiv h_0 \) mod \( f^{cn} \), thus \( h \in f^c A \), and \( g \in A \).

2. Use the convention (4.8.2.2), if \( g \in A_\ast[f^{-1}] \) is integral over \( A_\ast \), then there are polynomial \( H \) that \( H(g) = 0 \), now if \( \varepsilon = f^{\frac{1}{p^n}} \) consider another polynomial \( H(x/\varepsilon) \), then its coefficients are all in \( A \), thus \( \varepsilon g \) is integral over \( A \) thus \( \varepsilon g \in A \), and then \( g \in A_\ast \).

\[
\text{Prop. (4.8.2.10) [tic and Completion].} \text{Let } A \text{ be a ring with a non-zero-divisor } f \text{ that admits a compatible system of } p\text{-power roots } f^{\frac{1}{p^n}} \text{ for all } n > 0, \text{ and } A \text{ is totally integrally closed (tic) in } A[f^{-1}] \text{, then } \hat{A} \text{ is totally integrally closed in } \hat{A}[f^{-1}] \text{ and } A = A_\ast.
\]

\[
\text{Proof:} \quad 1: \text{Notice totally integrally closed is } p\text{-root closed, so } \hat{A} \subset \hat{A}[f^{-1}] \text{ is } p\text{-root closed. Now if } f^{k} g^N \subset \hat{A} \text{ for some } k, \text{ then by prc, } f^{\frac{1}{p^n}} g \in \hat{A} \text{ for all } n, \text{ thus } g \text{ in an almost zero element in } \hat{A}[f^{-1}]/A \cong A[f^{-1}]/A, \text{ and then } g \text{ is totally integrally closed over } A, \text{ because for any } n, \text{ let } n < p^k, \text{ then } f^{\frac{1}{p^n}} g \in A, \text{ thus } f^{\frac{1}{p^n}} g \in A, \text{ and } fg^n \in A.
\]

\[
\begin{align*}
\text{2: Because } f^{\frac{1}{p^n}} A_\ast & \subset A \text{ by convention (4.8.2.2), clearly } A_\ast \text{ is totally integrally closed in } A, \text{ thus } A_\ast \subset A. \\
\end{align*}
\]

**Almost Étale Map**

\[
\text{Def. (4.8.2.11). A map } A \to B \text{ of } R\text{-algebras is called almost étale iff:
\begin{itemize}
\item \( B \) is almost f.p. projective over \( A \).
\item \( \mu \) is almost f.p. projective over \( A \).
\end{itemize}
}\]

\[
\text{Prop. (4.8.2.12) [Example of Almost Étale Maps]. Let } K = Q_p[p^{\frac{1}{p^n}}] \text{ and } L = K(\sqrt[p]{p}) \text{ with } p \neq 2, \text{ then } L^0/K^0 \text{ is uniformly almost f.p projective } K^0\text{-module, by (4.8.2.7). We show it is finite étale: flatness is clear, as } L^0/K^0 \text{ is torsion-free and } K^0 \text{ is a valuation ring and use (4.8.3.3).}
\]

**Lemma (4.8.2.13) [Lemma for Almost Purity in Characteristic } p]. \text{If } \eta : R \to S \text{ is an integral map of perfect rings. If } \eta[t^{-1}] \text{ is finite étale for some } t \in R, \text{ then } \eta \text{ is almost finite étale w.r.t the ideal } I = (t^{\frac{1}{p^n}}).
\]
Proof: Firstly, we may assume $R, S$ are both $t$-torsion-free, because the $t$-torsion part $R[t^\infty]$ and $S[t^\infty]$ is almost zero: if $t^c\alpha = 0$, then $t^c\alpha^{p^n} = 0$, so $t^{\frac{c}{p^n}}\alpha = 0$. So we reduce to $R/R[t^\infty] \to S/S[t^\infty]$, which doesn’t change anything.

Now we reduce to the case that $R, S$ are integrally closed in $R[t^{-1}]$ and $S[t^{-1}]$: it suffices to show that $R_{int} \subset R_*$, thus they are almost isomorphic. For this, an element $f \in R_{int}$ satisfies $f^{R_0} t^k \in R$ for some $k$, so by perfectness, $ft^{\frac{1}{pm}} \in R$ for all $n$, so $f \in R_*$.

Now check unramifiedness: let $e \in (S \otimes_R S)[t^{-1}]$ be a diagonal idempotent, then $\alpha e \in S \otimes_R S$ for some $c$, now $e^2 = e$, so easily $e \in (S \otimes_R S)_*$.

Now check almost finite projective: for $m > 0$, represent $t^{\frac{1}{pm^m}} e = \sum a_i \otimes b_i \in S \otimes_R S$, then use the map $S \overset{\alpha}{\to} R^n \overset{\beta}{\to} S$ as in (4.4.7.14), then $\beta \alpha = t^{\frac{1}{pm}}$ on $S$, as $S$ is $t$-torsion free, $R^n \to S$ is injective with $t^{\frac{1}{pm}}$-torsion cokernel, for any $m$. So $S$ is almost finite projective. □

Prop.(4.8.2.14)[Almost Purity in Characteristic $p$]. If $R$ is a perfect ring of char $p$, then using the almost mathematics w.r.t. $I = (t^{\frac{1}{pm}})$, $S \to S_*[t^{-1}]$ gives an isomorphism of categories: $R_{af\ell t} \cong R[t^{-1}]_f\ell t$.

Proof: As in the proof of (4.8.2.13), we may assume $R$ is $t$-torsion-free. Notice that any integral extension of $R[t^{-1}]$ comes from an integral extension of $R$(choose the integral closure), so the lemma above (4.8.2.13) tells us the functor is essentially surjective.

Now we construct an inverse functor, $S_*[t^{-1}]$ maps to $T^a$, where $T$ is the integral closure of $R$ in $S_*[t^{-1}]$. By lemma (4.8.2.15) below, $S$ is almost perfect. So $S_*$ is $t$-torsion-free, as if $t^c f = 0$, then $t^{\frac{1}{pm}} f = 0$ for all $n$, so $f = 0 \in (S_*)_s = S_*$. So now $S_* \subset S_*[t^{-1}]$. Clearly $T$ is also perfect and $t$-torsion-free. So $R \to T$ is an integral extension that is identified with $R[t^{-1}] \to S_*[t^{-1}]$ after inversion of $t$.

To show that $T^a = S$, it suffices to show $T_* = S_*$. for $f \in T$, $f^{R_0}$ spans a finite module of $T[t^{-1}] = S_*[t^{-1}]$, so $t^c f^{R_0} \subset S_*$, then by perfectness, $f \in (S_*)_s = S_*$, so $T_* \in S_*$. Conversely, if $g \in S_*$, then $t^c g^{R_0}$ lies in a f.g. $R$-module of $S_*[t^{-1}]$, by almost f.g.. So $t^c g^{R_0} \subset T$, and then by perfectness $g \in T_*$. □

Lemma (4.8.2.15). Almost finite étale map of rings of char $p$ is almost relatively perfect.

Proof: Cf.[Bhatt notes on Perfectoid Spaces P28]. □

3 Almost Mathematics on Perfectoid Fields

Prop. (4.8.3.1)[Almost Elements]. If $K$ is a perfectoid field, $R = K^0$ and $I = K^{00}$, $M$ is an $R$-module, then

- If $M$ is torsion-free, then $M_* = \{m \in M \otimes_{K^0} K \mid Im \in M\} = \{m \in M \otimes_{K^0} K \mid t^{\frac{1}{pm}} m \in M\}$, by (10.3.8.12) and (4.8.2.2).
- $I_* = R_* = R$. More generally, for an ideal $J \subset R$, let $c = \sup \{|x| \mid x \in J\}$, then $J_* = \{a \in K_* \mid |a| \leq c\}$.

Prop. (4.8.3.2). Let $K$ be a perfectoid field with a pseudo-uniformizer $\pi$. If $\alpha : M \to N$ is an almost surjective map of $K^0$-algebras that $M$ is $\pi$-adically separated and $N$ is $\pi$-torsion-free that $\alpha \mod \pi$ is an almost isomorphism, then $\alpha$ is an almost isomorphism.
Prop. (4.8.3.3) [Almostification and Completeness]. Let \( K \) be a perfectoid field with a pseudo uniformizer \( t \) and \( R = K^0_1, I = K^{00}_1 \), let \( M \in \text{Mod}_R^a \), then:

- \( M \) is almost flat iff \( M_* \) is \( R \)-flat iff \( M_t \) is \( R \)-flat.
- Assume \( M \) is almost flat, then \( M \) is \( t \)-adically complete iff \( M_* \) does.
- Assume \( M \) is almost flat, then for each \( f \in K^0_1 \), \( fM_* \cong (fM)_* \), and \( M_*/fM_* \subset (M/fM)_* \).

And for any \( \varepsilon \in I \), the image of \((M/f\varepsilon M)_* \) and \( M_*/fM_* \) in \((M/fM)_* \) are identical.

**Proof**: 1: \( R \) is a valuation ring, so \( M_* \) is \( R \)-flat iff \( M_*[t] \) is flat by (4.4.1.12), as \( t \) is a pseudo uniformizer. As \((-)_* \) is left exact, \( M_*[t] = (M[t])_* \), so if \( M \) is almost flat, then \( M[t] = 0 \) as \( t \) is nonzero-divisor, so \( M_* \) is \( R \)-flat. The converse is true as \( M = (M_*)^a \), and the tensor is compatible.

For \((-)_t \), this follows from the observation that \((-)_t \) and \((-)_a \) are both exact and commute with tensor products, and notice \( M_t \otimes N = (M \otimes N)^a \).

2: As \((-)_a \) commutes with all limits and colimits, if \( M_* \) is \( t \)-adically complete then so does \( M = (M_*)^a \). Conversely, if \( M \) is \( R \)-flat and \( t \)-adically complete, then \( M_t, M_* \) are also \( R \)-flat, and consider the commutative diagram:

\[
\begin{array}{c}
M_t \xrightarrow{a} \lim(M/t^nM)_t = \lim M_t/t^nM_t = \hat{M}_t \\
\downarrow d \quad \quad \quad \downarrow b \\
M_* \xrightarrow{c} \lim(M/t^nM)_* 
\end{array}
\]

then \( d \) is almost isomorphism by (4.8.1.2) and so does \( b \) because \((-)_a \) commutes with all limits, and \( c \) is an isomorphism as \((-)_* \) commutes with limits and \( M \) is \( t \)-adically complete. So \( a \) is also almost isomorphism.

Now notice \( M_t \) is flat hence \( t \)-torsion-free, so the kernel of \( a, d \) must be 0, with almost zero cokernels. Now (4.2.3.9) shows first \( M_t \) is complete and next \( M_* \) is complete.

3: Notice \((fM)_* = fM \) as \((-)_a \) is exact, so

\[
(fM)_* = \text{Hom}(I, fM_*) = \{ y \in M_*[t^{-1}] | Iy \subset fM_* \} = f\{ y \in M_*[t^{-1}] | Iy \subset M_* \} = fM_*
\]

and \( M_*/fM_* \subset (M/fM)_* \) follows from the left exactness of \((-)_* \).

For the last assertion, consider the commutative diagram

\[
\begin{array}{c}
0 \longrightarrow M \xrightarrow{f} M \longrightarrow M/fM \longrightarrow 0 \\
0 \longrightarrow M/\varepsilon M \xrightarrow{f} M/f\varepsilon M \longrightarrow M/fM \longrightarrow 0
\end{array}
\]

and apply \((-)_* = \text{Hom}_{R^a}(R^a, -) \) and use (4.8.2.6), then

\[
\begin{array}{c}
0 \longrightarrow M_*/fM_* \xrightarrow{a} (M/fM)_* \longrightarrow \text{Ext}_{R^a}^1(R^a, M)[f] \longrightarrow 0 \\
0 \longrightarrow (M/f\varepsilon M)_* \xrightarrow{b} (M/fM)_* \longrightarrow \text{Ext}_{R^a}^1(R^a, M/\varepsilon M)
\end{array}
\]
To show \( a, b \) has the same image, it suffices to show that \( c \) is injective. For this, it suffices to show \( \text{Ext}^1_{R^a}(R^a, M) \rightarrow \text{Ext}^1_{R^a}(R^a, M/\varepsilon M) \) is injective. Consider the exact sequence \( 0 \rightarrow M \xrightarrow{\varepsilon} M \rightarrow M/\varepsilon M \rightarrow 0 \), it suffices to show that \( \varepsilon \text{Ext}^1_{R^a}(R^a, M) = 0 \), and this is obvious as \( \varepsilon \in I(4.8.2.6) \).

\[ \Box \]

Prop. (4.8.3.4) [General Completeness and Almostification]. More generally, if \( J = (f_1, \ldots, f_r) \subset R \) is a f.g. ideal, then an \( R^a \)-module \( M \) is \( J \)-adically complete if \( M^* \) does.

Proof: Cf.[Perfectoid Spaces Bhatt P32].

Banach Space

Prop. (4.8.3.5) [Uniform Banach \( K \)-Algebra]. If \( K \) is a non-Archimedean perfectoid(perfect) field with a pseudo uniformizer \( t \), then the following categories are equivalent:

- The category \( \mathcal{D}_{tic} \) of \( t \)-adically complete and \( t \)-torsionfree \( K^0 \)-algebras \( A \) with \( A \) totally integrally closed in \( A[t^{-1}] \).
- The category \( \mathcal{D}_{ic} \) of \( t \)-adically complete and \( t \)-torsionfree \( K^0 \)-algebras that \( A \) is integrally closed in \( A[t^{-1}] \) and \( A = A_* \).
- The category \( \mathcal{D}_{prc} \) of \( t \)-adically complete and \( t \)-torsionfree \( K^0 \)-algebras that \( A \) is \( p \)-root closed in \( A[t^{-1}] \) and \( A = A_* \).

Proof: The last three are equivalent, because if \( A \in \mathcal{D}_{tic} \), then \( A = A_* \) by (4.8.2.10), as \( K \) is perfect by (10.3.8.4). So \( \mathcal{D}_{tic} \subset \mathcal{D}_{ic} \subset \mathcal{D}_{prc} \), so it suffices to show that \( \mathcal{D}_{prc} \subset \mathcal{D}_{tic} \). Now for any \( f \) that \( f^N \subset t^{-k}A \), then \( t^k f^N a \subset A \), and \( A \) is \( p \)-root closed, so \( t^{\frac{k}{n}} f \subset A \) for all \( n \), so \( f \in A_* \) (4.8.2.3), but \( A_* = A \).

The equivalence of 1, 2 is general, by (12.1.2.7).

\[ \Box \]

Prop. (4.8.3.6). If \( K \) is a perfectoid field, then the category of uniform Banach spaces has all colimits and limits.

Proof: Cf.[Bhatt P38].

\[ \Box \]
5 | Algebraic Geometry I: Scheme Theory

5.1 Sites, Sheaves and Stacks

References are [Sta], [Ols16], [Vis08] and [Fibered Category to Algebraic Stacks Lamb].

1 Sites

Def. (5.1.1.1) [Sites]. A site is given by a category \( \mathcal{C} \) and a set \( \text{Cov}(\mathcal{C}) \) of families of morphisms with fixed target, called the coverings of \( \mathcal{C} \) that:

- An isomorphism is a covering.
- Coverings of covering is a covering.
- Base change of a covering is a covering.

Sometimes a site is wrongly called a topology, the difference is that the morphism of site is looks like a reverse of a morphism of topology (5.1.1.5).

Def. (5.1.1.2) [Discrete Topology]. A discrete topology or chaotic topology is a site that the only coverings are identities. In this way, we can regard any category as a site.

Def. (5.1.1.3) [Noetherian Topology]. An object \( U \) in a site \( \mathcal{C} \) is called quasi-compact if for each covering of \( U \), f.m. of them still forms a covering of \( U \). The site \( \mathcal{C} \) is called Noetherian if each object of \( \mathcal{C} \) is quasi-compact.

Given a site \( \mathcal{C} \), we can define a new site \( \mathcal{C}' \) whose coverings are coverings of \( \mathcal{C} \) that are finite. Then this is truly a site and it is Noetherian.

Def. (5.1.1.4) [Comma Topology]. For a site \( \mathcal{C} \) and an object \( S \), we have the comma category \( \mathcal{C}/S(3.1.1.17) \), and we can define a topology on it where the coverings are coverings of \( \mathcal{C} \) that is compatible over \( S \).

Def. (5.1.1.5) [Continuous Functor]. A continuous functor between sites \( \mathcal{C} \to \mathcal{D} \) is a functor that preserves covering and any base change by morphisms in a covering.

A morphism of sites \( \mathcal{C} \to \mathcal{D} \) is given by a continuous functor \( u : \mathcal{D} \to \mathcal{C} \) that \( u_*(5.1.2.11) \) is exact.

This exact condition is easy to be satisfied, by (5.1.2.14).

Def. (5.1.1.6) [Cocontinuous functors]. A cocontinuous functor between sites \( u : \mathcal{C} \to \mathcal{D} \) is a functor that for any \( U \in \mathcal{C} \) and any covering \( \{V_i \to u(U)\} \) in \( \mathcal{D} \), there is a covering \( \{U_i \to U\} \in \mathcal{C} \) that refines \( \{V_i \to u(U)\} \) after the functor \( u \).
Topologies and Sieves

Def. (5.1.1.7) [Sieves]. For a covering $U = \{U_i \to U\}$ in a category $\mathcal{C}$, define a subfunctor $h_U \subset h_U$, where for each $X$ $h_U(X)$ consists of elements in $\text{Hom}(X,U)$ that factor through some $U_i \to U$.

A sieve $S$ on $U$ is a subfunctor of $h_U$. Notice that any sieve must be of the form $h_U$, by choosing $U$ to consist of all arrows in $\{S(T)\}_{T \in \mathcal{C}}$.

Def. (5.1.1.8). If $\mathcal{T}$ is a Grothendieck topology on a category $\mathcal{C}$, then a sieve $S \subset h_U$ over $U$ is said to belong to $\mathcal{T}$ or just a sieve of the site $\mathcal{C}$ if there exists a covering $\mathcal{U}$ of $U$ that $h_U \subset S$.

$G$-Spaces

Def. (5.1.1.9) [G-Spaces]. A $G$-space is a set $X$ with a family of subsets of $X$ that they form a site w.r.t inclusions and that covering are all set-theoretic coverings (but not necessarily conversely). These subsets are called admissible opens of $X$ and covers are called admissible covers. (In other words, a $G$-topological space is a "topological space without unions"). Morphisms of $G$-spaces is simultaneously a continuous map and a morphism of sites.

Def. (5.1.1.10) [Completeness]. The completeness of a $G$-topological space $X$:

- G0: $\emptyset$ and $X$ are admissible open.
- G1: Let $\{U_i \to U\}$ be an admissible cover, then a subset $V \subset U$ is admissible if $V \cap U_i$ are all admissible.
- G2: Let $\{U_i \to U\}$ be a cover of admissible opens for $U$ admissible, then the cover is admissible if it has an admissible cover as a refinement.

Lemma (5.1.1.11) [Admissible is Local]. If $G_2$ is satisfied for a $G$-topological space $X$, then for an admissible covering $\{X_i \to X\}$ and another covering $\{U_i \to X\}$ between admissible opens, it is admissible iff $U_i \cap X_j$ is an admissible covering for $X_j$ for each $j$. (By composition, $\{U_i \cap X_i \to X\}$ is admissible, and it refines $\{U_i \to X\}$).

Prop. (5.1.1.12) [Glue of Complete G-topological spaces]. For sets $\cup X_i = X$, if there are Grothendieck category $\mathcal{I}_i$ on $X_i$ making $X_i$ into a $G$-topological space, and they all satisfies the completeness conditions $G_0$, $G_1$, $G_2$ of (5.1.1.10). Assume that $X_i \cap X_j$ is $\mathcal{I}_i$-open in $X_i$ and $\mathcal{I}_i, \mathcal{I}_j$ restrict to the same topology on $X_i \cap X_j$, then there is a unique Grothendieck category $\mathcal{I}$ on $X$ making $X$ a $G$-topological space that:

- $X_i$ is $\mathcal{I}$-open and $\mathcal{I}$ restricts to $\mathcal{I}_i$ on $X_i$,
- $\mathcal{I}$ satisfies the completeness conditions $G_0, G_1, G_2$.
- $X_i$ is a $\mathcal{I}$-covering of $X$.

Proof: By (5.1.1.10) and (5.1.1.11), the uniqueness is straightforward, for the existence,

- check Grothendieck first: Composition, base change.
- check condition 1: by hypothesis, and (5.1.1.10) applied to $X_i \cap X_j \to X_i$ (this is admissible because id$_X$, refined it).
- check condition 2: $G_0$ obvious, $G_1$ by if $V \cap U_i \cap X_i$ admissible, then $V \cap X_i$ admissible by admissibility of $U_i \to U$, then $V$ is admissible, $G_2$: obvious
- check condition 3: because $X_i \cap X_j \to X_i$ is admissible.
Def. (5.1.1.13). A $G$-topological space is called **connected** iff there isn’t two nonempty admissible open subset $X_1, X_2$ that $X_1 \cap X_2 = \emptyset$ and $\{X_1, X_2 \to X\}$ is an admissible cover.

**$G$-torsor**

Def. (5.1.1.14) [Torsors]. Let $\mathcal{C}$ be a site and $\mathcal{G}$ a sheaf of groups over $\mathcal{C}$, then a **pseudo $G$-torsor** is a sheaf of sets $\mathcal{F}$ over $\mathcal{C}$ endowed with an action $\mathcal{G} \times \mathcal{F} \to \mathcal{F}$ that $\mathcal{G} \times \mathcal{F} \to \mathcal{F} \times \mathcal{F} : (g, f) \mapsto (gf, f)$ is an isomorphism.

A pseudo $G$-torsor is called a **$G$-torsor** if for any $U \in \mathcal{C}$, there is a covering $\{U_i \to U\}$ that $\mathcal{F}(U_i)$ is non-empty for each $i$.

Prop. (5.1.1.15). A $G$-torsor on a site is trivial iff $\Gamma(\mathcal{C}, \mathcal{F}) \neq 0(5.3.1.2)$.

Proof: This is because the transitive action of $\mathcal{G}$ on the global section induces an isomorphism $\mathcal{G} \to \mathcal{F}$. □

Prop. (5.1.1.16). If $\mathcal{C}$ is a subcanonical site, and $\mathcal{G}$ a sheaf of groups over $\mathcal{C}$, then a sheaf of sets $\mathcal{F}$ together with an action $\alpha : \mathcal{G} \times \mathcal{F} \to \mathcal{F}$ is a $G$-torsor iff for any $U \in \mathcal{C}$, there is a covering $\{U_i \to U\}$ that the restrictions to $U_i$ are trivial torsors, i.e. $\alpha|_{\mathcal{C}/U_i} = \pi : \mathcal{G}|_{U_i} \times \mathcal{F}|_{U_i} \to \mathcal{F}|_{U_i}$.

Proof: If $\mathcal{F}$ is a $G$-torsor, then the restrictions of the torsor on $U_i$ are trivial because they have global sections in $\Gamma(\mathcal{C}/U_i, \mathcal{F}) = \mathcal{F}(U_i)$, by (5.1.1.15). Conversely, if there is a covering $\{U_i \to U\}$ that the restrictions to $U_i$ are trivial torsors, then the map $\mathcal{G} \times \mathcal{F} \to \mathcal{F} \times \mathcal{F} : (g, f) \mapsto (gf, f)$ are isomorphisms when restricted to $U_i$, which means $\mathcal{G}(U) \times \mathcal{F}(U) \to \mathcal{F}(U) \times \mathcal{F}(U)$ is an isomorphism for any $U$, because they are sheaves, so it is an isomorphism, and $\mathcal{F}$ is a $G$-torsor. □

Cor. (5.1.1.17) [Representable $G$-Torsor]. If $\mathcal{C}$ is a site and $\mathcal{G}$ is a group object in $\mathcal{C}$, then

- $X \to Y$ is a $G$-torsor in the category $\mathcal{C}/Y$ iff $X \to Y$ is a $G$-equivariant map(where the action of $G$ on $Y$ is trivial), $G \times X \to X \times_Y X : (g, x) \mapsto (gx, x)$ is an isomorphism, and $\{X \to Y\}$ is refined by a covering of $Y$.

- If $\mathcal{C}$ is a subcanonical site, then $X \to Y$ is a $G$-torsor in the category $\mathcal{C}/Y$ iff $X \to Y$ is a $G$-equivariant map(where the action of $G$ on $Y$ is trivial), and there exists a covering $\{Y_i \to Y\}$ that each $Y_i \times_Y X \to Y_i$ is a trivial torsor, i.e. $G$-equivariantly isomorphic to $G \times Y_i \to Y_i$.

Cor. (5.1.1.18). If $\mathcal{C}$ is a site and $\mathcal{G}$ is a group object in $\mathcal{C}$, $X \to Y$ is a $G$-torsor in the category $\mathcal{C}/Y$, then the map $G \times G \times X \to X \times_Y X \times_Y X : (g, h, x) \mapsto (ghx, hx, x)$ is an isomorphism.

**Presheaves**

Def. (5.1.1.19) [Presheaves]. On a category $\mathcal{C}$, a **presheaf** of sets/groups/* is a functor $\mathcal{C}^{op} \to \text{Ab}(\text{Set} / \mathcal{G})$. The category of presheaves of sets/groups/* on $\mathcal{C}$ is denoted by $\mathcal{PSh}(\mathcal{C})$ (or $\mathcal{PSh}^{\text{Set}}(\mathcal{C}), \mathcal{PSh}^{\text{Gp}}(\mathcal{C}), \mathcal{PSh}^{*}(\mathcal{C})$). For any $U \in \mathcal{C}$, $\Gamma(U, -)$ is the functor $\mathcal{PSh}^{\text{Set}}(\mathcal{C}) \to \text{Set} : F \mapsto F(U)$.

For a presheaf $\mathcal{F}$ with structures, $\mathcal{F}^{\text{Set}} \in \mathcal{PSh}^{\text{Set}}(\mathcal{C})$ is underlying presheaf of sets.

Prop. (5.1.1.20). The category of presheaves on a category admits all limits and colimits, and it commutes with $\Gamma(U, -)$ for any $U \in \mathcal{C}$.

Def. (5.1.1.21) [Points]. A **point of a site** is a $\text{Cf.[Sta]}00Y3$. 
2 Sheaves and Topoi

Def. (5.1.2.1) [Sheaves]. Let $\mathcal{C}$ be a site, then $F \in \mathcal{PSh}^{\text{Set}}(\mathcal{C})$ is called a sheaf (on $\mathcal{C}$) iff ?.

The category of sheaves (of sets/groups/*) on a site $\mathcal{C}$ is denoted by $\text{Sh}(\mathcal{C})$ (or $\text{Sh}^{\text{Sp}}(\mathcal{C}), \text{Sh}^{*}(\mathcal{C}))$.

Def. (5.1.2.2) [Separate Presheaves]. Let $\mathcal{C}$ be a site, then $F \in \mathcal{PSh}^{*}(\mathcal{C})$ is called a separated presheaf if $F(U) \hookrightarrow \prod_i F(U_i)$ is injective for any covering $U = \{U_i \to U\} \in \text{Cov}(\mathcal{C})$.

Def. (5.1.2.3) [Effective Epimorphisms]. An epimorphism $\{U_i \to V\}$ in a category is called a family of effective epimorphisms if $\text{Hom}(V, Z) \to \prod_i \text{Hom}(U_i, Z) \Rightarrow \prod_i \text{Hom}(U_i \times_{V} U_j, Z)$ is exact for each $Z$. Similarly for a family of universal effective epimorphisms.

Prop. (5.1.2.4) [Subcanonical Site]. The class of all families of universal effective epimorphisms in a category forms a Grothendieck topology, called the canonical topology. It is the finest topology that all representable presheaves are sheaves.

Topologies that are coarser than the canonical topology are called subcanonical topology. Equivalently, a subcanonical topology is a topology that every representable presheaf is a sheaf.

Proof: We only need to verify that family of universal effective epimorphisms is closed under composition. For this, first prove epimorphism, then use epimorphism to prove effectiveness. Universal follows routinely. Cf.[Tamme]. \qed

Prop. (5.1.2.5). For a subcanonical topology on a site $\mathcal{C}$, its restriction on a localizing category $\mathcal{C}/S$ is subcanonical.

Proof: The only nontrivial part is that the glued morphism is a morphism over $S$. For this, consider its composition that maps to $S$, then the uniqueness of the exact sequence (5.1.2.3) will show that it is truly a $S$-morphism. \qed

Prop. (5.1.2.6). Let $\mathcal{C}$ be a subcanonical site, and $f : X \to Y$ is an arrow in $\mathcal{C}/S$, suppose there is a covering $\{S_i \to S\}$ that the pullback of $f$ to $\mathcal{C}/S_i$ are all isomorphisms, then $f$ is an isomorphism.

Proof: This follows from (5.1.3.6) and (5.1.3.8). \qed

Prop. (5.1.2.7) [Sheafification]. Let $\mathcal{C}$ be a site, consider the functor

$$(\cdot)^+ : \mathcal{PSh}^{*}(\mathcal{C}) \to \text{Sh}^{*}(\mathcal{C}) : F^+(U) = \lim_{\longrightarrow} \ker(\prod_i F(U_i) \Rightarrow \prod_{i,j} F(U_i \times_{U} U_j)) = \check{H}^0(U, F).$$

Then

- For $F \in \mathcal{PSh}^{*}(\mathcal{C})$, $F^+$ is separated.
- If $F \in \mathcal{PSh}^{*}(\mathcal{C})$ is separated, $F \to F^+$ is injective and $F^+ \in \text{Sh}^{*}(\mathcal{C})$. (The problem of separated is that the cover may not be identical in $U_i \times_{U} U_j$ but only on a cover of it).
- $(\cdot)^+$ is left exact.
- Sheafification functor $(\cdot)^# : \mathcal{PSh}^{*} \to \text{Sh}^{*} : F \mapsto F^# = F^{++}$ is exact and it is left adjoint to the forgetful functor.
So the forgetful functor is left exact and it preserves injectives. Thus the sheaf cokernel is the sheafification of the presheaf kernel, the sheaf kernel is the presheaf kernel.

Proof: The separatedness is simple. For sheaf condition, an element of $F^+(U)$ is represented by a covering $\{V_{ij} \to U\}$, and there restriction to $U \times_U V_j$ coincide by separatedness hence the covering $\{V_{ij} \to U\}$ is an element of $F^+(U)$.

Sh is left exact because $(-)^+$ is left exact from $\mathcal{P}\mathcal{S}h^*$ to $\mathcal{P}\mathcal{S}h^*$ by (5.3.2.4) checked on every element $U$. It is right exact trivially, hence it is exact. □

Def. (5.1.2.8) [Constant Sheaf]. The constant sheaf $S$ for a set $S$ is the sheafification of the constant presheaf $U \mapsto S$.

Transfer of Sheaves under Morphisms of Sites

Def. (5.1.2.9) [Functoriality of Presheaves]. Given a functor of sites $u : \mathcal{C} \to \mathcal{C}'$, which should be regarded as an inverse map, there are maps

$$u^p F'(U) = F'(u(U)) : \mathcal{P}\mathcal{S}h(\mathcal{C}') \to \mathcal{P}\mathcal{S}h(\mathcal{C}), \quad u_p(F)(U') = \lim_{U_i | U' \to u(U_i)} F(U_i) : \mathcal{P}\mathcal{S}h(\mathcal{C}) \to \mathcal{P}\mathcal{S}h(\mathcal{C}')$$

Then $u_p$ is left adjoint to $u^p$.

We can also define a functor

$$p u : p u(F)(U') = \lim_{\{U_i | U' \to u(U_i)\}^{\text{op}}} F(U_i) : \mathcal{P}\mathcal{S}h(\mathcal{C}) \to \mathcal{P}\mathcal{S}h(\mathcal{C}')$$

Then this functor is right adjoint to $u^p$, by duality.

Proof: A map $f \in \text{Mor}(u_p(F), G)$ is represented by compatible maps

$$\lim_{U_i : U' \to u(U_i)} F(U_i) \to G(U'),$$

and this is represented by compatible maps $F(U_i) \to G(u(U_i))$ which is indexed over $\prod_{U' \in \mathcal{C}'} \mathcal{I}_{U'}$, where $\mathcal{I}_{U'} = \{U_i : U' \to u(U_i)\}$. Now this is equivalent to compatible maps $F(U_i) \to G(u(U_i))$, which is a map $g \in \text{Mor}(F, u^p(G))$. □

Cor. (5.1.2.10). $u^p$ is exact.

Def. (5.1.2.11) [Functoriality of Sheaves].

- Given a continuous functor $u : \mathcal{C} \to \mathcal{C}'$ between sites, there are maps

$$u_* = u^p \circ u_p \circ t : \mathcal{S} \to \mathcal{S}', \quad u^* = u^p \circ t : \mathcal{S}' \to \mathcal{S}.$$ 

$u_*$ is left adjoint to $u^*$, by adjointness of $u_p, u^p$ and $u, t$.

- Given a cocontinuous functor $u : \mathcal{C} \to \mathcal{C}'$ between sites, there are maps

$$u_* = u^p \circ u^p \circ t : \mathcal{S}' \to \mathcal{S}, \quad s u = p u \circ t : \mathcal{S} \to \mathcal{S}'.$$ 

$u^*$ is left adjoint to $s u$, by adjointness of $u^p, p u$ and $u, t$. Moreover, $u^*$ is exact.
Proof: 1: Notice if \( \mathcal{F} \) is a sheaf, then \( u^* \mathcal{F} \) is also a sheaf, by continuity (5.1.1.5).

2: \( p^* \mathcal{F} \) is a sheaf by [Sta00XK?]. \( u^p \) is clearly right exact, and it is left exact because \( \iota, \sharp \) do, and \( u^p \) is exact by (5.1.2.10).

**Cor. (5.1.2.12)** When \( u \) is continuous, \((u_\sharp(G))^* \cong (u_\sharp(G^\sharp))^* \) for any presheaf \( G \) on \( T \).

When \( u \) is cocontinuous, \((u^\sharp G)^* \cong (u^\sharp(G^\sharp))^* \) for any presheaf \( G \) on \( T \).

Proof: Use Yoneda lemma.

**Prop. (5.1.2.13)** For \( Z \in T, u_p h_Z = h_{u(Z)} \).

Proof: Use the adjointness of \( u_p, u^p \) (5.1.2.9), then for any presheaf \( F \),

\[
\text{Hom}(u_p h_Z, F) = \text{Hom}(h_Z, u^p F) = f^p(F)(Z) = F(f(Z)),
\]

thus we are done by Yoneda lemma.

**Prop. (5.1.2.14) [When is \( u_s \) Exact].** If \( f : \mathcal{C} \to \mathcal{C}' \) is a continuous functor between sites that \( U' \) is cofiltered for any \( U' \in \mathcal{C}' \), where \( U' \) the category of all pairs \( (U, \varphi) \) where \( U \in \mathcal{C} \) and \( \varphi : U' \to u(U) \), then \( u_s \) is exact.

In particular, this is the case when \( \mathcal{C}, \mathcal{C}' \) both have weakly final objects and finite fiber products and \( u \) preserves them. Notice the condition of weakly final objects can be released if we can show \( U' \) is nonempty for any \( U' \).

Proof: It suffices to show the left exactness of \( u_p \). By definition, \( u_p(U') = \lim_{\to_{U'}} F_{U'} \) where \( F_{U'} \)

is the covariant functor \( (U, \varphi) \to F(U) \). Because \( U' \text{ filters} \), this colimit process is exact form \( \text{Hom}(U', \mathcal{A}) \) to \( \mathcal{A} \) and \( u_p \) is exact. Now sheffification is also exact (5.1.2.7), so we conclude.

The last assertion is clear. (Notice the weakly-final object are used to assure \( U' \text{ is nonempty.} \)

**Prop. (5.1.2.15) [Localization Site].** For a site \( T \) and \( Z \in T \), there is a site \( T/Z \) as objects over \( T \), and \( i : T/Z \to T \) is continuous. Then \( i^* \) is exact.

Proof: \( R^i i^*(F) = (i^p(H^q(F)))^i(5.3.1.8), \) and \((H^q(F))^* = 0(5.3.2.14), \) so it suffices to show \( i^p \) and \( \sharp \) commutes. But \( i^* \) and \( \ast \) commute obviously.

**Prop. (5.1.2.16) [Sheaf Condition is Local].** To check sheaf condition for presheaf w.r.t. a topology, it suffice to show that for any covering, there is a refinement covering of it that sheaf condition hold, because by the definition of sheafification functor, \( F^+ = F, \) so \( F \) is a sheaf.

**Cor. (5.1.2.17).** For two topology on a same category that \( T' \) is finer than \( T \), then any \( T'-\text{sheaf} \) is a \( T-\text{sheaf}. \) And if any covering in \( T' \) can be refined by a covering in \( T, \) then \( S \to S' \) is an equivalence of categories. In particular, if \( T \) is Noetherian, \( S(T) \) and \( S(T') \) (5.1.1.3) are equivalent.

**Topoi**

**Def. (5.1.2.18) [Topoi].** A **topos** is an Abelian category that is equivalent to the category of sheaves \( \text{Sh}(\mathcal{C}) \) on a site \( \mathcal{C} \). A morphism of topos \( f : \text{Sh}(\mathcal{C}) \to \text{Sh}(\mathcal{D}) \) is an adjunction

\[
(f^{-1}, f_* : \text{Sh}(\mathcal{D}) \rightleftharpoons \text{Sh}(\mathcal{C}))
\]

s.t. \( f_* \) is right adjoint to \( f^{-1} \) and \( f^{-1} \) is exact. Compositions of morphisms of topos are defined routinely. A 2-morphism of topos between two morphisms of topos \( f, g : \text{Sh}(\mathcal{C}) \to \text{Sh}(\mathcal{D}) \) is a natural transformation \( t : f_* \to g_* \).
Prop. (5.1.2.19) [Continuous Maps and Topoi]. A morphism of sites \( f : \mathcal{D} \to \mathcal{C} \) consists of a continuous functor \( u : \mathcal{C} \to \mathcal{D} \) that \( u_s \) is exact, so it induces a functor of topoi \( f : \mathsf{Sh} (\mathcal{C}) \to \mathsf{Sh} (\mathcal{D}) \), if we define \( f^{-1} = u_* s, f_* = u^s \), by (5.1.2.11).

Prop. (5.1.2.20) [Cocontinuous Maps and Topoi]. Let \( u : \mathcal{C} \to \mathcal{D} \) be a cocontinuous functor between sites, then this defines a morphism of topoi \( g : \mathsf{Sh} (\mathcal{C}) \to \mathsf{Sh} (\mathcal{D}) \), if we define \( g^{-1} = u^s \) and \( g_* = u_* \), by (5.1.2.11).

Prop. (5.1.2.21) [Cocontinuous Map with a Right Adjoint]. Let \( u : \mathcal{C} \to \mathcal{D} \) be a cocontinuous functor between sites with a right adjoint \( v : \mathcal{D} \to \mathcal{C} \), then the morphism of topoi \( g : \mathsf{Sh} (\mathcal{C}) \to \mathsf{Sh} (\mathcal{D}) \) is pretty simple,

\[
g^{-1} G (U) = G (u(U)), \quad g_* F (V) = F (v(V)).
\]

This holds in particular for localization of sites.

Proof: It follows from adjunction that \( u^p h_V = h_{v(V)} \), so \( g^{-1} (h^s_V ) = (u^p h^s_V )^s = (u^p h_v )^s = h^s_{v(V)} \), and

\[
(g_* F )(V) = \text{Hom}(h^s_{v(V)}, g_* F ) = \text{Hom}(g^{-1} h^s_{v(V)}, F ) = \text{Hom}(h^s_{v(v(V))}, F ) = F (v(V)).
\]

The other identity is clear. \( \square \)

Prop. (5.1.2.22) [Continuous and Cocontinuous Maps and Topoi]. Let \( u : \mathcal{C} \to \mathcal{D} \) be a functor between sites that satisfies

- \( u \) is continuous and cocontinuous,
- \( u \) is fully faithful,
- \( \mathcal{C} \) has final objects and fiber products and \( u \) preserves them.

then there are two maps of topoi: \( f = (u_s, u^s) : \mathsf{Sh} (\mathcal{D}) \to \mathsf{Sh} (\mathcal{C}), g = (u^s, u_*) : \mathsf{Sh} (\mathcal{C}) \to \mathsf{Sh} (\mathcal{D}) \) induced by \( u \) (5.1.2.19)(5.1.2.14)(5.1.2.20). They satisfy \( f \circ g = \text{id}_{\mathsf{Sh} (\mathcal{C})} \), and \( f^{-1} = u_s \) is fully faithful.

In particular, if we define \( g_l = u_* \), then there are two adjunctions

\[
(g_l, g^{-1}) : \mathsf{Sh} (\mathcal{C}) \rightleftarrows \mathsf{Sh} (\mathcal{D}), \quad (g^{-1}, g_*) : \mathsf{Sh} (\mathcal{D}) \rightleftarrows \mathsf{Sh} (\mathcal{C}).
\]

Proof: We need to show that for any \( F \in \mathsf{Sh} (\mathcal{C}), F \cong g^{-1} g_l F \) and \( g^{-1} g_* F \cong F \). For this, Cf. [Sta]00XT.^2

Then \( f^! \) is fully faithful follows from the equality \( F \cong g^{-1} g_l F \). \( \square \)

Prop. (5.1.2.23) [Special Cocontinuous Maps and Topoi]. A functor \( u : \mathcal{C} \to \mathcal{D} \) between sites is called a special cocontinuous functor if:

- \( u \) is continuous and cocontinuous,
- Given any \( a, b : U' \to U \in \mathcal{C} \) s.t. \( u(a) = u(b) : u(U') \to u(U) \), there is a covering \( \{ f_i : U'_i \to U' \} \) that \( a f_i = b f_i \).
- Given any \( U', U \in \mathcal{C} \) and a morphism \( c : u(U') \to u(U) \in \mathcal{D} \), there exists a covering \( \{ f_i : U'_i \to U' \} \in \mathcal{C} \) and morphisms \( c_i : U'_i \to U \) that \( u(c_i) = c \circ u(f_i) \).
- Given any \( V \in \mathcal{D} \), there is a covering of the form \( \{ u(U_i) \to V \} \) in \( \mathcal{D} \).

Then the induced morphism of topoi \( g : \mathsf{Sh} (\mathcal{C}) \cong \mathsf{Sh} (\mathcal{D})(5.1.2.20) \) is an equivalence of topoi.

Proof: Cf. [Sta]03A0. \( \square \)
Cor. (5.1.2.24) [Comparing Topologies]. Let \( \mathcal{C}' \) be a fully subcategory of \( \mathcal{C} \), and
- \( i : \mathcal{C}' \to \mathcal{C} \) is continuous, i.e. \( \text{Cov}(\mathcal{C}') \to \text{Cov}(\mathcal{C}) \).
- \( i : \mathcal{C}' \to \mathcal{C} \) is cocontinuous, i.e. any covering \( \{U_i \to U'\} \in \text{Cov}(\mathcal{C}) \) s.t. \( U' \in \mathcal{C}' \) has a refinement \( \{U_j' \to U'\} \in \text{Cov}(\mathcal{C}') \).
- Each \( U \in \mathcal{C} \) has a covering \( \{U_i \to U\} \in \text{Cov}(\mathcal{C}) \) with \( U_i \in \mathcal{T}' \). Then \( i : \text{Sh}(\mathcal{C}') \to \text{Sh}(\mathcal{C}) \) is an equivalence of topoi. \( i^{-1} \) is just the restriction functor, and \( i_* \) is called the extension functor of sheaves.

In particular, this applies to the case \( i : \mathcal{C}' = \mathcal{C}/\mathcal{Z} \to \mathcal{C} \), the localization category, in with case for \( \mathcal{Z}' \in \mathcal{C}/\mathcal{Z} \), \( i^{-1}F(\mathcal{Z}') = F(\mathcal{Z}') \) is called the restriction sheaf.

Prop. (5.1.2.25) [Localizing at Sheaves]. Let \( \mathcal{C} \) be a site and \( \mathcal{F}_i \) be a set of topos on \( \mathcal{C} \), then there is an equivalence \( \text{Sh}(\mathcal{C}) \cong \text{Sh}(\mathcal{C}') \) induced by a special cocontinuous functor (5.1.2.23) that
- \( \mathcal{C}' \) has the subcanonical topology,
- A family of morphisms \( \{V_i \to V\} \) are a covering of \( \mathcal{C}' \) iff \( \prod h_{V_i} \to h_V \) is surjective.
- \( \mathcal{C}' \) has fiber products and a final object.
- Every subsheaf of a representable sheaf is representable,
- Each \( g_* \mathcal{F}_i \) is a representable sheaf.

**Proof:** Cf. [[Sta]03CI]. \( \square \)

3 Stacks

Def. (5.1.3.1) [Stacks]. Let \( \mathcal{F} \to \mathcal{C} \) be a fibered category on a site \( \mathcal{C} \). Then \( \mathcal{F} \) is called a prestack over \( \mathcal{C} \) if for each covering \( \{U_i \to U\} \) in \( \mathcal{C} \), the functor \( \text{Hom}(h_U, \mathcal{F}) \to \text{Hom}(h_{U_i}, \mathcal{F})(5.1.1.7) \) is faithfully faithful. It is called a stack over \( \mathcal{C} \) if it is moreover an equivalence of categories.

Def. (5.1.3.2) [Category of Descent Datum]. Let \( \mathcal{F} \to \mathcal{C} \) be a fibered category on a site \( \mathcal{C} \), \( U \in \mathcal{C} \) and \( \mathcal{U} \) is a covering of \( U \). Given a choice of fibered products \( U_{ij}, U_{ijk} \) in \( \mathcal{C} \), we can define the category of descent datum \( \mathcal{F}_{\text{desc}}(\mathcal{U}) \) to be the category of tuples \( (\xi_i, \xi_{ij}, \xi_{ijk}) \) where \( \xi_{ij} \in \mathcal{F}(U) \) with Cartesian morphisms between them that are commutative. A morphism in \( \mathcal{F}_{\text{desc}}(\mathcal{U}) \) is a family of morphisms \( (\varphi_i, \varphi_{ij}, \varphi_{ijk}) \) commuting with the Cartesian morphisms.

Then there is an equivalence of categories \( \text{Hom}(h_{\mathcal{U}}, \mathcal{F}) \cong \mathcal{F}_{\text{desc}}(\mathcal{U}) \).

**Proof:** For any \( F : h_{\mathcal{U}} \to \mathcal{F}, U_i \to U \in h_{\mathcal{U}}(U_i) \), applying \( F \) to the arrows \( \text{id}_{U_i}, U_{ij} \to U_i, U_{ijk} \to U_{ij} \in h_{\mathcal{U}} \), we get an element in \( \mathcal{F}_{\text{desc}}(\mathcal{U}) \). Also a natural transformation \( F \to G \) maps to a morphism in \( \mathcal{F}_{\text{desc}}(\mathcal{U}) \), so we get a functor \( T : \text{Hom}(h_{\mathcal{U}}, \mathcal{F}) \to \mathcal{F}_{\text{desc}}(\mathcal{U}) \).

Conversely, choose an arbitrary choice of pullbacks (that coincide with \( \xi_{ij} \to \xi_i \)), for any arrow \( f : T \to U \in h_{\mathcal{U}}(T) \), we choose a \( U_i \) that \( T \to U \) factors as \( T \to U_i \to U \)(also for \( f = \text{id}_{U_i} \), choose \( U_i \)), then define \( F(f) \) as the pullback of \( \xi_i \) along \( T \to U_i \). For any morphisms \( T' \to T \to U \in h_{\mathcal{U}} \) and their choice of \( U_i, U_j \) that \( T' \to U \) factors through \( U_j \to U \) and \( T \to U \) factors as \( U_i \to U \), then \( T' \to U_j \) factors through \( U_{ij} \), i.e. we have a commutative diagram

\[
\begin{array}{ccc}
T' & \to & U_{ij} \to U_j \\
\downarrow & & \downarrow \\
T & \to & U_i \to U
\end{array}
\]
Then by Cartesian properties, we get a unique map \( F(T') \to F(T) \), which is Cartesian by (3.1.7.8). It can be shown these maps make \( F \) a functor, using Cartesian property and the existence of \( \xi_{ijk} \). And also for any map of descent datum, we get a natural transformation in \( \text{Hom}(h_U, F) \). Thus we get a functor \( S : F_{\text{desc}}(U) \to \text{Hom}(h_U, F) \).

The construction of \( S \) shows \( T \) is essentially surjective and full, and also faithful, so \( (S, T) \) is an equivalence of categories.

**Def. (5.1.3.3) [Everyday Descent Datums]**. Let \( F/\cal{C} \) be a fibered category on a site \( \cal{C} \), \( U \in \cal{C} \) and \( \cal{U} \) is a covering of \( U \). Given a choice of fibered products \( U_{ij}, U_{ijk} \) in \( \cal{C} \) and a cleavage of \( \cal{F}/\cal{C} \), let \( \cal{F}(\cal{U}) \) be the category of tuples \( (\xi, \varphi_{ij}) \) where \( \xi_i \in \cal{F}(U_i) \) and \( \varphi_{ij} \) are isomorphisms \( \varphi_{ij} : \text{pr}^*_1 \xi_i \cong \text{pr}^*_2 \xi_j \in \cal{F}(U_{ij}) \) s.t.

\[
\text{pr}^*_1 \varphi_{ik} = \text{pr}^*_2 \varphi_{jk} \circ \text{pr}^*_1 \varphi_{ij} : \text{pr}^*_1 \xi_i \cong \text{pr}^*_2 \xi_k.
\]

**WARNING**: Notice this doesn’t make sense unless we insect three isomorphisms such as \( \text{pr}^*_1 \varphi_{ij} \).

Then there is a (non-canonical!)equivalence of categories \( F_{\text{desc}}(U) \to \cal{F}(\cal{U}) \).

**Proof**: For \( (\xi_i, \varphi_{ij}, \xi_{ijk}) \in F_{\text{desc}}(U) \), there are isomorphisms \( \xi_{ij} \cong \text{pr}^*_1 \xi_i \) and \( \xi_{ij} \cong \text{pr}^*_2 \xi_j \), which gives an isomorphism \( \varphi_{ij} : \text{pr}^*_1 \xi_i \to \text{pr}^*_2 \xi_j \). This gives an element of \( \cal{F}(\cal{U}) \), by comparison with \( \xi_{ijk} \).

Conversely, given \( (\xi_i, \varphi_{ij}) \in \cal{F}(\cal{U}) \), choose an ordering on \( I \), for \( i < j \), let \( \xi_{ij} = \text{pr}^*_1 \varphi_i \), and \( \text{pr}^*_2 \circ \varphi_{ij} : \xi_{ij} \to \xi_{ij} \) is Cartesian. And for \( i < j < k \), let \( \xi_{ijk} = \text{pr}^*_1 \xi_i \), then there are Cartesian morphisms \( \xi_{ijk} \to \xi_{ij}, \xi_{ijk} \to \xi_{ik}, \xi_{ijk} \to \xi_{jk} \) by Cartesian properties, and it can be verified that the cocycle condition guarantees the diagram can be completed.

**Cor. (5.1.3.4) [Cocycle Conditions]**. If \( \cal{F}/\cal{C} \) is a rigid fibered category, then there is no need to check the cocycle condition, because every automorphism over \( \text{id}_U \) is trivial.

**Cor. (5.1.3.5) [Stacks and Sheaves]**. A rigid (pre)stack over a site \( \cal{C} \) is equivalent to a (pre)sheaf on \( \cal{C} \), by (3.1.7.28).

**Cor. (5.1.3.6)**. A site is subcanonical iff any representable fibered category \( h_U \to C \) is a stack.

**Prop. (5.1.3.7) [Equivalence Categories and Stacks]**. Let \( \cal{F} \to \cal{G} \) be an equivalence of fibered categories over a site \( \cal{C} \), then \( \cal{F} \) is a prestack/stack (in groupoid) iff \( \cal{G} \) is.

**Proof**: There is a strict commutative diagram of categories

\[
\begin{array}{ccc}
\text{Hom}(h_U, \cal{F}) & \longrightarrow & \text{Hom}(h_U, \cal{F}) \\
\downarrow & & \downarrow \\
\text{Hom}(h_U, \cal{G}) & \longrightarrow & \text{Hom}(h_U, \cal{G})
\end{array}
\]

that the vertical arrows are equivalences of categories, then we are done.

**Prop. (5.1.3.8) [Prestack and Hom Functor]**. Let \( \cal{F} \) be a fibered category over a site \( \cal{C} \), then \( \cal{F} \) is a prestack iff for any object \( S \) of \( \cal{C} \) and two objects \( \xi, \eta \in \cal{F}(S) \), the presheaf \( \text{Hom}_S(\xi, \eta) : (\cal{C}/S)^{\text{op}} \to \text{Set}(3.1.7.19) \) is a sheaf in the comma site \( \cal{C}/S(5.1.1.4) \).

**Proof**: By (5.1.3.7), it suffices to show \( \text{Hom}_S(\xi, \eta) \) is a stack in the comma topology \( \cal{C}/S \). Then it can be shown that \( \text{Hom}(h_U, \text{Hom}_S(\xi, \eta)) \to \text{Hom}(h_U, \text{Hom}_S(\xi, \eta)) \) is an equivalence of categories iff \( \text{Hom}(h_U, \cal{F}) \to \text{Hom}(h_U, \cal{F}) \) is fully faithful.
**Lemma (5.1.3.9).** Let \( F \) be a prestack over a site \( \mathcal{C} \), \( S, S' \) be sieves belonging to the topology of \( \mathcal{C} \) that \( S' \subset S \), then the restriction functor

\[
\text{Hom}_\mathcal{C}(S, F) \to \text{Hom}_\mathcal{C}(S', F)
\]

is faithful.

**Proof:** it suffices to show for \( S' = h_U \) for some covering \( U \). Let \( F, G \in \text{Hom}_\mathcal{C}(S', F) \) and \( \varphi, \psi \) be two natural transformations from \( F \) to \( G \) that induce the same natural transformation from the restriction of \( F \) to \( h_U \) to the restriction of \( G \) to \( h_U \), then \( \varphi = \psi \). For this, just notice there are commutative diagrams

\[
\begin{array}{ccc}
F(T \times_U U_i/U) & \xrightarrow{\varphi_{T \times_U U_i/U}} & G(T \times_U U_i/U) \\
\downarrow & & \downarrow \\
F(T/U) & \xrightarrow{\varphi_{T/U}} & G(T/U)
\end{array}
\]

where the vertical arrows are Cartesian, and the hypothesis implies \( \varphi_{T \times_U U_i/U} = \psi_{T \times_U U_i/U} \). Then we deduce \( \varphi_{T/U} = \psi_{T/U} \) as \( \text{Hom}_\mathcal{T}(F(T/U), G(T/U)) \) is a sheaf, as \( F \) is a presheaf (5.1.3.8).

**Prop. (5.1.3.10) [Stack and Sieves].** A prestack \( F \to \mathcal{C} \) is stack iff for any \( U \in \mathcal{C} \) and any sieve \( S \) on \( U \) belonging to \( T \),

\[
\text{Hom}(h_U, F) \to \text{Hom}(S, F)
\]

is an equivalence of categories.

**Proof:** Let \( S \) be a sieve on \( U \) belong to \( \mathcal{C} \), choose a covering \( U \) of \( U \) that \( h_U \subset S \subset h_U \), then there is a factorization

\[
\text{Hom}(h_U, F) \to \text{Hom}(S, F) \to \text{Hom}(h_U, F).
\]

Then we are done by (5.1.3.9).

**Cor. (5.1.3.11).** Let \( T, T' \) be two topologies on a category \( \mathcal{C} \) that \( T' \) is subordinate to \( T \) and \( F \to C \) is a fibered category, then if \( F \) is a prestack/stack relative to \( T \), it is also true for \( T' \).

**Prop. (5.1.3.12) [2-Fiber Products of Stacks].** There is a natural 2-category of stacks over \( \mathcal{C} \) defined as a sub-2-category of the 2-category of fibered-categories over \( \mathcal{C} \), and the (2,1)-category of stacks over \( \mathcal{C} \) has 2-fibered products, which coincides with that of (3.1.7.15).

**Proof:** Let \( \mathcal{X} \to S, \mathcal{Y} \to S \) be morphisms of stacks over \( \mathcal{C} \), then the category \( \mathcal{X} \times_S \mathcal{Y} \) is a fibered category over \( \mathcal{C} \), by (3.1.7.15). It remains to show that the morphism presheaves sheaves and descent datum are effective.

For this, Cf.[Sta]026G.

**Prop. (5.1.3.13) [Associated Stack in Groupoids].** Let \( \mathcal{C} \) be a site and \( F \) be a prestack, and \( F_{\text{cart}} \) is the associated category fibered in groupoids (3.1.7.24), then \( F_{\text{cart}} \) is also a prestack. And in this case, \( F \) is a stack iff \( F_{\text{cart}} \) is a stack.

**Proof:** The categories \( F(U) \) and \( F_{\text{cart}}(U) \) have the same isomorphism classes of objects, as isomorphisms are Cartesian, so it suffices to show \( F \) is a prestack iff \( F_{\text{cart}} \) is a prestack. For this, use (5.1.3.8) and consider \( \xi, \eta \in F(U) \) and a covering \( \{U_i \to U\} \), if there are arrows \( \alpha_i : \xi_i \to \eta_i \) that
are compatible, then there is a unique arrow $\alpha : \xi \to \eta$ restricting to $\alpha_i$, thus it suffices to show $\alpha$ is Cartesian. But since $\mathcal{F}_{\text{cart}}$ is a category fibered in groupoids, each $\alpha_i$ is invertible, and their inverses glue together to a morphism $\beta : \eta \to \xi$ which is the inverse of $\alpha$, so $\alpha$ is also an isomorphism thus Cartesian.

\begin{prop}[2-Fibered Products of Stacks Fibered in Groupoids] Let $\mathcal{C}$ be a category, the 2-category of stacks fibered in groupoids over $\mathcal{C}$ (automatically a $(2,1)$-category) has 2-fiber products, and coincide with that of $(5.1.3.12)$.\end{prop}

\begin{proof}
 This is clear from $(5.1.3.12)$ and $(3.1.7.26)$.
\end{proof}

\begin{prop}[Equivalence of Stacks] Let $F : \mathcal{S}_1 \to \mathcal{S}_2$ be a morphism of stacks over a site $\mathcal{C}$. If $F$ is fully faithful, then $F$ is an equivalence iff for any $x \in \mathcal{S}_{2,U}$, there exists a covering $\{f_i : U_i \to U\}$ s.t. $f_i^*x$ is in the essential image of the functor $F : \mathcal{S}_{1,U} \to \mathcal{S}_{2,U}$.

\begin{proof}
 Easy.
\end{proof}

\end{prop}

\begin{prop}[Subcanonical Site Prestack] If $\mathcal{C}$ is a subcanonical site $(5.1.2.4)$ and $\mathcal{P}$ is a class of arrows in $\mathcal{C}$ stable under base change, then the corresponding fibered category $\mathcal{P} \to \mathcal{C}$ is a prestack.

\begin{proof}
 By $(5.1.3.8)$, we need to prove for any covering $\{U_i \to U\}$ and arrows $X \to U, Y \to U$, $X_i = U_i \times_U X$, and $X_{ij} = U_{ij} \times_U X$ and analogous for $Y$, if there are arrows $f_i : X_i \to Y_i$ over $U_i$ that the arrows $X_{ij} \to Y_{ij}$ induced by $f_i$ and $f_j$ coincide, then there is a unique arrow $f : X \to Y$ over $U$ that induces $f_i$.

Notice that the composite $X_i \xrightarrow{f_i} Y_i \to Y$ give section $g_i \in \text{h}(Y)(X_i)$, and the pullback of $g_i, g_j$ to $X_{ij}$ coincide by hypothesis. Now $\text{h}(Y)$ is a sheaf by hypothesis, so there is an arrow $f : X \to Y$ that pulls back to $f_i$ on $X_i$. Finally $f$ is compatible over $U$ because $(Y \to U) \circ f$ and $(X \to U)$ coincide when composed with $X_i \to X$, and $h_U$ is a sheaf.

\end{proof}

\end{prop}

\begin{prop}[Category of Sheaves is a Stack] Let $\mathcal{C}$ be a site, we denote $(\text{Sh}/\mathcal{C})(X) = \text{Sh}(\mathcal{C}/X)$, then $\text{Sh}/\mathcal{C}$ is a stack over $\mathcal{C}$.

\begin{proof}
 To show $\text{Sh}/\mathcal{C}$ is a prestack, by $(5.1.3.8)$, it suffices to show for any $F, G \in \text{Sh}(\mathcal{C}/X)$, $\text{Hom}_X(F, G)$ is a sheaf. For this, let $\{U_i \to U\}$ be a covering, and $\varphi_i : F_{U_i} \to G_{U_i}$ be morphisms of sheaves that their restrictions to $F_{U_{ij}} \to G_{U_{ij}}$ are compatible, then for any $T \to U$, there are commutative diagrams

\[
\begin{array}{ccc}
F(T) & \rightarrow & \prod_i F_i(T_i) \\
\downarrow & & \downarrow \\
G(T) & \rightarrow & \prod_i G_i(T_i) \\
\end{array}
\]

where $\varphi_T : F(T) \to G(T)$ is the unique function of sets that makes the diagram commutative. And it can be shown that these $\varphi_T$ defines a natural transformation $F_U \to G_U$.

Now for any covering $\{U_i \to U\}$ and a descent datum $(F_i, F_{ij})$, we need to show it is effective. We define a function $F$ on $\mathcal{C}/U$: $F(T) = \text{equal}(\prod_i F_i(T_i) \Rightarrow \prod_{ij} F(T_{ij}))$, then it can be shown that this is a sheaf by spectral sequence.

Then it suffices to check $F_{U_k} = F_k$. For any $T \to U_k$, $T_i$ maps to $U_{ik}$, so $F_i(T_i) = F_k(T_i)$, thus for any $s \in F_k(T)$, we can produce an element $(s_{T_i}) \in \prod_i F_i(T_i)$ that satisfies compatibility conditions, which gives us an element of $F(T)$. It can be shown this is a natural transformation $F_k \to F_{U_k}$, and it is an isomorphism of sheaves.

\end{proof}

\end{prop}
Prop. (5.1.3.18) [Descent Along Torsors]. Let \( \mathcal{C} \) be a site, \( G \) a group object and \( X \to Y \) a \( G \)-torsor, \( \mathcal{F} \to \mathcal{C} \) a stack. Then there exists a canonical equivalence of categories between \( \mathcal{F}(Y) \) and the category of \( G \)-equivariant objects \( \mathcal{F}^G(X) \) (3.1.7.17).

Proof: By (5.1.1.17) \( X \to Y \) is refined by a covering, thus by (5.1.3.10), \( \mathcal{F}(Y) \) is equivalent to \( \mathcal{F}(X) \cong \mathcal{F}^G(X) \). Then by (5.1.1.18), \( \mathcal{F}(X \to Y) \) consists of elements \( \xi \in \mathcal{F}(X), \eta \in \mathcal{F}(G \times X) \) and Cartesian arrows \( \varphi_1, \varphi_2 \) over \( \alpha, \pi_2 \). Cf. [Vi08] P106.

□

Stackifications

Prop. (5.1.3.19) [Stackification]. Let \( \mathcal{C} \) be a site and \( p : \mathcal{F} \to \mathcal{C} \) a fibered category over \( \mathcal{C} \), then there exists a stack \( p' : \mathcal{F}' \to \mathcal{C} \) and a morphism \( G : \mathcal{F} \to \mathcal{F}' \) of fibered categories over \( \mathcal{C} \) s.t. for any stack \( \mathcal{X} \to \mathcal{C} \), a morphism \( \mathcal{F} \to \mathcal{X} \) of fibered categories over \( \mathcal{C} \) factors through \( G \) 2-commutatively and uniquely up to 2-isomorphisms. In other words, there is a canonical equivalence of categories:

\[
\text{Mor}_{\mathcal{F}ib/\mathcal{C}}(\mathcal{F}, \mathcal{X}) \cong \text{Mor}_{\mathcal{Sta}/\mathcal{C}}(\mathcal{F}', \mathcal{X}).
\]

In particular, such a stack \( \mathcal{F}' \) is determined up to unique 2-isomorphisms, and is called the stackification of \( \mathcal{F} \).

Proof: By (3.1.7.20), we may assume \( \mathcal{F} \) is split, thus \( \mathcal{F} \) corresponds to the functor \( \mathcal{C}^{op} \to \text{Cat} : U \mapsto \text{Hom}(h_U, \mathcal{F}) \). Then we define a functor

\[
\mathcal{F}' : \mathcal{C}^{op} \to \text{Cat} : U \mapsto \lim_{U \in \text{Cov}(U)} \text{Hom}(h_U, \mathcal{F}).
\]

then there is a natural map of fibered categories \( \mathcal{F} \to \mathcal{F}' \). For any stack \( \mathcal{X} \to \mathcal{C} \), because \( \text{Hom}(h_U, \mathcal{X}) \to \text{Hom}(h_U, \mathcal{X}') \) is an isomorphism for any covering \( \mathcal{U} \) of \( U \), we get the desired equivalence of categories. □

Cor. (5.1.3.20). Let \( G : \mathcal{S} \to \mathcal{S}' \) be the stackification of a fibered category over \( \mathcal{C} \), then

- For any \( U \in \mathcal{C} \) and \( x, y \in \mathcal{S}_U \), the map

\[
\text{Hom}(x, y) \to \text{Hom}(G(x), G(y))
\]

identifies the RHS as the shiffication of the LHS.

- For any \( U \in \mathcal{C} \) and \( x \in \mathcal{S}'_U \), there exists a covering \( \{U_i \to U\} \) that for any \( i \), \( x|_{U_i} \) is in the essential image of \( G_U: \mathcal{S}_U \to \mathcal{S}'_U \).

Proof: Cf. [Sta] 0435. □

Prop. (5.1.3.21) [Stackifications Commute with 2-Fibered Products]. Stackifications commute with 2-fibered products.

Proof: Cf. [Sta] 04Y1. □

Prop. (5.1.3.22). If \( \mathcal{F}, \mathcal{G} \) are prestacks over a topological space \( X \), if there is a morphism \( \eta : \mathcal{F} \to \mathcal{G} \) that satisfies:

- \( \mathcal{F} \) is a stack and \( \mathcal{G} \) is a prestack.
- \( \eta \) induces isomorphisms on stalks.
• \(\eta(U) : \mathcal{F}(U) \to G(U)\) is fully faithful.

Then \(\eta\) is an equivalence of prestacks. In particular, \(G\) is also a stack.

Proof: Let \(\mathcal{H}\) be the stackification of \(G\), then \(\mathcal{F} \to \mathcal{G} \to \mathcal{H}\) is a morphism of stacks that is isomorphism on the stalk, so it is an isomorphism. But \(G\) is separated, so for any open \(U\), \(\mathcal{F}(U) \to \mathcal{G}(U), \mathcal{G}(U) \to \mathcal{H}(U)\) is fully faithful, and their composition is an equivalence, thus both of them are equivalences.

\[
\begin{array}{c}
\mathcal{G}|_U \\
\downarrow \\
\text{Aut}(x) \\
\end{array} \xrightarrow{\alpha \mapsto \phi \circ \alpha \circ \phi^{-1}} \begin{array}{c}
\mathcal{G}|_U \\
\downarrow \\
\text{Aut}(y)
\end{array}
\]

is commutative.

Proof: It can be checked by using the fact \(\text{Aut}(x)\) is Abelian that there are canonical morphisms \(\text{Aut}(x) \to \text{Aut}(y)\) induced by any morphism \(\varphi : x \to y\).

If there is no morphism from \(x\) to \(y\), then we can use the condition of gerbe to obtain morphisms \(\text{Aut}(x)|_{U_i} \to \text{Aut}(y)|_{U_i}\) locally, and then glue together. Similarly, if \(S_U\) is empty, then we can restrict to a covering and then glue.

Finally, notice this gives an Abelian sheaf \(\mathcal{G} = \text{Aut}\) on \(\mathcal{C}\).

\[\square\]

Gerbes

Def.(5.1.3.23)[Gerbe]. Let \(\mathcal{C}\) be a site, a gerbe over \(\mathcal{C}\) is a stack in groupoids over \(\mathcal{C}\) s.t.

• For any \(U \in \mathcal{C}\), there is a covering \(\{U_i \to U\}\) that \(S_{U_i}\) is nonempty for any \(i\).

• For any \(U \in \mathcal{C}\) and \(x, y \in S_U\), there exists a covering \(\{U_i \to U\}\) that \(x|_{U_i} = y|_{U_i}\) for any \(i\).

Prop.(5.1.3.24). Let \(p : \mathcal{S} \to \mathcal{C}\) be a gerbe over a site \(\mathcal{C}\), assume that for all \(U \in \mathcal{C}\) and \(x \in S_U\), the sheaf of groups \(\text{Aut}(x)\) on \(\mathcal{C} \leftarrow U\) is Abelian, then there exists a sheaf of Abelian groups over \(\mathcal{C}\) and for any \(x \in S_U\) an isomorphism \(G|_U \to \text{Aut}(x)\) that for any morphism \(\varphi : x \to y \in S_U\), the diagram

\[
\begin{array}{ccc}
\mathcal{G}|_U & \longrightarrow & \mathcal{G}|_U \\
\downarrow & & \downarrow \\
\text{Aut}(x) & \xrightarrow{\alpha \mapsto \phi \circ \alpha \circ \phi^{-1}} & \text{Aut}(y)
\end{array}
\]

is commutative.

Proof: It can be checked by using the fact \(\text{Aut}(x)\) is Abelian that there are canonical morphisms \(\text{Aut}(x) \to \text{Aut}(y)\) induced by any morphism \(\varphi : x \to y\).

If there is no morphism from \(x\) to \(y\), then we can use the condition of gerbe to obtain morphisms \(\text{Aut}(x)|_{U_i} \to \text{Aut}(y)|_{U_i}\) locally, and then glue together. Similarly, if \(S_U\) is empty, then we can restrict to a covering and then glue.

Finally, notice this gives an Abelian sheaf \(\mathcal{G} = \text{Aut}\) on \(\mathcal{C}\).

\[\square\]

Bands

4 Sites over Schemes

Prop.(5.1.4.1). Fiber products exist in the category of schemes, by(5.2.7.15).

Zariski Topology

Def.(5.1.4.2)[Zariski Topology]. The Zariski topology has the the covering of a scheme \(T\) as classes of open immersions \(\{T_i \to T\}\) that their images cover \(T\).

The Zariski site \(\mathcal{Sch}_{\text{Zar}} / S\) has the objects as all schemes over \(S\).

The small Zariski site \(S_{\text{Zar}}\) has the objects as all open subschemes over \(S\).

The restricted Zariski site \(S_{\text{Zar} f_p}\) has the objects as all schemes that are qcqs open subschemes of \(S\).

The big affine Zariski site \(\text{Aff}_{\text{Zar}} / S\) has the objects as all schemes affine over \(S\).

These are all topologies because open immersions satisfies base change trick(5.4.4.60).
In particular when the cover has only one element and is affine, the descent datum is equivalent to compatible isomorphisms
\[ \varphi_{13} : N \otimes_A B \otimes_A B \xrightarrow{\varphi_{12}} B \otimes_A M \otimes_B \xrightarrow{\varphi_{23}} B \otimes_A B \otimes_A M. \]

**Def. (5.1.4.3) [Zariski Stacks]**. The category of sheaves on \( \mathcal{S}ch_{\text{Zar}} / S \) is denoted by \( \text{Sh}_{\text{Zar}} / S \). The category of stacks on \( \mathcal{S}ch_{\text{Zar}} / S \) is denoted by \( \text{Sta}_{\text{Zar}} / S \).

**Prop. (5.1.4.4) [Affine and Full Sites]**. The inclusion functor \( \mathcal{A}ff_{\text{Zar}} / S \to \mathcal{S}ch_{\text{Zar}} / S \) is a special cocontinuous functor, so by (5.1.2.23), it induces an equivalence of topoi \( \text{Sh}(\mathcal{A}ff_{\text{Zar}} / S) \cong \text{Sh}_{\text{Zar}} / S \).

**Def. (5.1.4.5) [Restriction to Small Sites]**. The inclusion functor \( S_{\text{Zar}} \to \mathcal{S}ch_{\text{Zar}} / S \) satisfies the hypothesis of (5.1.2.22), thus induces morphisms of topoi
\[ \pi_S : \text{Sh}_{\text{Zar}} / S \to \text{Sh}(S_{\text{Zar}}), \quad i_S : \text{Sh}(S_{\text{Zar}}) \to \text{Sh}_{\text{Zar}} / S \]
that satisfies \( \pi_S \circ i_S = \text{id}_{S_{\text{Zar}}} \). In particular, \( i_S^{-1} \mathcal{F} \) is called the **restriction to small sites** of \( \mathcal{F} \).

**Prop. (5.1.4.6)**. A sheaf w.r.t the small Zariski topology is equivalent to a sheaf on \( S \), trivially, so the sheaf cohomology on \( \mathcal{A}ff_{\text{Zar}} / S \) is equivalent to usual sheaf cohomology on \( S \).

**Prop. (5.1.4.7) [Transfer of Big Sites]**. Let \( f : T \to S \in \mathcal{S}ch_{\text{Zar}} / S \), then \( \mathcal{S}ch_{\text{Zar}} / T \to \mathcal{S}ch_{\text{Zar}} / S \) is a localization, so by (5.1.2.21) it induces a morphism of topoi
\[ f : \text{Sh}_{\text{Zar}} / T \to \text{Sh}_{\text{Zar}} / S : f^{-1} \mathcal{G}(U/T) = \mathcal{G}(U/S), \quad f_\ast \mathcal{F}(U/S) = \mathcal{F}(U \times_S T/T). \]

**Prop. (5.1.4.8) [Transfer of Small Sites]**. Let \( f : T \to S \in \mathcal{S}ch_{\text{Zar}} / S \), then the base change functor \( S_{\text{Zar}} \to T_{\text{Zar}} \) is continuous, and by (5.1.2.14) induces a morphism of topoi
\[ f : \text{Sh}_{\text{Zar}} / T \to \text{Sh}_{\text{Zar}} / S. \]

**Prop. (5.1.4.9)**. If \( X \) is qs, then \( \text{Sh}(X_{\text{Zar}}) \to \text{Sh}(X_{\text{Zar}} fp) \) is an equivalence by \( i_s \) and \( i^s \)

*Proof:* The proof is the same proof as that of (5.1.20). \( \square \)

---

**Étale Topology**

**Def. (5.1.4.10) [Étale Topology]**. The **étale topology** has the covering of a scheme \( T \) as classes of étale morphisms that their images cover \( T \).

- The **étale site** \( \mathcal{S}ch_{\text{ét}} / S \) has the objects as all schemes over \( S \).
- The **small étale site** \( S_{\text{ét}} \) has the objects as all schemes that are étale over \( S \).
- The **restricted étale site** \( S_{\text{ét}} fp \) has the objects as all schemes that are étale and qcqs over \( S \).
- The **big affine étale site** \( \mathcal{A}ff_{\text{ét}} / S \) has the objects as all schemes affine over \( S \).

These are truly topologies because étale is stable under base change and composition.

**Prop. (5.1.4.11)**. Zariski covering is étale , because open immersions are étale.

**Prop. (5.1.4.12)**. For a family of maps in \( S_{\text{ét}} \) to be a covering, it suffices to check their image is adjointly surjective, by (5.6.6.4).

**Prop. (5.1.4.13) [Affine and Full Sites]**. The inclusion functor \( \mathcal{A}ff_{\text{ét}} / S \to \mathcal{S}ch_{\text{ét}} / S \) is a special cocontinuous functor, so by (5.1.2.23), it induces an equivalence of topoi \( \text{Sh}(\mathcal{A}ff_{\text{ét}} / S) \cong \text{Sh}_{\text{ét}} / S. \)
Def. (5.1.4.14) [Restriction to Small Sites]. The inclusion functor $S_{\text{ét}} \to \mathcal{S}_{\text{ét}}/S$ satisfies the hypothesis of (5.1.2.22), thus induces morphisms of topoi

$$
\pi_S : \mathcal{S}_{\text{ét}}/S \to \mathcal{S}(S_{\text{ét}}), i_S : \mathcal{S}(S_{\text{ét}}) \to \mathcal{S}_{\text{ét}}/S
$$

that satisfies $\pi_S \circ i_S = \text{id}_{\mathcal{S}_{\text{ét}}}$. In particular, $i_S^{-1} F$ is called the restriction to small sites of $F$.

Prop. (5.1.4.15). Any étale covering of a qc scheme can be refined a finite covering by affine étale schemes, this is because étale map are open (5.6.6.3).

Def. (5.1.4.16) [Étale Stacks]. The category of sheaves on $\mathcal{S}_{\text{ét}}/S$ is denoted by $\mathcal{S}(S_{\text{ét}})/S$. The category of stacks on $\mathcal{S}_{\text{ét}}/S$ is denoted by $\mathcal{S}_{\text{ét}}/S$.

Prop. (5.1.4.17). For a qc scheme $X$, $X_{\text{ét}}/\text{fp}$ is a Noetherian topology, because étale map is open, and any object in $X_{\text{ét}}/\text{fp}$ is qc.

Prop. (5.1.4.18) [Transfer of Big Sites]. Let $f : T \to S \in \mathcal{S}_{\text{ét}}/S$, then the functor $u : \mathcal{S}_{\text{ét}}/T \to \mathcal{S}_{\text{ét}}/S$ is cocontinuous, and has base change as a right adjoint, so by (5.1.2.21) it induces a morphism of topoi

$$
f : \mathcal{S}(T_{\text{ét}})/T \to \mathcal{S}(S_{\text{ét}})/S : f^{-1} \mathcal{G}(U/T) = \mathcal{G}(U/S), \quad f_* F(U/S) = F(U \times_S T/T).
$$

Prop. (5.1.4.19) [Transfer of Small Sites]. Let $f : T \to S \in \mathcal{S}_{\text{ét}}/S$, then the base change functor $S_{\text{ét}} \to T_{\text{ét}}$ is continuous, and by (5.1.2.14) induces a morphism of topoi

$$
f : \mathcal{S}(T_{\text{ét}}) \to \mathcal{S}(S_{\text{ét}})
$$

Prop. (5.1.4.20). If $X$ is qs, then $\mathcal{S}(X_{\text{ét}}) \to \mathcal{S}(X_{\text{ét}}/\text{fp})$ is an equivalence by $i_s$ and $i^s$.

Proof: Want to use (5.1.2.24), one condition is satisfied by (5.1.4.15), so it suffice to check any $X' \in X_{\text{ét}}$ has an étale covering by schemes étale and qcqs over $X$. For any point $p \in X'$, there is an affine nbhd $U'$ that maps to an affine nbhd $U'$ of $X$, so $U' \to U$ is étale and qcqs, and $U \to X$ is open immersion and qs, it is qc because $X$ is qs and $U$ is qc (5.4.4.27). So these affine nbhds $U'$ cover $X'$.

Prop. (5.1.4.21) [Cohomology Big and Small Sites]. The inclusion of small sites to the big sites has no infection on the sheaf cohomology, by (5.3.1.5). This is applicable to all topologies $\tau$ considered here.

Prop. (5.1.4.22) [Topological Invariance of Étale Sites]. If $f : S' \to S$ is universally homeomorphism, then $f : S'_{\text{ét}} \to S_{\text{ét}}$ is an equivalence of sites.

In particular this applies to $S' = S_{\text{red}}$.

Proof: Cf. [Étale Cohomology Conrad P18].

Smooth Topology

This topology will be shown to be identical to the étale topology, so it is not so important.

Def. (5.1.4.23) [Smooth Topology]. The smooth topology has the covering of a scheme $T$ as classes of smooth morphisms that their images cover $T$.

The big smooth site $\mathcal{S}_{\text{sm}}/S$ has the objects as all schemes over $S$.

The small smooth site $S_{\text{sm}}$ has the objects as all schemes that are smooth over $S$.

The restricted smooth site $S_{\text{ét}}/\text{fp}$ has the objects as all schemes that are smooth and qcqs over $S$.

The big affine smooth site $\mathcal{A}_{\text{ff}}/S$ has the objects as all schemes affine over $S$.

These are truly topologies because smoothness is stable under base change and composition.
Syntomic Topology

Def. (5.1.4.24) [Syntomic Topology]. The syntomic topology has the covering of a scheme $T$ as classes of syntomic morphisms that their images cover $T$.

fppf Topology

Def. (5.1.4.25) [Fppf Topology]. The fppf topology has the covering of a scheme $T$ as classes of flat locally of finite presentation morphisms that their images cover $T$. (f.f.+locally of f.p.).

The big Zariski site $\text{Sch}_{\text{fppf}}/S$ has the objects as all schemes over $S$.

The big affine Zariski site $\text{Aff}_{\text{fppf}}/S$ has the objects as all schemes affine over $S$.

They are all topologies because flatness and finite presentedness satisfy base change trick by (5.6.2.1) and (5.6.1.1).

Prop. (5.1.4.26) [Syntomic Covering is Fppf]. A syntomic covering is fppf by definition (4.4.4.18).

Prop. (5.1.4.27). A fppf covering of an affine scheme can be refined a finite affine fppf covering, because fppf map are open (5.6.2.10).

Def. (5.1.4.28) [Fppf Stacks]. The category of sheaves on $\text{Sch}_{\text{fppf}}/S$ is denoted by $\text{Sh}_{\text{fppf}}/S$. The category of stacks on $\text{Sch}_{\text{fppf}}/S$ is denoted by $\text{Sta}_{\text{fppf}}/S$.

fpqc Topology

Def. (5.1.4.29) [Fpqc Topology]. The fpqc topology has the covering of a scheme $T$ as classes of flat morphisms s.t. their images cover $T$ and for any affine open $U \subset T$, the restriction on $T$ can be refined by a finite affine cover of open affine subschemes of the covering (f.f.+qc). It is a topology by (5.6.2.1) and (5.4.4.25).

When the covering consists of affine schemes, it is called a standard fpqc covering.

Def. (5.1.4.30) [Fpqc Stacks]. Defining fpqc sites has inescapable set-theoretic difficulties, thus we don’t consider fpqc sites and fpqc cohomologies. Cf. [Sta]0BBK.

Nevertheless, we will denote the category of presheaves on $\text{Sch}/S$ satisfying the sheaf condition w.r.t. the fpqc topology by $\text{Sh}_{\text{fpqc}}/S$, and denote the category of fibered categories over $\text{Sch}/S$ satisfying the sheaf condition w.r.t. the fpqc topology by $\text{Sta}_{\text{fpqc}}/S$.

Prop. (5.1.4.31) [fppf is fpqc]. Fppf coverings are fpqc.

Proof: Use (5.6.2.10), we see that fppf covering consists of open morphisms, thus it is qc because affine scheme is quasi-compact.

Prop. (5.1.4.32). A covering consisting of flat morphisms refined by a fpqc covering is a fpqc covering.

Hence being fpqc is local on the target, because a Zariski cover is a fpqc covering.

If $U$ is a covering consisting of flat morphisms that there is a fpqc covering $V$ that $U \times V \rightarrow V$ is a fpqc covering, then $U$ is fpqc, because $U \times V$ does and it refines $U$.

Lemma (5.1.4.33) [Checking Sheaf Condition]. Let $S \in \text{Sch}$, $F \in \mathcal{P}h^{\text{Set}}((\text{Sch}_S)_{\text{fpqc}})$ is a sheaf iff it is a sheaf w.r.t the Zariski topology and satisfies sheaf property w.r.t the single covering $V \rightarrow U$ f.f. between affine schemes.

Proof: This follows from (5.1.3.5)(5.1.3.6) and (5.1.5.7).
Prop. (5.1.4.34) [fpqc Site is Subcanonical]. The coverings in $(\text{Sch}_S)_{\text{fpqc}}$ are families of universal effective epimorphisms. In other words, $(\text{Sch}_X)_{\text{fpqc}}$ is subcanonical. In particular, for any covering $\mathcal{U} = \{U_i \to X\} \in \text{Cov}((\text{Sch}_S)_{\text{fpqc}})$ and $\{V_{ijk} \to U_i \times_X U_j\} \in \text{Cov}((\text{Sch}_S)_{\text{fpqc}})$,

$$X = \text{Coeq}(\prod_{i,j,k} V_{ijk} \Rightarrow \prod_i U_i) \in \text{Sch}_S.$$ 

Proof: By (5.1.4.33), it suffices to show that any representable presheaf is a sheaf w.r.t Zariski topology and f.f. affine morphisms. The Zariski case follows from (5.1.5.3), for the second, $\text{Spec } B \to \text{Spec } Z$, for any scheme $X$, the morphism corresponds to $0 \to \text{Hom}(R,A) \to \text{Hom}(R,B) \to \text{Hom}(R,B \otimes_A B)$, but this follows immediately from (4.4.2.2), with $M = A$. □

Cor. (5.1.4.35). For $f : Y \to X$ a morphism of schemes, if $Z \in X_\tau$ for the above topologies $\tau$, then $f^* (\text{Hom}_X(-,Z)) \cong \text{Hom}(-,Z \otimes_X Y)$, in other words, the inverse sheaf of a representable sheaf is representable.

Proof: By definition, $f^* (\text{Hom}_X(-,Z))$ is the sheaf associated to the presheaf $f_* (\text{Hom}_X(-,Z))$, which by (5.1.2.13) is just the presheaf represented by $Z \otimes_X Y$, but by the proposition, it is already a sheaf. □

Prop. (5.1.4.36) [Coherent Sheaves on $\text{Sch}_{\text{fpqc}} / X$]. Let $F \in \mathcal{QCoh}(X)$, then the functor $X' \to \Gamma(X', \mathcal{F} \otimes_{O_X} O_{X'})$ satisfies the the axiom for Abelian sheaves on $\text{Sch}_{\text{fpqc}} / X$, by (5.1.5.13).

Prop. (5.1.4.37) [Qco Sheaves on Sites]. For $X \in \text{Sch}, \tau \in \{\text{fppf, étale, smooth, syntomic, Zariski}\}$, restriction defines an equivalence of categories

$$\mathcal{QCoh}(X) \cong \mathcal{QCoh}(\text{Sch}_\tau / X).$$

And if $\tau \in \{\text{Zariski, étale}\}$, restriction defines an equivalence of categories

$$\mathcal{QCoh}(X) \cong \mathcal{QCoh}(X_\tau).$$

Proof: Cf. [Sta]03DX. □

PH-Covering

Def. (5.1.4.38) [Standard PH-Covering].

Def. (5.1.4.39) [PH-Topology].

Prop. (5.1.4.40) [Zariski Covering is PH-Covering]. A Zariski covering is a PH-covering.

Proof: Cf. [Sta]0DBH. □

Prop. (5.1.4.41). A proper surjective morphism is a ph-covering.

Proof: Cf. [Sta]0DES. □
V-Topology

Def. (5.1.4.42) [Standard V-Covering]. A finite family of morphisms $T_i \to X$ of affine schemes is a covering in the standard $v$-topology if for any morphism $\text{Spec} \, V \to X$ where $V$ is a valuation ring, there is an extension of valuation rings (10.3.2.11) $V \to W$ and a morphism $\text{Spec} \, W \to \text{Spec} \, V \times_X T_i$ for some $i$.

Def. (5.1.4.43) [V-Topology]. A family of morphisms $\{T_i \to T\}$ is called a $v$-covering in the $v$-topology if for any open affine subscheme $U$ of $T$, the base change is refined by a standard $v$-covering of $U$.

The $v$-coverings form a topology, by [Sta]0ETJ.

Lemma (5.1.4.44). A standard fpqc covering is a standard $v$-covering.

Proof: Cf. [Sta]022E. □

Prop. (5.1.4.45) [fpqc Covering is V-Covering]. A fpqc covering is a $v$-covering.

Proof: This follows immediately from (5.1.4.44). □

Prop. (5.1.4.46). A standard ph-covering is a standard $v$-covering.

Proof: Cf. [Sta]0ETD □

Prop. (5.1.4.47) [ph-Covering is V-Covering]. A ph-covering is a $v$-covering.

Proof: This follows immediately from (5.1.4.46). □

Cor. (5.1.4.48). A proper and surjective map is a $v$-covering, by (5.1.4.47) and (5.1.4.41).

Arc-Topology

Def. (5.1.4.49) [Arc-Topology]. A finite family of morphisms $\{T_i \to X\}$ of schemes is a covering in the arc-topology if for any morphism $\text{Spec} \, V \to X$ where $V$ is a rank 1 valuation ring, there is a rank 1 valuation ring $W$ and a morphism $\text{Spec} \, W \to \text{Spec} \, V \times_X T_i$ for some $i$ that $V \to W$ is f.f..

Prop. (5.1.4.50). $V$-coverings are arc coverings.

Proof: This is by the definition and (10.3.2.11). □

5 Descent for Algebraic Spaces

Main references are [Sta] Chap34, 10.158.

General Principal

Prop. (5.1.5.1). A property of schemes is called local in a topology if for any covering $\{U_i \to S\}$, $S$ has $P$ iff $U_i$ has $P$. A property of morphisms is called local in a topology if for any covering $\{U_i \to S\}$, $X \to S$ has $P$ iff $X \times_S U_i \to U_i$ has $P$.

Prop. (5.1.5.2) [Twists and Čech Cohomology]. Let $\xi$ be an object of a stack $\mathcal{F}$ over a site $\mathcal{C}$ lying over an object $U$ of $\mathcal{C}$, we call an object $\xi' \in \mathcal{F}(U)$ a twist of $\xi$ if there is some covering $\{U_i \to U\}$ that the pullback of $\xi$ and $\xi'$ to $U_i \to U$ are isomorphic.

Then there is a natural bijection between $\mathcal{F}(U)$-isomorphism classes of twists of $\xi$ with $\hat{H}^1(U, \text{Aut}(\xi))$.

Proof: Cf. [Appendix of Lamb]. □
5.1. SITES, SHEAVES AND STACKS

Zariski Descent

Lemma (5.1.5.3) [Zariski Descent of Qco Sheaves]. The fibered category $X \mapsto (\mathcal{Q}\text{coh}/X)$ is a stack over $\text{Sch}_{\text{Zar}}/S$.

Proof: This is a consequence of (5.1.3.17) and the fact quasi-coherentness is a Zariski local property. □

Prop. (5.1.5.4) [Zariski Descent of Schemes]. The fibered category $X \mapsto \text{Sch}/X$ is in $\text{St}_{\text{Zar}}/S$.

Proof: Firstly it is a prestack by (5.1.3.16) and (5.1.4.34).

To show any descent datum of effective, let $\{U_i \to U\}$ be a Zariski covering, and $X_i \to U_i$ be schemes with descent datum $\varphi_{ij} : X_i \times_{U_i} U_{ij} \cong X_j \times_{U_j} U_{ij}$, then we define $X = \bigsqcup X_i/\sim$, where $x_i \sim x_j$ if $x_i \in U_{ij}, x_j \in U_{ji}$ and $\varphi_{ij}(x_i) = \varphi_{ji}(x_j)$. It can be shown this is an equivalence relation. Denote $\varphi_i : X_i \to X$ the natural map, and $U_i = \varphi_i(X_i)$. Define the topology on $X$ as the quotient topology. In particular, $\varphi_i$ is a homeomorphism onto the image. Then we can use (5.1.3.17) to glue the sheaves of rings $(\varphi_i)_*(\mathcal{O}_{X_i})$ to a sheaf of rings $\mathcal{O}_X$ on $X$ that $\varphi_i^*\mathcal{O}_X = \mathcal{O}_{X_i}$. Also we have a map $f : X \to U$ by set-theoretical and topological consideration. For the structure map $f^{-1}(\mathcal{O}_U) \to \mathcal{O}_X$, use (5.1.3.17). □

Cor. (5.1.5.5). If $\mathcal{P}$ is a subclass of arrows of schemes that is stable under base change and local on the target, then $\mathcal{P}/S$ is a stack over $(\text{Sch}/S)_{\text{Zar}}$.

Cor. (5.1.5.6) [Zariski Descent of Schemes with a Qco Sheaf]. The fibered category $X \mapsto \{$Schemes over $X$ with a Qco sheaf $\mathcal{F}\}$ is a stack in the Zariski topology $\text{Sch}_{\text{Zar}}/S$.

Proof: This is a combination of (5.1.5.4) and (5.1.5.3). □

Fpqc Descent

Prop. (5.1.5.7) [Reduction to Affine Case]. Let $S$ be a scheme and $\mathcal{F}$ be a fibered category over $\text{Sch}/S$. Suppose that

- $\mathcal{F}$ is a stack w.r.t. the Zariski topology.
- When $V \to U$ is a f.f. morphism of affine $S$-schemes, $\mathcal{F}(U) \to \mathcal{F}(V \to U)$ is an equivalence of categories.

then $\mathcal{F}$ is a stack w.r.t the fpqc topology.

Proof: Firstly, to show $\mathcal{F}$ is a prestack, using (5.1.3.8), it suffices to show for an $S$-scheme $T \to S$ and objects $\xi, \eta \in \mathcal{F}(T)$, the functor

$$\text{Hom}_T(\xi, \eta) : (\text{Sch}/T)^{\text{op}} \to \text{Set}$$

is a sheaf. But then we can use (5.1.4.33) to achieve this.

Next, according to (3.1.7.20) and (5.1.3.7), we may assume $\mathcal{F}$ is splitting.

Notice that $\mathcal{F}(\emptyset)$ is equivalent to the category pt. This is because $\mathcal{F}(\emptyset)$ is equivalent to $\mathcal{F}(\mathcal{U})$, where $\mathcal{U}$ is the null Zariski covering of $\emptyset$(with no mapping or objects at all!). Then for any disjoint union of open subschemes $U = \bigsqcup U_i$, there is a natural isomorphism of categories $\mathcal{F}(U) \cong \bigsqcup \mathcal{F}(U_i)$.

Thus for any covering $\mathcal{U} = \{U_i \to X\}$, to show $\mathcal{F}(X) \to \mathcal{F}(\mathcal{U})$ is an equivalence of categories, it suffices to show that $\mathcal{F}(X) \to \mathcal{F}(\bigsqcup U_i \to X)$ is an equivalence of categories: this is because $\bigsqcup U_i \times_X \bigsqcup U_i \cong \bigsqcup U_i \times_X U_j$, so $\mathcal{F}(\bigsqcup U_i \to X) \to \mathcal{F}(\mathcal{U})$ is an equivalence of categories.
If \( \mathcal{U} = \{ V \to U \} \) is a covering of \( F \) with a single morphism that is qc and \( U \) is affine, then by the proof of (5.1.3.10), we can choose a finite affine cover of \( V \) reduce to the case of covering of f.m. affine maps, then we finish by the case above.

If \( \mathcal{U} = \{ V \to U \} \) is a covering of \( F \) with a single morphism and \( U \) is affine, then we can find a Zariski covering \( \{ V_i \to V \} \) that each \( V_i \) is qc. and surjects onto \( U \). Then there are maps of categories \( \mathcal{F}(U) \to \mathcal{F}(\{ V \to U \}) \to \mathcal{F}(\{ V_i \to V \}) \), where \( \mathcal{F}(U) \to \mathcal{F}(\{ V_i \to V \}) \) is an equivalence and \( \mathcal{F}(U) \to \mathcal{F}(\{ V \to U \}) \) is fully faithful. Thus to show \( \mathcal{F}(U) \to \mathcal{F}(\{ V \to U \}) \) is an equivalence, it suffices to show \( \mathcal{F}(\{ V \to U \}) \) is faithful, which is true by (5.1.3.9).

For general case, Cf. [Vis08] P88. \( \square \)

**Prop. (5.1.5.8).** Mor \( /S : X \to \text{Sch} / X \) is a prestack over \( \text{Sch}_{\text{fpqc}} / S \), by (5.1.4.34) and (5.1.3.16).

**Def. (5.1.5.9) [Affine Fpqc Descent Datum].** For \( A \to B \in \mathcal{C}_{\text{Alg}} \), define a category \( \text{Mod}_{A \to B} \) as follows: its objects are pairs \( (N, \psi) \), where \( N \in \text{Mod}_B \) and \( \psi : N \otimes_A B \to B \otimes_A N \) is an isomorphism of \( B \otimes_A B \)-modules s.t. that

\[
\psi_{ij} \circ \psi_{01} = \psi_{02} : N \otimes_A B \otimes_A B \to B \otimes_A B \otimes_A N
\]

where \( \psi_{ij} \) is permuting the \( i \), \( j \)-parts using \( \psi \). The morphisms in \( \text{Mod}_{A \to B} \) are maps in \( \text{Mod}_B \) that is compatible with \( \psi \).

There is a natural functor \( \text{Mod}_{A \to B} \to \text{Mod}_B \).

**Lemma (5.1.5.10) [Affine Fpqc Descent].** For \( A \to B \in \mathcal{C}_{\text{Alg}} \), there is a functor \( F : \text{Mod}_A \to \text{Mod}_{A \to B} \), where \( M \) is mapped to \( (B \otimes_A M, \psi_M) \) with

\[
\psi_M : (B \otimes_A M) \otimes_A B \to B \otimes_A (B \otimes_A M) : b \otimes m \otimes b' \mapsto b \otimes b \otimes m.
\]

Then when \( A \to B \) is f.f., this is an equivalence of categories.

**Proof:** We construct an inverse \( T \) that maps \( (N, \psi) \) to \( \{ n | \psi(n \otimes 1) = 1 \otimes n \} \). Then \( TF \cong \text{id} \) because of the first exactness of (4.4.2.2).

And for \( FT \cong \text{id} \), let \( T((N, \psi)) = M \). Notice if \( \psi(n \otimes 1) = \sum_i b_i \otimes n_i \), then by cocycle condition,

\[
\sum_i b_i \otimes 1 \otimes n_i = \sum_i b_i \otimes \psi(n_i \otimes 1).
\]

so \( \psi(N \otimes 1) \subset \ker(\text{id}_B \otimes (n \mapsto \psi(n \otimes 1) - 1 \otimes n)) = B \otimes M \) because \( B/A \) is flat.

So we defined a map \( N \xrightarrow{\psi} B \otimes_A M \in \text{Mod}_B \), and the composition \( B \otimes_A M \xrightarrow{\text{mul.}} N \xrightarrow{\psi} B \otimes_A M \) is identity, because

\[
\psi(bm \otimes 1) = (b \otimes 1)\psi(m \otimes 1) = (b \otimes 1)(1 \otimes m) = b \otimes m.
\]

This shows \( \Psi \) is surjective. And \( \Psi \) is injective because \( n \mapsto n \otimes 1 \) is injective as \( B/A \) is f.f., and \( \psi \) is an isomorphism. So \( \Psi \) is an isomorphism of \( N \cong FT(N) \).

Finally, to show \( \psi = \psi_M \), as now \( B \otimes_A M \xrightarrow{\text{mul.}} N \) is an isomorphism, we check

\[
\psi((bm) \otimes b') = (b \otimes b')\psi(m \otimes 1) = (b \otimes b')(1 \otimes m) = b \otimes (b'm).
\]

\( \square \)
**Remark (5.1.5.11).** In fact, a descent datum is always effective iff $A \to B$ is universally injective. Cf.[Sta]. And f.f. extension is u.i.(4.4.1.28).

**Prop. (5.1.5.12) [fpqc Descent for Qco Sheaves].** Let $S$ be a scheme, then $\mathcal{QCoh}/\mathcal{Sch} \in \mathcal{St}_{\text{fpqc}}/S$.

*Proof:* We use(5.1.5.7), the first condition is satisfied by(5.1.5.3), and for the second condition, let $\text{Spec} B \to \text{Spec} A$ be a f.f. morphism of affine schemes, then $\mathcal{QCoh}(\text{Spec} B \to \text{Spec} A)$ is equivalent to $	ext{Mod}_{A\to B}$, and $\mathcal{QCoh}(\text{Spec} A)$ is equivalent to $\text{Mod}_{A}$, so the conclusion follows from(5.1.5.10). □

**Cor. (5.1.5.13).** For any $\mathcal{F} \in \mathcal{QCoh}(S)$, the functor $(\mathcal{Sch}/S)^{\text{op}} \to Ab: T \to \Gamma(T, f^{*}\mathcal{F}) \in \mathcal{St}_{\text{fpqc}}/S$, hence are also sheaves w.r.t. the fppf, étale, Zariski topologies.

*Proof:* Because this functor is just $\text{Hom}_{S}(\mathcal{O}_{S}, \mathcal{F})$, and it is a sheaf(5.1.3.8). □

**Cor. (5.1.5.14).** If $\mathcal{P}$ is a property of Qco sheaves that is stable under base change and fpqc local, then $\mathcal{QCoh}_{\mathcal{P}}/S \in \mathcal{St}_{\text{fpqc}}/S$.

**Prop. (5.1.5.15) [Descending Affine Morphisms].** For a scheme $S$, let $\mathcal{P}$ be the class of affine arrows in $\mathcal{Sch}/S$ that denote by $\text{Mor}^{\text{Aff}}$ the resulting fibered category, then $\text{Mor}^{\text{Aff}}_{S} \in \mathcal{St}_{\text{fpqc}}/S$.

*Proof:* Firstly $\text{Mor}^{\text{Aff}}/S \in \mathcal{St}_{\text{Zar}}/S$, and it satisfies the affine fpqc descent condition of(5.1.5.7)(Notice the $\{n|\psi(n \otimes 1) = 1 \otimes n\}$ is now a ring, because $\psi$ is a ring homomorphism), so we are done by(5.1.5.7). □

**Cor. (5.1.5.16).** If $\mathcal{P}$ is a subclass of affine arrows stable under base change and fpqc local on the target, then $\text{Mor}^{\mathcal{P}}/S \in \mathcal{St}_{\text{fpqc}}/S$.

**Prop. (5.1.5.17) [Descent via Ample Invertible Sheaves].** Let $S$ be a scheme and $\mathcal{P}$ be a class of flat proper morphisms of f.p. in $\mathcal{Sch}/S$ that is local in the fpqc topology. Assume that for each object $\xi: X \to U \in \mathcal{P}$, we have an invertible sheaf $\mathcal{L}_{\xi}$ on $X$ that is ample relative to $X \to U$, and for an arrow $f: (X \xrightarrow{\xi} U) \to (Y \to \eta V)$, we have an isomorphism $\rho_{f}: f^{*}\mathcal{L}_{\eta} \cong \mathcal{L}_{\xi}$ that satisfies $\rho_{gf} = \rho_{f} \circ f^{*}\rho_{g}$, then $\text{Mor}^{\mathcal{P}}/S \in \mathcal{St}_{\text{fpqc}}/S$.

*Proof:* Cf.[Vistoli, P96]. □

**Étale Descent**

**Prop. (5.1.5.18) [Galois Descent].** Let $L/K$ be a finite separable field extension with Galois group $G$, then $\text{Spec} L \to \text{Spec} K$ is a $G$-torsor in the étale topology. so Galois descent is a special case of étale descent along torsors(5.1.3.18).

Notice this is also true for arbitrary finite separable field extensions with continuity condition added, because we can take direct limits of categories over its finite normal subextensions.

*Proof:* Consider the locally constant group scheme $G = \text{Spec} (\prod_{g \in G} K)$, let $X = \text{Spec} L, Y = \text{Spec} K$, then $\{X \to Y\}$ is an étale cover, and the action $G \times X \to X$ is given by

$$L \to \prod_{g \in G} L : x \mapsto \prod_{g \in G} (g(x)).$$

Thus $X \to Y$ is a $G$-equivariant map, and there is an isomorphism $G \times X \cong X \times_{Y} X : (g, x) \mapsto (gx, x)$ that corresponds to the isomorphism

$$L \otimes_{K} L \cong \prod_{g \in G} L : (a, b) \mapsto \prod_{g \in G} (g(a)b)$$

□
Cor. (5.1.5.19) [Galois Descent of Closed Immersions]. Let $X$ be a scheme over a field $k$, and $K/k$ be a Galois field extension with Galois group $\Gamma$, $X' = X \otimes_K K$. Then the category of closed subschemes of $X$ is equivalent to the category of closed subschemes that is base change from some $X'_{k'}$ where $k'/k$ is finite, and is stable under the action of $\Gamma$. This weird finiteness condition can be removed when $X$ is locally algebraic over $k$.

Proof: This is because the class of closed immersions is a stack (5.1.5.16).

Remark (5.1.5.20). When $Y$ is a subvariety of $X$ and $K = k^s$, to check $Y$ is stable under action of $\Gamma$, it suffices to check that the geometric points is closed under action of $\Gamma$. This is because the geometric points are dense in $Y'$ (5.10.1.10).

Cor. (5.1.5.21) [Galois Descent for Ideals of Algebras]. Let $A \in \mathcal{C}_{\text{Alg}}_k$, and $K/k$ be a Galois field extension with Galois group $\Gamma$, then the category of ideals of $A$ is equivalent to the category of ideals of $A_K$ that is base change from some $A_{k'}$ where $k'/k$ is finite, and is stable under the action of $\Gamma$. This weird finiteness condition can be removed when $A$ is f.g. over $k$.

Cor. (5.1.5.22) [Galois Descent of Morphisms]. Let $X, Y$ be locally algebraic schemes over $k$ and $K/k$ a Galois field extension with Galois group $\Gamma$, $X' = X \otimes_K K, Y' = Y \otimes_K K$. If $Y$ is separated, then a morphism $\varphi' : X' \to Y'$ arises from a morphism $X \to Y$ iff its graph $\Gamma_{\varphi'} \subset X' \times_{k'} Y'$ is stable under action of $\Gamma$. In this case $\varphi$ is unique.

And when $X, Y$ are varieties and $K = k^s$, then it suffices to check the map

$$\varphi'(k^s) : X'(k^s) \to Y'(k^s)$$

commutes with action of $\Gamma$.

Cor. (5.1.5.23) [Galois Descent for Qco Sheaves]. Let $K/k$ be a Galois extension with Galois group $\Gamma$ and $X$ be a scheme over $k$ with $X' = X \otimes_K K$, then $\mathcal{Q}\text{coh}/X \to (\mathcal{Q}\text{coh}/X')^\Gamma$ is an equivalence of categories.

Proof: This is because $\mathcal{Q}\text{coh}/\text{Sch}$ is a fpqc stack (5.1.5.12).

Cor. (5.1.5.24) [Galois Descent for Vector Spaces]. Let $K/k$ be a Galois extension with Galois group $\Gamma$. Then the functor $V \mapsto K \otimes_V K$ induces an equivalence between the category of vector spaces over $k$ and the category of vector spaces over $K$ together with a continuous semi-linear action of $\Gamma$.

Prop. (5.1.5.25) [Failure of Étale Descent for proper smooth morphisms]. Cf. [Vis08] P107.

Descend Properties

Prop. (5.1.5.26) [Properties of Morphisms Local in Fpqc Topology]. The following properties of morphisms are local on the target w.r.t. the fpqc topology.

1. quasi-compact.
2. (quasi-)separated.
3. Universally closed.
4. universally open.
5. universally submersive.
6. surjective.
7. universally injective.
8. universally homeomorphism.
9. (locally)of f.t.
10. (locally)of f.p.
11. properness.
12. flatness.
13. (closed/open)immersion.
14. isomorphism/monomorphism.
15. (quasi-)affineness.
16. quasi-compact immersion.
17. integral
18. (locally)(quasi-)finite.
19. syntomic.
20. smooth, unramified, étale.
21. finite locally free.

Proof: Cf. [Sta] Chap 34.20.
18.
19. Cf. [Sta]00SM.
20.
21.

Prop. (5.1.5.27) [Properties of Schemes Local in the Fppf Topology].


Prop. (5.1.5.28) [Descending Properties that is not Fpqc Local].

- If $X \to Y$ is a faithfully flat morphism of schemes and $X$ is (geo.) reduced, then $Y$ is also (geo.) reduced.
- If $X \to Y$ is a faithfully flat morphism of f.p. between schemes and $X$ is (geo.) regular, then $Y$ is also (geo.) regular.

Proof: Looking stalkwise, these follows from (4.4.2.1).

Prop. (5.1.5.29) [Torsors]. Let $G$ be a group object in $(\text{Sch}_S)^{\tau}$ and $X \to S$ a $G$-torsor. Then if $\tau$ is a subcanonical site and $P$ is a property that is local on $(\text{Sch}_S)^{\tau}$ and $G \to S$ has $P$, then $X \to S$ has $P$.

Proof: By (5.1.1.17), there is a covering $\{Y_i \to S\}$ s.t. each $X \times_S Y_i \to Y_i \cong G \times_S Y_i$ is trivial, thus each $X \times_S Y_i \to Y_i$ has $P$, and then $X \to S$ has $P$.

Weil Restrictions

Def. (5.1.5.30) [Weil Restrictions]. Let $L/k$ be a finite extension of fields, $X \in \text{Sch}/L$, then the Weil restriction $\text{res}_{L/k}(X)$ is the scheme over $k$ representing the functor

$$\text{Sch}/k \to \text{Set} : S \mapsto X(S \times_k L).$$

Prop. (5.1.5.31). Let $L/k$ be a finite extension of fields, and $X \in \text{Sch}/L$. If every finite subset of $X$ is contained in some affine open subset of $X$, then $\text{res}_{L/K}(X)$ exists. In particular, this applies to the case that $X$ is quasi-projective.

Proof: Cf. [BLR90, Chap 7.6. Thm 4].

6 Étale Torsors

Prop. (5.1.6.1). For $X \in \text{Sch}$, $\check{H}^1(X, \text{GL}(n)) \cong \text{Vect}^n(X)$ as pointed sets, by (5.1.5.2).
5.2 Ringed Topoi, Ringed Sites, Ringed $G$-Spaces and Schemes

1 Ringed Topoi, Ringed Sites

Def.(5.2.1.1)[Ringed Topoi]. A ringed topos is a pair $(\mathcal{S}h(\mathcal{C}), \mathcal{O})$ where $\mathcal{C}$ is a site and $\mathcal{O}$ is a unital object in $\mathcal{S}h(\mathcal{C})$, called the structure sheaf. A morphism of of ringed topoi $(f, f^\#) : (\mathcal{C}, \mathcal{O}) \to (\mathcal{C}', \mathcal{O}')$ consists of a morphism of topoi (5.1.2.18) $f : \mathcal{S}h(\mathcal{C}) \to \mathcal{S}h(\mathcal{C}')$ and a map of sheaves of rings $f^\# : f^{-1}\mathcal{O}' \to \mathcal{O}$. A composition of morphism of topoi is defined to be $(g, g^\#) \circ (f, f^\#) = (g \circ f, f^\# \circ f^{-1}(g^\#))$.

Def.(5.2.1.2)[Ringed Sites]. A ringed site is pair $(\mathcal{C}, \mathcal{O})$ where $\mathcal{C}$ is a site and $\mathcal{O}$ is a sheaf of rings on $\mathcal{C}$, called the structure sheaf. A ringed site induces a ringed topos. A morphism of ringed sites is a morphism of sites that the induced morphism of topoi (5.1.2.19) is a morphism of ringed topoi (5.2.1.1).

A site is naturally a ringed site where $\mathcal{O} = \mathbb{Z}$ the constant sheaf (5.1.2.8). So we only consider ringed sites afterwards, then a morphism of ringed sites is naturally a morphism of ringed sites. So whenever we say $\mathcal{C}$ is a site, it is understood as a ringed site $(\mathcal{C}, \mathbb{Z})$.

Prop.(5.2.1.3)[Ringed Topoi and Ringed Sites]. Let $(f, f^\#) : (\mathcal{S}h(\mathcal{C}), \mathcal{O}_C) \to (\mathcal{S}h(\mathcal{D}), \mathcal{O}_D)$ be a morphism of ringed topoi, then we can find ringed sites $(\mathcal{C}', \mathcal{O}_{C'})$ and $(\mathcal{D}', \mathcal{O}_{D'})$ and a diagram

$$(\mathcal{S}h(\mathcal{C}), \mathcal{O}_C) \xrightarrow{(f, f^\#)} (\mathcal{S}h(\mathcal{D}), \mathcal{O}_D) \xleftarrow{(g, g^\#)} (\mathcal{S}h(\mathcal{C}'), \mathcal{O}_{C'}) \xrightarrow{(h, h^\#)} (\mathcal{S}h(\mathcal{D}'), \mathcal{O}_{D'})$$

where

- $(g, g^\#)$ and $(e, e^\#)$ are equivalence of ringed topoi.
- $\mathcal{C}', \mathcal{D}'$ have final objects and finite products.
- $(h, h^\#)$ is induced by a continuous functor $\mathcal{D}' \to \mathcal{C}'$ that the preserves the final object and finite products,(thus induces a morphism of sites by (5.1.2.14)).

Moreover, given a set of sheaves $\mathcal{F}_i$ on $\mathcal{C}$ and a set of sheaves $\mathcal{G}_i$ on $\mathcal{D}$, we may choose $\mathcal{C}'$ and $\mathcal{D}'$ that these sheaves are representable by objects in $\mathcal{C}'$ or $\mathcal{D}'$.

Proof: [Sta]03CR. □

Prop.(5.2.1.4)[Multiplicative Structure Sheaf]. Given a ringed topos $(\mathcal{S}h(\mathcal{C}), \mathcal{O})$, the presheaf $U \mapsto \mathcal{O}^*(U)$ is a sheaf of groups, called the multiplicative structure sheaf $\mathcal{O}^*$.

Proof: This comes from the sheaf property of $\mathcal{O}$ and the fact the inverse of an element is unique. □

Def.(5.2.1.5)[Local Ringed Site]. A ringed site $(\mathcal{C}, \mathcal{O})$ is called a local ringed site if

$$\mathcal{O}^\# \to \text{Equalizer}(0, 1 : \text{pt} \to \mathcal{O})$$

is an isomorphism of sheaves, and for any $U \in \mathcal{C}$ and $f \in \mathcal{O}(U)$, there exists a covering $\{U_i \to U\}$ s.t. for any $j$, either $f|_{U_i}$ is invertible or $(1 - f)|_{U_i}$ is invertible.
Prop. (5.2.1.6) [Characterizing Local Ringed Sites]. Let \((\mathcal{C}, \mathcal{O})\) be a ringed site, the following are equivalent:

- \((\mathcal{C}, \mathcal{O})\) is a local ringed site.
- (Partition of Unity) For any \(U \in \mathcal{C}, f_1, \ldots, f_n \in \mathcal{O}(U)\) that \((f_1, \ldots, f_n) = (1)\), there is a covering \(\{U_i \to U\}\) that for each \(j\), there exists an \(i\) that \(f_i\) is invertible on \(U_j\).
- The map of sheaves of sets:
  \[
  (\mathcal{O} \otimes \mathcal{O}) \coprod (\mathcal{O} \times \mathcal{O}) \to \mathcal{O} \times \mathcal{O}
  \]
  which maps \((f, a)\) in the first component to \((f, af)\) and \((f, b)\) in the second component to \((f, b(1 - f))\) is surjective.

Proof: Cf. [Sta]04ES.

Def. (5.2.1.7) [Local Ringed Topoi]. If \(f : \text{Sh}(\mathcal{C}') \to \text{Sh}(\mathcal{C})\) is a morphism of topoi and \((\mathcal{C}, \mathcal{O})\) is a local ringed site, then \((\text{Sh}(\mathcal{C}'), f^{-1}\mathcal{O})\) is also a local ringed site. In particular, being a local ringed site is an intrinsic property, so we can define local ringed topoi to be ringed topoi that the underlying ringed sites are local ringed.

Proof: Because \(f^{-1}\) is exact (5.1.2.18) and commutes with products and equalizers, it maps the isomorphism

\[
\emptyset \to \text{Equalizer}(0, 1 : \text{pt} \to \mathcal{O})
\]

to the corresponding isomorphism of \(\mathcal{C}'\), and also the sejection of

\[
(\mathcal{O} \otimes \mathcal{O}) \coprod (\mathcal{O} \times \mathcal{O}) \to \mathcal{O} \times \mathcal{O}
\]

in (5.2.1.6) to that of \(\mathcal{C}'\), thus \((\text{Sh}(\mathcal{C}'), f^{-1}\mathcal{O})\) is also a local ringed site.

Def. (5.2.1.8) [Morphisms of Local Ringed Topoi]. A morphism of local ringed topoi is a morphism of ringed topoi \((f, f^\#) : (\text{Sh}(\mathcal{C}), \mathcal{O}_C) \to (\text{Sh}(\mathcal{D}), \mathcal{O}_D)\) that the diagram of sheaves

\[
\begin{array}{ccc}
  f^{-1}(\mathcal{O}_D^\ast) & \xrightarrow{f^\#} & \mathcal{O}_C^\ast \\
  \downarrow & & \downarrow \\
  f^{-1}(\mathcal{O}_D) & \xrightarrow{f^\#} & \mathcal{O}_C
\end{array}
\]

is Cartesian, where \(\mathcal{O}_C^\ast\) is the multiplicative structure sheaf (5.2.1.4). Morphisms of local ringed topoi are stable under compositions.

**Ringed Spaces**

Def. (5.2.1.9) [Ringed Spaces]. A ringed space is a pair \((X, \mathcal{O}_X)\) consisting of a topological space \(X\) and a sheaf of rings \(\mathcal{O}_X\) on \(X\). A morphism of ringed spaces \((X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)\) consists of a pair \((f, f^\#)\) where \(f\) is a continuous map \(X \to Y\) and \(f^\#\), which induces a map of sites \((f^{-1}, f^\#) : X_{\text{Zar}} \to Y_{\text{Zar}}\) (5.2.6.7), and \(f^\#_s\) is a map \(f^\# : f^{-1}(\mathcal{O}_Y) \to \mathcal{O}_X\) (5.2.6.2), such that \((f, f^\#)\) is a morphism of ringed topoi (5.2.1.1).
Def. (5.2.1.10)[Local Ringed Space]. A local ringed space is a topological space $X$ with a sheaf of rings $\mathcal{O}_X$ that $(X, \mathcal{O}_X)$ forms a local ringed site $(5.2.1.5)$. A morphism of local ringed space is a morphism of ringed spaces that the corresponding morphism of ringed topoi $(\mathcal{S} \mathcal{h}(\mathcal{C}), \mathcal{O}_C) \to (\mathcal{S} \mathcal{h}(\mathcal{D}), \mathcal{O}_D)$ is a morphism of local ringed topoi $(5.2.1.8)$.

Prop. (5.2.1.11). A ringed space $(X, \mathcal{O}_X)$ is a locally ringed space iff any stalks $\mathcal{O}_{X,x}$ is either 0 or a local rings.

Proof: Cf. [Sta]04ET. □

2 Modules on Ringed Topoi

Main References are [Sta]Chap 18.

Def. (5.2.2.1)[Modules on Ringed Topoi]. Let $(\mathcal{S} \mathcal{h}(\mathcal{C}), \mathcal{O})$ be a ringed topos, then a sheaf of $\mathcal{O}$-modules is a presheaf of $\mathcal{O}$-modules that the underlying presheaf of Abelian groups is a sheaf.

Def. (5.2.2.2)[Support]. Let $(X, \mathcal{O}_X)$ be a ringed space, $\mathcal{F}$ a $\mathcal{O}_X$-module, then the support of $\mathcal{F}$ is the set of points $x$ that $\mathcal{F}_x \neq 0$. It is denoted by $\text{Supp}(\mathcal{F})$. For a section $s \in \Gamma(X, \mathcal{F})$, $\text{Supp}(s)$ is defined to be the set of points $x$ that $s_x \neq 0 \in \mathcal{F}_x$.

Prop. (5.2.2.3). Glueing sheaves is available for ringed spaces, similar to (5.1.5.3).

Proof:

Prop. (5.2.2.4). Glueing ringed spaces is available.

Proof:

Def. (5.2.2.5)[Local Properties of Modules]. On a ringed site $(\mathcal{C}, \mathcal{O})$, an $\mathcal{O}$-module $\mathcal{F}$ is called locally has property $P$ if for any object $U \in \mathcal{C}$, there is a covering $\{U_i \to U\}$ that $\mathcal{F}|_{U_i}$ has property $P$.

Def. (5.2.2.6)[Intrinsic Properties of Modules]. An intrinsic property of sheaves of modules in a ringed topos $(\mathcal{S} \mathcal{h}(\mathcal{C}), \mathcal{O})$ that is invariant under equivalence of topoi.

Def. (5.2.2.7)[Tensor Products Sheaf]. Let $(\mathcal{C}, \mathcal{O})$ be a ringed site and $\mathcal{F}, \mathcal{G}$ be $\mathcal{O}$-modules, then the tensor product $\mathcal{F} \otimes_{\mathcal{O}} \mathcal{G}$ is defined to be the shification of the presheaf $U \mapsto \mathcal{F}(U) \otimes_{\mathcal{O}(U)} \mathcal{G}(U)$.

The tensor product is easily seen to be an intrinsic notion $(5.2.2.6)$, so it can be defined on any ringed topos.

Prop. (5.2.2.8)[Base Change]. Let $(\mathcal{C}, \mathcal{O})$ be a ringed site and $\mathcal{O}_2$ be a sheaf $\mathcal{O}_1$-algebras, $\mathcal{G}$ be a sheaf of $\mathcal{O}_1$-module and $\mathcal{F}$ a sheaf of $\mathcal{O}_2$-module, then

$$\text{Hom}_{\mathcal{O}_1}(\mathcal{G}, \mathcal{F}_{\mathcal{O}_1}) = \text{Hom}_{\mathcal{O}_2}(\mathcal{G} \otimes_{\mathcal{O}_1} \mathcal{O}_2, \mathcal{F}).$$

Proof: This can be seen from the definition of tensor product and the fact shification doesn’t bother because $\mathcal{F}$ is a sheaf. □

Def. (5.2.2.9)[Transfer of Modules on Ringed Sites]. Let $(f, f^\sharp)$ be a morphism of ringed topoi $(\mathcal{S} \mathcal{h}(\mathcal{C}), \mathcal{O}) \to (\mathcal{S} \mathcal{h}(\mathcal{C}', \mathcal{O}'))$, then there are functor:

- the pushforward: $f_* : \text{Mod}(\mathcal{O}) \to \text{Mod}(\mathcal{O}') : f_* \mathcal{F} = f_* \mathcal{F}$ as a $\mathcal{O}'$-module via $\mathcal{O}' \to f_* \mathcal{O}$. 


• the pullback $f^*: \text{Mod}(O') \to \text{Mod}(O) : f^*G = O \otimes_{f^{-1}O'} f^{-1}G$ via $f^2: f^{-1}O' \to O$. $f^*$ is left adjoint to $f_*$, by the adjointness of $f^{-1}$ and $f_*(5.1.2.18)$.

If $(f, f^2)$ is a morphism of ringed sites $(C, O) \to (C', O')$, then there is an extension by zero functor:

- (Extension by zero): For the localization of sites $j_U : (C/U, O_U) \to (C, O)$ the localization map of site, $j_U^* = j_U^{-1}$ has a left adjoint $j_U^!$ defined by shifification of the presheaf $G \mapsto j_U!(G) : j_U!(G)(V) = \bigoplus_{\varphi: V \to U} G(V) \otimes O$.  

Proof: To show $j_U^!$ is left adjoint to $j_U^*$, Cf.[Sta]03DI. \hfill \square

Remark (5.2.2.10). The $f^*$ may not be exact. $f^{-1}$ is exact, but we tensored with $O_X$, it is exact when $f$ is flat(5.2.2.15).

Prop.(5.2.2.11)[Extension by Zero is Exact]. Let $(C, O)$ be a ringed site and $U \in C$, then the extension by zero functor $j_U^! : \text{Mod}(O_U) \to \text{Mod}(O)$ is exact and reflects exactness.

Proof: It is right exact because it is a left adjoint, and it is left exact by direct inspection. 

For reflection of exactness, Cf.[Sta]08E5G. \hfill \square

Prop.(5.2.2.12)[Tensor Products and Pullbacks]. Tensor products commute with pullbacks, in particular with taking stalks. So tensoring with a locally free sheaf is exact.

Proof: By (5.2.3.3) and (5.2.3.5), for any $O$-module $H$,

\[ \text{Hom}(f^*F \otimes f^*G, H) = \text{Hom}(F, f_*\text{Hom}(f^*G, H)) = \text{Hom}(F, \text{Hom}(G, f_*H)) = \text{Hom}(f^*(F \otimes G), H). \]

\hfill \square

Prop.(5.2.2.13)[$j_U^!$ Commutes with Restriction]. Let $(C, O)$ be a ringed site and $U \in C, G \in \text{Mod}(O_U), F \in \text{Mod}(O)$, then there is a natural isomorphism $j_U^!G \otimes_O F \cong j_U^!(G \otimes_{O_U} F|_U)$

Proof: By (5.2.3.3) and (5.2.3.5), for any $H \in \text{Mod}(O)$,

\[ \text{Hom}_O(j_U^!(G \otimes_{O_U} F|_U), H) = \text{Hom}_{O_U}(G \otimes_{O_U} F|_U, H|_U) = \text{Hom}_{O_U}(G, \text{Hom}_O(F|_U, H|_U)) = \text{Hom}_O(j_U^!G, \text{Hom}_O(F, H)) = \text{Hom}_O(j_U^!G \otimes_O F, H) \]

then use Yoneda lemma. \hfill \square

Prop.(5.2.2.14)[Properties of Tensor Products]. Let $(C, O)$ be a ringed site and $F, G$ be sheaves of $O$-modules, then

1. If $F, G$ are locally free, then so does $F \otimes G$.
2. If $F, G$ are locally finite free, then so does $F \otimes G$.
3. If $F, G$ are locally generated by sections, then so does $F \otimes G$.
4. If $F, G$ are of f.t., then so does $F \otimes G$.
5. If $F, G$ are quasi-coherent, then so does $F \otimes G$.
6. If $F, G$ are of f.p., then so does $F \otimes G$.
7. If $F$ is of f.p. and $G$ is coherent, then $F \otimes G$ is coherent. In particular, if $F, G$ are coherent, then so does $F \otimes G(5.2.2.27)$.

Proof: Cf.[Sta]03L6. \hfill \square
Flat Modules

Def. (5.2.2.15) [Flat Modules and Flat Morphisms]. Let \( \mathcal{C} \) be a site and \( \mathcal{O} \) a presheaf of rings, then a presheaf \( \mathcal{F} \) of \( \mathcal{O} \)-modules is called **flat** if the functor \( \text{PMod}(\mathcal{O}) \to \text{PMod}(\mathcal{O}) : \mathcal{G} \mapsto \mathcal{G} \otimes_{\mathcal{O}} \mathcal{F} \) is exact.

Let \( \mathcal{C} \) be a ringed site, and \( \mathcal{F} \) is a sheaf of \( \mathcal{O} \)-modules, then it is called **flat** if the functor \( \text{Mod}(\mathcal{O}) \to \text{Mod}(\mathcal{O}) : \mathcal{G} \mapsto \mathcal{G} \otimes_{\mathcal{O}} \mathcal{F} \) is exact.

A morphism \((f, f^\#)\) is called a **flat morphism** if the ring map \( f^\# : f^{-1} \mathcal{O}' \to \mathcal{O} \) is flat, or equivalently, the pullback functor (5.2.2.9) \( f^* \) is exact.

Prop. (5.2.2.16). Let \( \mathcal{C} \) be a site and \( \mathcal{O} \) a presheaf of rings with shiffication \( \mathcal{O}^\sharp \).
- If \( \mathcal{F} \) is a presheaf of \( \mathcal{O} \)-modules that each \( \mathcal{F}(U) \) is flat \( \mathcal{O}(U) \)-modules, then \( \mathcal{F} \) is flat.
- If \( \mathcal{F} \) is a flat presheaf of \( \mathcal{O} \)-modules, then \( \mathcal{F}^\# \) is a flat \( \mathcal{O}^\sharp \)-modules.
- A filtered colimits of flat presheaves of modules is flat. A direct sum of flat presheaves of modules is flat.
- A filtered colimits of flat sheaves of modules is flat. A direct sum of flat sheaves of modules is flat.

Prop. (5.2.2.17) [Flatness is Stalkwise]. Let \((X, \mathcal{O}_X)\) be a ringed space, then an \( \mathcal{O}_X \)-module \( \mathcal{F} \) is flat iff the stalks \( \mathcal{F}_x \) are all flat \( \mathcal{O}_{X,x} \)-modules.

Proof: Cf. [Sta]05NE. \( \square \)

Prop. (5.2.2.18) [Flat Morphism and Support]. Let \( f : (X, \mathcal{O}_X) \to (X', \mathcal{O}_{X'}) \) be a flat morphism of local ringed spaces, \( \mathcal{F} \) an \( \mathcal{O}_{X'} \)-module, then \( \text{Supp}(f^*(\mathcal{F})) = f^{-1}(\text{Supp}(\mathcal{F})) \).

Proof: Use the fact flat ring map of local rings is faithfully flat. \( \square \)

Modules of Finite Type & Finite Presentation

Def. (5.2.2.19) [Finite Type]. An \( \mathcal{O} \)-module is called **finite type** iff locally a quotient of a finite free sheaf.

Prop. (5.2.2.20) [Extension of F.T. Sheaves]. if \( 0 \to \mathcal{F}_1 \to \mathcal{F}_2 \to \mathcal{F}_3 \to 0 \) is an exact sequence of \( \mathcal{O} \)-modules and \( \mathcal{F}_1, \mathcal{F}_3 \) are of f.t., then \( \mathcal{F}_2 \) is of f.t..

Proof: For any \( U \in \mathcal{C} \), choose a covering \( \{ U_i \to U \} \) that \( \mathcal{F}_3(U_i) \) is generated by f.m. sections, then by passing to a covering, we may assume these sections come from \( \mathcal{F}_2 \). Pass to another covering that \( \mathcal{F}_1 \) is generated by f.m. sections, then on this covering, \( \mathcal{F}_2 \) is generated by f.m. sections. \( \square \)

Def. (5.2.2.21) [Finite Presentation]. A sheaf of modules \( \mathcal{F} \) is called **of finite presentation** iff locally it is a cokernel of two finite free modules. The pullback of a f.p. sheaf is f.p, by the left adjointness of \( f^* \).

Prop. (5.2.2.22) [FP-FT-FT]. If \( f : \mathcal{G} \to \mathcal{F} \) is a surjection of \( \mathcal{O} \)-modules, \( \mathcal{F} \) is of f.p. and \( \mathcal{G} \) is of f.t., then the kernel is of finite type.
Proof: We first show for $G = \mathcal{O}_n$: By pass to covering, we can construct a diagram

$$
\begin{array}{ccc}
\mathcal{O}^n_{U_{ij}} & \longrightarrow & \mathcal{O}^n_{U_{ij}} \\
& & \downarrow \alpha \\
0 & \longrightarrow & \ker(f)|_{U_{ij}} \\
\end{array}
\quad \Rightarrow 
\begin{array}{ccc}
\mathcal{G}|_{U_{ij}} & \longrightarrow & \mathcal{F}|_{U_{ij}} \\
& & \downarrow \\
0 & \longrightarrow & \mathcal{F}|_{U_{ij}} \\
\end{array}
$$

and then use snake lemma. The image and cokernel of $\alpha$ are all of f.t., then $\ker(f)|_{U_{ij}}$ is of f.t. by (5.2.2.20).

For general $G$, locally choose a surjection $\varphi : \mathcal{O}_n|_{U_t} \rightarrow G|_{U_t}$, then $\ker(f|_{U_t}) = \varphi(\ker(\varphi \circ f|_{U_t}))$, which is of f.t.. $\square$

Prop. (5.2.2.23). Pullbacks of a module of finite type is of finite type. Pullback of a module of finite presentation is of finite presentation.

Finite type and finite presentation are local on the target.

Proof: This is because pullback is a left adjoint thus right exact. They are local on the target because they are defined locally. $\square$

Prop. (5.2.2.24) [Support is Zariski Closed]. If $(X, \mathcal{O}_X)$ is a ringed space and $f : \mathcal{G} \rightarrow \mathcal{F}$ is surjective at a point $x$ and $\mathcal{F}$ is of f.t., then it is surjective on a Zariski nbhd of $x$. Thus the support of a f.t. sheaf is closed (look at $0 \rightarrow \mathcal{F}$).

Proof: Choose a nbhd of $x$ that $\mathcal{F}(U)$ is generated by $s_1, \ldots, s_n \in \mathcal{F}(U)$, because $f$ is surjective at the stalk of $x$, after shrinking $U$, we may assume $s_i = f(t_i)$ for $t_i \in \mathcal{G}(U)$, so $f$ is surjective on $U$. $\square$

(Quasi-)Coherent Sheaves

Def. (5.2.2.25) [Quasi-Coherent Sheaf]. An $\mathcal{O}$-module $\mathcal{F}$ on a ringed site is called quasi-coherent iff locally it is a cokernel of two free modules. A locally f.p. sheaf of modules is $\text{Qco}$.

Prop. (5.2.2.26) [Associated $\text{Qco}$ Sheaves]. And for a ringed space $(X, \mathcal{O}_X)$ and a $R = \Gamma(X, \mathcal{O}_X)$-module $M$, we have a coherent sheaf $\mathcal{F}_M$ on $X$, defined as $\pi^*(M)$, where $M$ is seen as a qco sheaf on $(\text{pt}, R)$. It is the sheaf associated to the presheaf $U \mapsto \mathcal{O}_X(U) \otimes M$.

This construction is a functor from the category of $R$-module to the category of $\text{Qco} \mathcal{O}_X$-modules, and it commutes with colimits because $\pi^*$ does. And it is left adjoint to $\Gamma$ by (5.2.2.9):

$$\text{Hom}_A(M, \Gamma(X, \mathcal{G})) \cong \text{Hom}_{\mathcal{O}_X}(\mathcal{F}_M, \mathcal{G})$$

Def. (5.2.2.27) [Coherent Sheaves]. A coherent sheaf is an $\mathcal{O}$-module $\mathcal{F}$ that is of f.t. and for any object $U$ and for any set of elements of $\Gamma(U, \mathcal{F})$, the kernel of $\oplus \mathcal{O}_U \rightarrow \mathcal{F}|_U$ is of f.t..

A coherent sheaf is of f.p., by base change to a smaller covering, and it is $\text{Qco}$.

Prop. (5.2.2.28) [Properties of Coherent Sheaves]. Any f.t. subsheaf of a coherent sheaf is coherent, by definition. Any kernel of a morphism from a f.t. sheaf to a coherent sheaf is of f.t..

$\text{Coh}(X)$ is a weak Serre subcategory of $\text{Mod}_{\mathcal{O}_X}$. In particular, if $\mathcal{O}_X$ is coherent, then a sheaf is coherent iff it is f.p.
Prop. (5.2.2.29). The pullback of a (quasi-)coherent module is a (quasi-)coherent, because \( f^* \) is a left adjoint.

Prop. (5.2.2.30). (Quasi-)Coherence is local on the target.

Proof: This is because they are defined locally. □

Prop. (5.2.2.31). Let \((X, \mathcal{O}_X)\) be a ringed space and \(x \in X\).

- Let \(f : \mathcal{G} \to \mathcal{F}\) be a map of \(\mathcal{O}_X\)-modules. If \(\mathcal{G}\) is of f.t. and \(\mathcal{F}\) is coherent, and \(f\) is injective at the stalk of \(x\), then there exists a nbhd \(U\) of \(x\) that \(f|_U\) is injective.

- Let \(f : \mathcal{G} \to \mathcal{F}\) be a map of coherent \(\mathcal{O}_X\)-modules that is surjective at the stalk of \(x\), then there exists a nbhd \(U\) of \(x\) that \(f|_U\) is surjective.

- Let \(f : \mathcal{G} \to \mathcal{F}\) be a map of coherent \(\mathcal{O}_X\)-modules that is isomorphism at the stalk of \(x\), then there exists a nbhd \(U\) of \(x\) that \(f|_U\) is an isomorphism.

Proof: 1: Consider the kernel of \(f\), then it is of f.t. by definition (5.2.2.27). Then \(\ker(f)_x = 0\), so there is a nbhd \(U\) of \(x\) that \(\ker(f)|_U = 0\), by (5.2.2.24), which means \(f|_U\) is injective.

2: this is immediate from (5.2.2.24).

3 follows from 1 and 2. □
3 Construction of Sheaves

Internal Hom

Def.(5.2.3.1)[Internal Hom]. Let \(\mathcal{C}\) is a category and \(\mathcal{O}\) is a presheaf of rings, \(\mathcal{F}, \mathcal{G}\) be presheaves of \(\mathcal{O}\)-modules, then \(U \mapsto \text{Hom}_{\mathcal{O}|U}(\mathcal{F}|U, \mathcal{G}|U)\) defines a presheaf \(\text{Hom}(\mathcal{F}, \mathcal{G})\) of \(\mathcal{O}\)-modules, and there is a natural evaluation map

\[
\mathcal{F} \otimes_{\mathcal{O}} \text{Hom}(\mathcal{F}, \mathcal{G}) \to \mathcal{G}.
\]

Now if \(\mathcal{C}\) is a site and \(\mathcal{O}\) is a sheaf of rings, \(\mathcal{F}, \mathcal{G}\) be sheaves of \(\mathcal{O}\)-modules, then \(\text{Hom}_{\mathcal{O}}(\mathcal{F}, \mathcal{G})\) is a sheaf of \(\mathcal{O}\)-modules by (5.1.3.17), called the internal Hom sheaf. Denote \(\text{Hom}(\mathcal{F}, \mathcal{O})\) by \(\mathcal{F}^\vee\).

Prop.(5.2.3.2). Internal Hom sheaf commutes with localization: \(\text{Hom}_{\mathcal{O}|U}(\mathcal{F}|U, \mathcal{G}|U) = \text{Hom}_{\mathcal{O}}(\mathcal{F}, \mathcal{G})|_U\). This follows from the definition.

Prop.(5.2.3.3)[Tensoring and Inner Hom]. If \(\mathcal{C}\) is a site, \(\mathcal{O}\) is a sheaf of rings and \(\mathcal{F}, \mathcal{G}, \mathcal{H}\) are sheaves of \(\mathcal{O}\)-modules, then there is a canonical isomorphism of sheaves:

\[
\text{Hom}_{\mathcal{O}}(\mathcal{H} \otimes_{\mathcal{O}} \mathcal{F}, \mathcal{G}) \cong \text{Hom}_{\mathcal{O}}(\mathcal{F}, \text{Hom}_{\mathcal{O}}(\mathcal{H}, \mathcal{G})).
\]

In particular, taking limit over \(\mathcal{C}\), we see \(- \otimes_{\mathcal{O}} \mathcal{H}\) is left adjoint to \(\text{Hom}_{\mathcal{O}}(\mathcal{F}, -)\):

\[
\text{Hom}_{\mathcal{O}}(\mathcal{H} \otimes_{\mathcal{O}} \mathcal{F}, \mathcal{G}) \cong \text{Hom}_{\mathcal{O}}(\mathcal{F}, \text{Hom}_{\mathcal{O}}(\mathcal{H}, \mathcal{G})).
\]

In particular, the monoidal category of \(\mathcal{O}_X\)-modules is closed (5.2.2.15).

Proof: Omitted (Recall the definition of tensor product sheaf (5.2.2.7)).

Prop.(5.2.3.4).

\[
\text{Hom}(\lim A_i, B) \cong \lim \text{Hom}(A_i, B) \quad \text{Hom}(A, \lim B_i) \cong \lim \text{Hom}(A, B_i)
\]

Proof: This is immediate from (3.1.4.9).

Prop.(5.2.3.5). \(f^\ast\) is left adjoint to \(f_\ast\) by (5.2.2.9): \(\text{Hom}_{\mathcal{O}_Y}(f^\ast \mathcal{G}, \mathcal{F}) \cong \text{Hom}_{\mathcal{O}_Y}(\mathcal{G}, f_\ast \mathcal{F})\). In fact

\[
f_\ast(\text{Hom}_{\mathcal{O}}(f^\ast \mathcal{G}, \mathcal{F})) \cong \text{Hom}_{\mathcal{O}}(\mathcal{G}, f_\ast \mathcal{F}).
\]

by checking on every open subset \(U \subset Y\).

Prop.(5.2.3.6). Let \(\mathcal{C}\) be a site and \(\mathcal{O} \to \mathcal{O}'\) is a map of sheaves of rings, then for any \(\mathcal{G} \in \text{Mod}(\mathcal{O}')\) and \(\mathcal{F} \in \text{Mod}(\mathcal{O})\), there is a natural isomorphism

\[
\text{Hom}_{\mathcal{O}}(\mathcal{G}, \mathcal{F}) = \text{Hom}_{\mathcal{O}'}(\mathcal{G}, \text{Hom}_{\mathcal{O}}(\mathcal{O}', \mathcal{F})).
\]

by checking on every open subset \(U \subset Y\).

Prop.(5.2.3.7). Let \(f_\ast : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)\) be a morphism of ringed spaces, and \(\mathcal{F}, \mathcal{G}\) are \(\mathcal{O}_Y\)-modules. If \(\mathcal{F}\) is f.p. and \(f\) is flat, then the canonical map

\[
f^\ast \text{Hom}_{\mathcal{O}_Y}(\mathcal{F}, \mathcal{G}) \to \text{Hom}_{\mathcal{O}_X}(f^\ast \mathcal{F}, f^\ast \mathcal{G})
\]

is an isomorphism.
5.2. RINGED TOPOI, RINGED SITES, RINGED G-SPACES AND SCHEMES

Proof: 

Prop.(5.2.3.8). Let \((X, \mathcal{O}_X)\) be a ringed space and \(\mathcal{F}, \mathcal{G}\) be \(\mathcal{O}_X\)-modules. If \(\mathcal{F}\) is f.p. or locally free, then the canonical map

\[\text{Hom}(\mathcal{F}, \mathcal{G})_x \to \text{Hom}_{\mathcal{O}_X,x}(\mathcal{F}_x, \mathcal{G}_x)\]

is an isomorphism.

Proof: Choose a presentation of \(\mathcal{F}\). This follows from the exactness of taking stalks and (5.2.3.4).

Prop.(5.2.3.9). Let \((X, \mathcal{O}_X)\) be a ringed site and \(\mathcal{F}, \mathcal{G}\) be \(\mathcal{O}_X\)-modules. If \(\mathcal{F}\) is f.p. and \(\mathcal{G}\) is coherent, then \(\text{Hom}(\mathcal{F}, \mathcal{G})\) is also coherent. In particular, this applies to \(\mathcal{F}, \mathcal{G}\) both coherent.

Proof: This follows from (5.2.3.4) and (5.2.2.28).

Tensor Sheaves

Def.(5.2.3.10)[Tensor Sheaves]. Let \((\mathcal{C}, \mathcal{O})\) be a ringed site and \(\mathcal{F}\) an \(\mathcal{O}\)-module, then we define

- \(T(\mathcal{F})\) to be the sheafification of the presheaf \(U \mapsto T_{\mathcal{O}_X}(\mathcal{F}(U))\) (4.1.1.20).
- \(\wedge \mathcal{F}\) to be the sheafification of the presheaf \(U \mapsto \wedge_{\mathcal{O}_X(U)}(\mathcal{F}(U))\) (4.1.1.20).
- \(\text{Sym}(\mathcal{F})\) to be the sheafification of the presheaf \(U \mapsto \text{Sym}_{\mathcal{O}_X(U)}(\mathcal{F}(U))\) (4.1.1.20).

Cor.(5.2.3.11). Over a ringed space \((X, \mathcal{O}_X)\), the construction of \(T(\mathcal{F}), \wedge(\mathcal{F})\) and \(\text{Sym}(\mathcal{F})\) commutes with taking stalks, because the construction of tensor algebras and sheffification are both left adjoints (4.1.1.21). Also they commutes with pullbacks, because they satisfy the same universal properties.

Prop.(5.2.3.12). let \(\mathcal{F}\) be an \((\mathcal{C}, \mathcal{O})\)-module, then the following properties are preserved under the construction of \(T(\mathcal{F}), \wedge(\mathcal{F})\) and \(\text{Sym}(\mathcal{F})\):

- Locally generated by sections.
- Finite Type.
- Finite Presented.
- Coherent.
- Quasi-coherent.
- Locally free.

Proof: Cf.[Sta]01CL.

4 Sheaf of Differentials

Prop.(5.2.4.1). If \(\mathcal{C}\) is a site and \(\mathcal{O}_1 \to \mathcal{O}_2\) is a homomorphism of sheaves of rings and \(\mathcal{F}\) is a sheaf of \(\mathcal{O}_2\)-modules, then an \(\mathcal{O}_1\)-derivation from \(\mathcal{O}_2\) to \(\mathcal{F}\) is a map that for any \(U \in \mathcal{C}\), the map \(\mathcal{O}_2(U) \to \mathcal{F}(U)\) is a \(\mathcal{O}_1(U)\)-derivation (4.4.3.1).

Prop.(5.2.4.2)[Sheaf of Differentials]. Let \(\mathcal{C}\) be a site and \(\mathcal{O}_1 \to \mathcal{O}_2\) is a homomorphism of sheaves of rings and \(\mathcal{F}\) is a sheaf of \(\mathcal{O}_2\)-modules, then the functor \(\text{Mod}(\mathcal{O}_2) \to \text{Ab}: \mathcal{F} \to \text{Der}_{\mathcal{O}_1}(\mathcal{O}_2, \mathcal{F})\) is representable by a sheaf of modules \(\Omega_{\mathcal{O}_2/\mathcal{O}_1}\), called the sheaf of differentials, and the map \(d: \mathcal{O}_2 \to \Omega_{\mathcal{O}_2/\mathcal{O}_1}\) is called the universal derivation.
Prop. (5.2.4.3)[Localness of Sheaf of Differentials]. If \( \mathcal{O}_1 \to \mathcal{O}_2 \) is a homomorphism of presheaves of rings, then \( \Omega_{\mathcal{O}_2/\mathcal{O}_1} \) is the sheafification of the presheaf \( U \mapsto \Omega_{\mathcal{O}_2(U)/\mathcal{O}_1(U)} \).

Proof: This is because the construction of \( \Omega_{\mathcal{O}_2/\mathcal{O}_1} \) for all \( U \) gives an exact sequence of presheaves, and the sheafification of which is just the construction in (5.2.4.2), so we are done because sheafification is exact (5.1.2.7).

Prop. (5.2.4.4)[Change of Sites]. Let \( f : \text{Sh}(\mathcal{D}) \to \text{Sh}(\mathcal{C}) \) be a morphism of topoi and \( \varphi : \mathcal{O}_1 \to \mathcal{O}_2 \) a homomorphism of rings on \( \mathcal{C} \), then there is a canonical isomorphism \( f^{-1}\Omega_{\mathcal{O}_2/\mathcal{O}_1} \cong \Omega_{f^{-1}\mathcal{O}_2/f^{-1}\mathcal{O}_1} \) compatible with the universal derivations.

Proof: This follows from the construction (5.2.4.2) and the fact \( f^{-1} \) is exact (5.2.4.2).

Prop. (5.2.4.5)[Functoriality of \( \Omega \)]. Let \( \varphi : (\mathcal{O}_1 \to \mathcal{O}_2) \to (\mathcal{O}'_1 \to \mathcal{O}'_2) \) be a commutative diagram of sheaves of rings over a site \( \mathcal{C} \), then the map \( \mathcal{O}'_1 \to \mathcal{O}'_2 \) composed with the derivative \( \mathcal{O}'_2 \to \Omega_{\mathcal{O}'_2/\mathcal{O}'_1} \) is a \( \mathcal{O}'_1 \)-derivative, thus we obtain a map of \( \mathcal{O}_2 \)-modules \( \Omega_{\mathcal{O}_2/\mathcal{O}_1} \to \Omega_{\mathcal{O}'_2/\mathcal{O}'_1} \), or equivalently a map of \( \mathcal{O}'_2 \)-modules \( \Omega_{\mathcal{O}_2/\mathcal{O}_1} \otimes_{\mathcal{O}_2} \mathcal{O}'_2 \to \Omega_{\mathcal{O}'_2/\mathcal{O}'_1} \). Thus \( \Omega_{-/-} \) is a functor of arrows.

Moreover, if \( \mathcal{O}'_2 = \mathcal{O}_2 \otimes_{\mathcal{O}_1} \mathcal{O}'_1 \), then this map is an isomorphism, by (5.2.4.3) and (4.4.3.6).

Prop. (5.2.4.6). Let \( \mathcal{O}_1 \to \mathcal{O}_2 \to \mathcal{O}'_2 \) be a map of sheaves of rings that \( \mathcal{O}_2 \to \mathcal{O}'_2 \) is surjective with kernel \( \mathcal{I} \subset \mathcal{O}_2 \), then there is a canonical exact sequence of \( \mathcal{O}'_2 \)-modules

\[
\mathcal{I}/\mathcal{I}^2 \to \Omega_{\mathcal{O}_2/\mathcal{O}_1} \otimes_{\mathcal{O}_2} \mathcal{O}'_2 \to \Omega_{\mathcal{O}'_2/\mathcal{O}_1} \to 0,
\]

where the first map is characterized by mapping local sections \( f \) of \( \mathcal{I} \) to \( df \otimes 1 \).

Proof: The first map is well-defined if \( d(\mathcal{I}^2) = 0 \). To show the exactness, let \( \mathcal{O}_2'' \subset \mathcal{O}_2 \) be the presheaf of \( \mathcal{O}_1 \)-algebras that \( \mathcal{O}_2''(U) \) the image of \( \mathcal{O}_2(U) \to \mathcal{O}_2''(U) \). Then there is an exact sequence

\[
\mathcal{I}(U)/\mathcal{I}(U)^2 \to \Omega_{\mathcal{O}_2(U)/\mathcal{O}_1(U)} \otimes_{\mathcal{O}_2(U)} \mathcal{O}_2''(U) \to \Omega_{\mathcal{O}'_2''(U)/\mathcal{O}_1(U)} \to 0
\]

by (4.4.3.8). Now sheafification of these presheaves gives use the desired result by (5.2.4.3).

Def. (5.2.4.7)[Sheaf of Differentials]. Let \( (X, \mathcal{O}_X) \to (S, \mathcal{O}_S) \) be a morphism of ringed sites,

- Let \( \mathcal{F} \) be an \( \mathcal{O}_X \)-module, an \( S \)-derivation from \( \mathcal{O}_X \) to \( \mathcal{F} \) is a derivation over \( f^{-1}\mathcal{O}_S \). The set of \( S \)-derivations is denoted by \( \text{Ders}_S(\mathcal{O}_X, \mathcal{F}) \).
- the sheaf of differentials \( \Omega_{X/S} \) is defined to be a sheaf of modules \( \Omega_{\mathcal{O}_X/f^{-1}\mathcal{O}_S} \) (5.2.4.2), with a universal derivation \( d_X/S : \mathcal{O}_X \to \Omega_{X/S} \).
5 Locally Free sheaves

Prop.(5.2.5.1). Pullbacks of (finite)locally free sheaves are (finite)locally free. Sub-$\mathcal{O}_X$-modules of a (finite)locally free sheaf is (finite)locally free, by (2.2.4.21).

Prop.(5.2.5.2) [Finite Locally Free Sheaves and $\mathcal{H}om$]. For any finite locally free sheaf $\mathcal{E}$ on a ringed site $(\mathcal{C}, \mathcal{O})$:
- $\mathcal{E}^\vee \cong \mathcal{E}$.
- $\mathcal{H}om_{\mathcal{O}}(\mathcal{E}, \mathcal{F}) \cong \mathcal{E}^\vee \otimes_{\mathcal{O}} \mathcal{F}$.
- $\mathcal{H}om_{\mathcal{O}}(\mathcal{F}, \mathcal{G}) \otimes_{\mathcal{H}} \mathcal{H} \cong \mathcal{H}om_{\mathcal{O}}(\mathcal{F}, \mathcal{G} \otimes_{\mathcal{O}} \mathcal{H})$ if $\mathcal{F}$ or $\mathcal{H}$ is finite locally free.
- $\mathcal{H}om_{\mathcal{O}}(\mathcal{E} \otimes \mathcal{F}, \mathcal{G}) \cong \mathcal{H}om_{\mathcal{O}}(\mathcal{E}^\vee \otimes \mathcal{G})$, by the first and (5.2.3.3).

Proof: We define the map, and verify locally, which is by 1. □

Prop.(5.2.5.3). $\mathcal{H}om(\mathcal{H}, -)$ is exact for any locally free sheaf $\mathcal{H}$.

Invertible Sheaves

Def.(5.2.5.4) [Invertible Sheaf]. An invertible sheaf $\mathcal{L}$ on a ringed topoi $(\mathcal{Sh}(\mathcal{C}), \mathcal{O})$ is an invertible object in the symmetric monoidal category $\text{Mod}_{\mathcal{O}}$(3.1.4.24).

Prop.(5.2.5.5). Let $(\mathcal{C}, \mathcal{O})$ be a ringed site and $\mathcal{L}$ an $\mathcal{O}$-module, the following are equivalent:
- $\mathcal{L}$ is an invertible sheaf.
- there exists some $\mathcal{O}$-module $\mathcal{N}$ that $\mathcal{L} \otimes_{\mathcal{O}} \mathcal{N} \cong \mathcal{O}$.

And in this case, $\mathcal{L}$ is flat and of finite presentation, and $\mathcal{N} \cong \mathcal{H}om_{\mathcal{O}}(\mathcal{L}, \mathcal{O})$.

Proof: $\mathcal{L}$ is flat because tensoring $\mathcal{L}$ is an equivalence thus exact. Let $\psi : \mathcal{L} \otimes_{\mathcal{O}} \mathcal{N} \cong \mathcal{O}$ the isomorphism, $U$ an element of $\mathcal{C}$, then by construction of $\otimes$, after localization, we may assume there exists sections $x_i \in \mathcal{L}(U), y_i \in \mathcal{N}(U)$ that $\psi(x_i \otimes y_i) = 1$. Then there is an automorphism of $\mathcal{L}|_U : x \mapsto \sum \psi(x \otimes y_i)x_i$. This automorphism factors through $\mathcal{L}|_U \to \mathcal{O}^\oplus_{\mathcal{U}} \to \mathcal{L}|_U$,

thus $\mathcal{L}|_U$ is a direct summand of a finite free $\mathcal{O}_U$-module, thus $\mathcal{L}$ is of finite presentation.

Assume $\mathcal{L}$ is invertible, consider the evaluation map $\mathcal{L} \otimes_{\mathcal{O}} \mathcal{H}om(\mathcal{L}, \mathcal{O}) \to \mathcal{O}$,

and by (5.2.3.3),

$$\text{Hom}(\mathcal{O}, \mathcal{O}) = \mathcal{H}om_{\mathcal{O}}(\mathcal{L} \otimes \mathcal{N}, \mathcal{O}) \to \mathcal{H}om_{\mathcal{O}}(\mathcal{N}, \mathcal{H}om_{\mathcal{O}}(\mathcal{L}, \mathcal{O})).$$

The image of 1 gives a morphism $\mathcal{N} \to \mathcal{H}om_{\mathcal{O}}(\mathcal{L}, \mathcal{O})$. Tensoring $\mathcal{L}$ gives the inverse of the evaluation map. □

Cor.(5.2.5.6). The pullback of an invertible sheaf is an invertible sheaf, because tensoring commutes with pullbacks (5.2.2.12).

Def.(5.2.5.7) [Picard Groups]. For any ringed site $(\mathcal{C}, \mathcal{O})$, there is a set of invertible modules over $\mathcal{C}$ that any invertible module is isomorphic to exactly one of them. Then this set forms an Abelian group, called the Picard group $\text{Pic}(\mathcal{O})$. 

For more details on the Picard group, please refer to the corresponding section in the text.
Prop. (5.2.5.8) [Invertible Sheaves and Locally Free Sheaves of Rank 1]. If \((X, \mathcal{O}_X)\) is a ringed space, then any locally free \(\mathcal{O}_X\)-module of rank 1 is invertible. And when \((X, \mathcal{O}_X)\) is a local ringed space, the converse holds as well.

Proof: Assume \(\mathcal{L}\) is locally free of rank 1 and consider the evaluation map (5.2.3.1)

\[
\mathcal{L} \otimes \mathcal{O} \to \mathcal{L}.
\]

This map is an isomorphism when restricting to any trivializing covering of \(\mathcal{L}\), so it is an isomorphism. Thus \(\mathcal{L}\) is invertible by (5.2.5.5).

Assume \((\text{Sh}(\mathcal{C}), \mathcal{O})\) is a local ringed topoi and \(\mathcal{L}\) is invertible, the proof of (5.2.5.5) shows there exists a covering \(\{U_i \to U\}\) that \(\mathcal{L}|_{U_i}\) is a direct summand of a finite free \(\mathcal{O}_{U_i}\)-module. Replacing \(U_i\) by \(U\), let \(\pi\) be the projection of \(\mathcal{O}_U^\ast\) onto \(\mathcal{L}|_U\) which corresponds to a matrix with entries in \(\mathcal{O}(U)\). The image of \(\pi\) acting on \(\mathcal{O}(U)^\ast\) is a finite free \(\mathcal{O}(U)\)-module \(M\), thus there are \(f_1, \ldots, f_t\) generating unit ideal of \(\mathcal{O}(U)\) such that \(M_{f_i}\) is finite free. Now by definition of local ringed topoi (5.2.1.6), after replacing \(U\) by a covering, we may assume \(M\) is finite free, which means \(\mathcal{L}|_U\) is free summand of \(\mathcal{O}_U^\ast\). But \(\mathcal{L}\) is invertible, thus rank of \(\mathcal{L}\) is 1. \(\square\)

Prop. (5.2.5.9). Let \(X\) be a locally ringed space and \(\mathcal{L} \in \text{Pic}(X)\) that is generated by global sections \(s_0, \ldots, s_n\). If \(\mathcal{F}\) is the kernel of the map \(\mathcal{O}_X^\oplus n+1 \to \mathcal{L}\), then \(\mathcal{F} \otimes \mathcal{L}\) is globally generated.

Proof: \(\mathcal{F}\) is finite locally free of rank \(n\) by (5.2.5.1). The elements

\[
s_{ij} = (0, \ldots, 0, s_j, 0, \ldots, 0, s_i, \ldots, 0) \in \Gamma(X, \mathcal{L}^\oplus n+1)
\]

is in \(\Gamma(X, \mathcal{F} \otimes \mathcal{L})\), and it can be verified locally s.t. they generate \(\mathcal{F} \otimes \mathcal{L}\). \(\square\)

6 Sheaves on Spaces

Sheaves on Topological Spaces

Remark (5.2.6.1). A topological space can be regarded as a ringed space by assigning the locally constant sheaf \(\mathbb{Z}\) as the structure sheaf.

Def. (5.2.6.2) [Grothendieck’s Six Operators]. Let \(f: X \to Y\) be a continuous map of topological spaces, then the inverse image defines a continuous map between sites \(Y_{\text{Zar}} \to X_{\text{Zar}}\), so by (5.1.2.9) and (5.1.2.11) we can define

- the pushforward \(f^p \mathcal{F}, f^p \mathcal{F}(U) = \mathcal{F}(f^{-1}(U))\) sends presheaf to presheaf.
- the direct image \(f_* \mathcal{F}, f_* \mathcal{F}(U) = \mathcal{F}(f^{-1}(U))\) sends sheaf to sheaf.
- the inverse image \(f_p \mathcal{G}, f_p \mathcal{G}(U) = \lim_{\substack{\to \mathcal{G}(V) \to \mathcal{G}(V)}} f(U) \cap V\) that sends presheaf to presheaf.
- the inverse image \(f^{-1} \mathcal{G} = f_*(\mathcal{G})\) that sends sheaf to sheaf.
- For a morphism of locally compact spaces, we can define a proper direct image:

\[
f_t(\mathcal{F})(U) = \{ s \in \Gamma(f^{-1}(U), \mathcal{F}) | \text{Supp}(s) \to U \text{ proper} \}
\]

This is a subsheaf of \(f_* \mathcal{F}\) and it is left exact. we denote \(\Gamma_c(X, \mathcal{F})\) as the group \(f_t(\mathcal{F})\) where \(f: X \to \text{pt}\). And the stalk \(f_t(\mathcal{F})_y = \Gamma_c(f^{-1}(y), \mathcal{F}|_{f^{-1}(y)})\) Cf. [Gelfand P224 P225].
5.2. RINGED TOPOI, RINGED SITES, RINGED G-SPACES AND SCHEMES

- the **proper inverse image** (special case) $i^!$ for a closed immersion $Z \subset X$ defined by

$$i^!(\mathcal{F})(U = V \cap Z) = \{ s \in \Gamma(V, \mathcal{F}) | \text{Supp}(s) \in Z \}.$$ 

sends Abelian sheaves to Abelian sheaves.

- the internal tensor product.

- the internal Hom.

**Proof:** Check that $f_!$ is a sheaf: it is separated clearly, it suffices to show that for a covering $\cup U_i = W$ and $\xi_i \in F(f^{-1}(U_i))$, the section $\xi \in F(f^{-1}(W))$ they generated by sheaf property of $F$ is in $f_! F(W)$. For a compact subset $K$, there is a finite cover $\cup_i U_i$ of it, thus $K - \cup_{i \neq j} U_j$ is compact in $U_j$, thus its inverse image is compact in $\text{Supp}(\xi)$. there are f.m. $U_j$, thus the inverse image of $K$ is compact in $\text{Supp}(\xi)$. □

**Def. (5.2.6.3) [Stalks].** The convenience of rings spaces compared to the case of sites is the it has stalk functors: For any presheaf $\mathcal{F}$ on $X$ and a point $i : x \to X$, define the **stalk** $\mathcal{F}_x = i_p(\mathcal{F})$ (5.2.6.2).

**Prop. (5.2.6.4) [Stalks Commutes with Shifification].** Taking stalks commutes with shifification.

**Proof:** Cf. [Sta]007Z. □

**Prop. (5.2.6.5).** If a sheaf on a ringed space has only one non-vanishing stalk, then it is a skyscraper sheaf. (Because the restriction map to that point for every open set is an isomorphism).

**Prop. (5.2.6.6) [Stalks].** Taking stalks is a left adjoint to the skyscraper sheaf from Presheaves to Sets, thus it preserves cokernel. Moreover, for a map of sheaves $\mathcal{F} \to \mathcal{G}$ on $X$,

- $\varphi$ is a monomorphism iff $\varphi_x$ is injective for all $x \in X$.
- $\varphi$ is an epimorphism iff $\varphi_x$ is surjective for all $x \in X$.
- $\varphi$ is an isomorphism iff $\varphi_x$ is surjective for all $x \in X$.

**Proof:** 1: If $\varphi$ is a monomorphism, then $\varphi_x$ is clearly. Conversely, if $\varphi_x$ are all injective, if $s \in \mathcal{F}(U)$ mapsto 0 $\in (U)$, then $s_x$ mapsto 0 $\in \mathcal{G}_x$ for all $x$, thus $s_x = 0$ for all $x$, thus $s = 0$.

2: If $\varphi$ is an epimorphism, then $\varphi_x$ is surjective by definition. The converse is also true.

3: If $\varphi_x$ is isomorphism for all $x$, then $\varphi$ is monomorphism by 1, and for any $t \in \mathcal{G}(U)$, $t$ is locally coming from some section of $s$, and these sections are compatible on their intersections because of monomorphism, so they glue together to a section $s \in \mathcal{F}(U)$ that $\varphi(U)(s) = t$. □

**Prop. (5.2.6.7) [Topological Spaces and Sites].** Let $f : X \to Y$ be a continuous map of topological spaces, then $f$ induces a map of sites $X \to Y$ because $f^{-1}$ is exact (5.1.2.14), thus induces a map of topoi $f : \text{Sh}(X) \to \text{Sh}(Y)$ (5.1.2.19).

**Cor. (5.2.6.8).** Let $f : X \to Y$ be a continuous map of topological spaces,

- Let $\mathcal{G}$ be a presheaf on $Y$, then there is a canonical bijection of stalks $(f_p(\mathcal{G}))_x = \mathcal{G}_{f(x)}$. If $\mathcal{G}$ is a sheaf on $Y$, then there is a canonical bijection of stalks $(f^{-1}(\mathcal{G}))_x = \mathcal{G}_{f(x)}$.
- $f^{-1}$ is left adjoint to $f_!$.
- $f_!$ is left exact when $X, Y$ are locally compact. And $j_!$ is left adjoint to the functor $j^{-1}$ for an inclusion of open subset $j : U \subset X$. 


• $i^!$ is right adjoint to $i_*$ for a closed immersion $i : Z \to X$, in particular $i_*$ is exact when $i$ is a closed immersion.

Proof: 1: This is because $(-)_p$ commutes with composition (5.2.6.3), and also shifification commutes with $(-)_p$ (5.2.6.4).
2: This is immediate.
3: 4: The adjointness follows from the fact that any section under a homomorphism $i_* \mathcal{G} \to \mathcal{F}$ has support contained in $Z$.

Prop. (5.2.6.9). Let $i : Z \to X$ be a closed immersion, then the functor $i_* : \text{Ab}(Z) \to \text{Ab}(X)$ is exact, fully faithful, with the essential image those sheaves with support in $Z$.

Prop. (5.2.6.10) [Canonical Exact Sequences]. We have a canonical exact sequences of sheaves of modules:

$$0 \to j_!(\mathcal{F}|_U) \to \mathcal{F} \to i_*(\mathcal{F}|_Z) \to 0$$

$$0 \to i_* i^! Y \mathcal{F} \to \mathcal{F} \to j_* (\mathcal{F}|_U) \to 0$$

(check on stalks), which is important to use reduction to calculate sheaf cohomology. The latter induces long exact sequences:

$$0 \to H^0_Y(X, \mathcal{F}) \to H^0(X, \mathcal{F}) \to H^0(U, \mathcal{F}|_U) \to H^1_Y(X, \mathcal{F}) \to \cdots$$

Proof: Cf. [Sta]02UT. □

Prop. (5.2.6.11). On a topological space $X$, for a qc open subset $U$, $(\oplus F_i)(U) = \oplus F_i(U)$. This uses the compactness of $U$.

Morphisms of Local Ringed Spaces

Def. (5.2.6.12) [Open Immersion of Ringed Spaces]. A morphism $f : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ of ringed spaces is called an open immersion if $f$ is a homeomorphism of $X$ onto an open subset of $Y$, and the map $f^\sharp : f^{-1}(\mathcal{O}_Y) \to \mathcal{O}_X$ is an isomorphism.

Prop. (5.2.6.13). Let $(X, \mathcal{O}_X)$ be a ringed space, $U \subset X$ an open subset, and $\mathcal{O}_U = \mathcal{O}_X|_U$ is a sheaf of rings on $U$, then $(U, \mathcal{O}_U) \to (X, \mathcal{O}_X)$ is an open immersion, and $(U, \mathcal{O}_U)$ is called the open subspace associated to $U$.

Prop. (5.2.6.14) [Universal Property of Open Immersions]. Let $f : (X, \mathcal{O}_X) \to (Y, \mathcal{O}_Y)$ be an open immersion of ringed spaces, then it has the universal property that any morphism of ringed spaces $(T, \mathcal{O}_T) \to (Y, \mathcal{O}_Y)$ that factors set-theoretically through $f(X)$ factors uniquely through $(X, \mathcal{O}_X)$.

Def. (5.2.6.15) [Closed Immersion]. Let $i : Z \to X$ be a morphism of local ringed spaces, then $i$ is called a closed immersion if:

• $i$ is a homeomorphism of $Z$ onto a closed subspace of $X$.

• the map $\mathcal{O}_X \to i_* \mathcal{O}_Z$ corresponding to $f^\sharp$ is surjective with kernel $\mathcal{I}$.

• the $\mathcal{O}_X$-module $\mathcal{I}$ is locally generated by sections.

And for a closed immersion, $\mathcal{I}$ is called the ideal sheaf of $i$. 
Def. (5.2.6.16) [Closed Immersion Defined by Ideals]. Let \((X, \mathcal{O}_X)\) be a local ringed space, and \(\mathcal{I} \subset \mathcal{O}_X\) a sheaf of ideals on \(X\) locally generated by sections. Let \(Z\) be the support of the sheaf of rings \(\mathcal{O}_X/\mathcal{I}\). \(Z\) is closed in \(X\) because it is the support of \(1\). By (5.2.6.9), there is a unique sheaf of rings \(\mathcal{O}_Z\) on \(Z\) that \(i^* \mathcal{O}_Z = \mathcal{O}_X/\mathcal{I}\). For any \(z \in Z\), the stalk \(\mathcal{O}_z = \mathcal{O}_{X,z}/\mathcal{I}_z\) is a quotient of a local ring and is non-zero, thus a local ring. Then \((Z, \mathcal{O}_Z)\) is a local ringed space and \(i : (Z, \mathcal{O}_Z) \to (X, \mathcal{O}_X)\) is a closed immersion, called the closed immersion defined \(\mathcal{I}\).

Prop. (5.2.6.17) [Closed Immersions are Equivalent to Ideals]. Let \(f : X \to Y\) be a closed immersion of local ringed spaces with ideal sheaf \(\mathcal{I}\). Let \(i : Z \to X\) be the closed immersion defined by \(\mathcal{I}\), then \(f\) is isomorphic to \(i\).

Proof: Because \(f_* \mathcal{O}_Z \cong \mathcal{O}_X/\mathcal{I}\) on \(X\). □

Prop. (5.2.6.18). For a closed immersion of ringed spaces \(f, f_*\) on \(\mathcal{O}_X\)-mod is fully faithful, with image those modules annihilated by \(\mathcal{I}\), where \(\mathcal{I}\) is the structural kernel.

Proof: Cf. [Sta]08KS. □

7 Spec and Schemes

Def. (5.2.7.1) [Spectrum]. Given a commutative ring \(A\), the spectrum of \(A\) \(\text{Spec} A\) is a locally ringed space whose underlying space is the set of primes of \(A\), and the topology is generated by the standard open subsets \(D(f) = \{p \mid f \not\in p\}\).

To define the structure sheaf \(\mathcal{O}_X\), we first define a sheaf on the site of standard open subsets, which takes value \(R_f\) on \(D(f)\). This is truly a sheaf by (4.4.2.3), and then we can use (5.1.2.24) to extend this sheaf to a sheaf on \(\text{Spec} A\), called the structure sheaf \(\mathcal{O}_X\).

A locally ringed space of the form \(\text{Spec} A\) is called an affine scheme. The category of affine schemes is denoted by \(\text{Aff}\).

Def. (5.2.7.2) [Schemes]. The category \(\text{Sch}\) of schemes is a fully faithful category of the category of local ringed spaces (5.2.1.10) consisting of local ringed spaces that are locally isomorphic to \(\text{Spec} A\).

Lemma (5.2.7.3). If \(X\) is a local ringed space, \(x \in X\), and \(Y = \text{Spec} A\) an affine scheme, \(f : X \to Y\) is a morphism, consider the ring map \(\Gamma(X, \mathcal{O}_X) \xrightarrow{f^*} \Gamma(Y, \mathcal{O}_Y) \to \mathcal{O}_{X,x}\), and consider the inverse image \(p\) of \(m_x\), which corresponds to \(y \in Y\), then \(f(x) = y\).

Proof: There are commutative diagrams

\[
\begin{align*}
\Gamma(Y, \mathcal{O}_Y) & \xrightarrow{f^*} \Gamma(Y, \mathcal{O}_Y) \\
\Gamma(X, \mathcal{O}_X) & \xrightarrow{f} \mathcal{O}_{X,x}
\end{align*}
\]

and the map of local rings is a local ring map. So the inverse image of \(m_x\) is just \(m_{f(x)}\), so \(m_{f(x)} = m_y\). □

Prop. (5.2.7.4). Let \(X\) be a local ringed spaces and \(Y = \text{Spec} A\) an affine scheme, then the map \(\text{Hom}(X, \text{Spec} A) \to \text{Hom}(A, \Gamma(X, \mathcal{O}_X))\) is an isomorphism.
The inverse map is constructed as follows: for any \( \varphi : A \to \Gamma(X, \mathcal{O}_X) \) and \( x \in X \), define \( \Phi(x) \) to be the point corresponding to the inverse image of \( m_x \) in \( A \to \Gamma(X, \mathcal{O}_X) \to \mathcal{O}_{X,x} \). In this way, \( \Phi^{-1}(D(f)) \) is just \( D(\varphi(f)) \subset X \) which is open, thus \( \Phi \) is continuous. Now we want to construct a sheaf homomorphism \( f^{-1}(\mathcal{O}_Y) \to \mathcal{O}_X \), and it suffices to construct compatible maps on the affine open basis \( D(f) \), by (5.1.3.17). Now \( \Gamma(D(f), \mathcal{O}_Y) = A_f \), and because \( f \) is invertible on \( D(\varphi(f)) \), there is by universal property a unique map \( A_f \to D(\varphi(f)) \) extending \( \varphi \). Then by universal property these maps are compatible. Notice the construction here also shows the homomorphism is determined by the map set-theoretically.

Finally, we need to show this induces a local ring map on the stalks, and this is quite obvious from the definition.

Then we show these two maps are inverse to each other: It suffices to show any ring map \( A \to \Gamma(X, \mathcal{O}_X) \) comes uniquely from a map \( X \to Y \): the uniqueness is proven by (5.2.7.3), and the sheaf homomorphism is determined by the set-theoretical map by the above argument.

Cor. (5.2.7.5). The \( \text{Spec} \) operator \( \text{Spec} : \text{CAlg}^{op} \to \text{Sch} \) is right adjoint to \( X \to \Gamma(X, \mathcal{O}_X) \):

\[
\text{Hom}_{\text{Sch}}(X, \text{Spec}(A)) \cong \text{Hom}_{\text{CAlg}}(A, \Gamma(X, \mathcal{O}_X)).
\]

Notice the category of schemes is a full subcategory of the category of locally ringed spaces.

Cor. (5.2.7.6). \( \text{Aff} \) is equivalent to \( \text{CAlg}^{op} \).

Prop. (5.2.7.7). Let \( X \) be a scheme and \( R \) a local ring, then there is a natural bijection between morphisms \( \text{Spec} R \to X \) and pairs \( (p, \varphi) \) where \( p \in X \) is a point and \( \varphi : \mathcal{O}_{X,x} \to R \) is a local ring map.

\[
\begin{array}{c}
\mathcal{O}_{Y,y} \rightarrow Y \\
\downarrow \\
\mathcal{O}_{X,x} \rightarrow X
\end{array}
\]

Prop. (5.2.7.10). The closure of a subset \( T \) of \( \text{Spec}(A) \) is \( V(\cap p, p \in T) \).

Prop. (5.2.7.11). The underlying space of a scheme is sober.

\[
\begin{array}{c}
\mathcal{O}_{Y,y} \rightarrow Y \\
\downarrow \\
\mathcal{O}_{X,x} \rightarrow X
\end{array}
\]
Construction of Schemes

**Prop.(5.2.7.12) [Global Spec].** There is an $S$-scheme $f : \text{Spec}_S A \to S$ for every Qco sheaf of $\mathcal{O}_S$-algebras $A$ on $S$ that for any affine open subscheme $U \subset X$, $f^{-1}(U) \cong \text{Spec} \mathcal{A}(U)$ over $U$. This construction is right adjoint to the direct image map:

$$\text{Hom}_{\text{Alg}_{S}}(A, \pi_+ \mathcal{O}_X) \cong \text{Hom}_{\text{Sch}/S}(X, \text{Spec}_S A).$$

and defines an equivalence of affine morphisms over $S$ and Qco $\mathcal{O}_S$-algebras. Moreover, this defines an equivalence of the category of $A$-modules and the category of $\mathcal{O}_{\text{Spec}_A}$-modules.

**Proof:** Choose an affine open covering $\{U_i \to X\}$ of $X$, and consider the schemes $\text{Spec} \mathcal{A}(U_i) \to U_i$ over $U_i$, then their restrictions to $U_{ij}$ are compatible, because this is true after further restriction to an affine open covering of $U_{ij}$, we can use(5.1.5.4). Then we can use(5.1.5.4) to get an $S$-scheme $f : \text{Spec}_S A \to S$ that $f^{-1}(U_i) \cong \text{Spec} \mathcal{A}(U_i)$.

Now we check that for any affine open subset $U \subset X$, $f^{-1}(U) \cong \text{Spec} \mathcal{A}(U)$ over $U$. But this is true after base change to $U \cap U$ for any $i$, so it is true, by(5.1.5.4).

To show the adjointness condition, by(5.1.5.4), it suffices to show canonical(thus compatible) isomorphism for $S$ affine. In this case, this reduces to(5.2.7.5).

**Cor.(5.2.7.13).** Let $S$ be a scheme and $A$ is a Qco sheaf of $\mathcal{O}_S$-algebras, then

- For any morphism $g : S' \to S$, $S' \times_S \text{Spec}_S(A) \cong \text{Spec}_{S'}(g^*A)$.
- The natural map $A \to \pi_+ \mathcal{O}_{\text{Spec}_S(A)}$ is an isomorphism of $\mathcal{O}_S$-algebras.

**Proof:** 1: It can be checked that $S' \times_S \text{Spec}_S(A)$ and $\text{Spec}_{S'}(g^*A)$ satisfy the same universal property.

2: It suffices to check on affine opens, then it is trivial.

**Lemma (5.2.7.14) [Affine Case].** Fiber product of affine schemes is also affine that corresponds to the tensor product of their corresponding rings, by(5.2.7.5).

**Prop.(5.2.7.15) [Finite Limits of Schemes].** Fiber products exist in the category of schemes, and there is a final object Spec $\mathbb{Z}$, so arbitrary limits exist in the category of schemes(3.1.1.47).

In fact, finite limits exists in the category of ringed spaces, and finite limits of schemes coincide with finite limits as ringed spaces.

**Proof:** Let $f : X \to S, g : Y \to S$, and $U_i$ is an affine open covering of $S$, $V_i,j$ is an affine open covering of $f^{-1}(U_i)$ and $W_{ik}$ is an affine open covering of $g^{-1}(U_i)$, then we can check $h_{V_i,j} \times h_{U_i} h_{W_{ik}}$ is a covering of $h_X \times h_Y$ by representable open subfunctors(7.7.1.13), by(5.2.7.14), thus it is representable.

**Cor.(5.2.7.16) [Open Subschemes].** Let $X \to S, Y \to S$, and $V \subset X, W \subset Y$ be open subschemes mapping into open subscheme $U \subset S$, then there is a natural open immersion $V \times_U W \to X \times_S Y$ with image $\pi_1^{-1}V \cap \pi_2^{-1}(W)$.

**Proof:** There is a natural map $V \times_U W \to X \times_S Y$ by Yoneda lemma, and this map has the universal property that any map $f : (T, \mathcal{O}_T) \to X \times_S Y$ that $\pi_1 \circ f$ has image in $V$ and $\pi_2 \circ f$ has image in $W$ factors uniquely through $V \times_U W$. But so does the open immersion $\pi_1^{-1}V \cap \pi_2^{-1}(W) \to X \times_S Y(5.2.6.14)$, so they are equal. □
Cor. (5.2.7.17). Let $f : X \to S, g : Y \to S$, and $U_i$ is an affine open covering of $S$, $V_{ij}$ is an affine open covering of $f^{-1}(U_i)$ and $W_{ik}$ is an affine open covering of $g^{-1}(U_i)$, then

$$X \times_S Y = \bigcup_i \bigcup_{j,k} V_{ij} \times_{U_i} W_{ik}$$

is an affine open covering of $X \times_S Y$.

Also, the structure sheaf of $X \otimes_S Y$ is given by $\mathcal{O}_{X \times_S Y} = \pi_1^{-1}\mathcal{O}_X \otimes_{\mathcal{O}_S} \pi_2^{-1}\mathcal{O}_Y$.

Cor. (5.2.7.18). The equalizer of two morphisms from $X$ to $Y$ exists, it is a locally closed subscheme of $X$, and it is a closed subscheme of $X$ if $Y$ is separated.

Proof: because it is the base change of $\Delta : Y \to Y \times_S Y$ (3.1.1.47), then use (5.4.4.76). □

Remark (5.2.7.19) [Infinite Product of Schemes Doesn’t Exists]. WARNING: infinite products of schemes may not exists, Cf. [Sta]0CNH. Intuitively, if you want to glue affine products together, you will notice you can identify only those products that is equal a.e..

Remark (5.2.7.20). Let $X$ be a scheme over $S$ and $S' \to S$ is a morphism of schemes, then we sometimes denote $X \times_S S'$ by $X_{S'}$, if no confusion is caused.

Def. (5.2.7.21) [Generic Fibers and Special Fibers]. If $X$ is a scheme over an integral ring $A$, then the generic fiber of $X/A$ is the stalk $X_\eta$, where $\eta = (0) \in \text{Spec } A$.

If $X$ is a scheme over a ring $R$, a special fiber is the stalk of $X$ over a maximal ring $m$.

8 Rational Maps

Def. (5.2.8.1) [Rational Maps]. Let $X, Y \in \text{Sch}/S$ and $Y/S$ separated, a rational map over $S$ $f : X \to Y$ is an equivalence class of maps $U \to Y$ over $S$ where $U$ is an open dense subset of $X$. A rational function on $X$ is a rational map $X \to \mathbb{A}^1$. It has a ring structure. The ring of rational functions is denoted by $R(X)$.

Because two rational maps are equivalent iff they are compatible on the intersection of their domain as $Y/S$ is separated, a rational map $\varphi : X \to Y$ has a maximal domain of definition, denoted by $\text{dom}(\varphi)$.

Prop. (5.2.8.2). If $X$ is a scheme with f.m. generic points $\eta_i$, then

$$R(X) = \prod \mathcal{O}_{X, \eta_i}.$$  

Proof: Cf. [Sta]01RV. □

Def. (5.2.8.3) [Birational Maps]. $X, Y \in \text{Sch}/S$ are called birational over $S$ if they are isomorphic in the category of $S$-schemes with dominant rational maps.

Prop. (5.2.8.4). Two schemes $X, Y$ over $S$ are birational over $S$ iff there are nonempty open subschemes $U \subset X, V \subset Y$ that are isomorphic over $S$.

Proof: □

Def. (5.2.8.5) [$S$-Dense Subsets]. Let $X \in \text{Sch}/S$, a subscheme $U \subset X$ is called $S$-dense if $U_s$ is dense in $X_s$ for any $s \in S$. 


Prop.(5.2.8.6). Let $X \in \text{Sch}^{pf}/S$ and $V \subset X$ is a qc open subscheme, then the set of points $s \in S$ s.t. $V_s \subset X_s$ is not dense is locally constructible in $S$. And if $V$ is $S$-dense in $X$, then it is also schematically dense in $X$.

Proof: Cf.[?]P56. □

Prop.(5.2.8.7). If $X \in \text{Sch}_{qc}/S$ and $U \subset X$ is an $S$-dense open subscheme, then $U$ contains an $S$-dense open subscheme of $S$ that is qc.

Proof: Cf.[?]P56. □

Def.(5.2.8.8)[S-Rational Maps]. Let $X,Y \in \text{Sch}_{\text{sep},\text{loc}}^{\text{sep},\text{loc},\text{pf}}/S$ an $S$-rational map $f : X \to Y$ is an equivalence class of maps $U \to Y$ over $S$ where $U$ is an open subset of $X$ that is $S$-dense.

Because two rational maps are equivalent iff they are compatible on the intersection of their domain as $Y/S$ is separated, a rational map $X \to Y$ has a maximal domain of definition.

Def.(5.2.8.9)[S-Birational Maps]. Let $X,Y \in \text{Sch}_{\text{sep},\text{loc}}^{\text{sep},\text{loc},\text{pf}}/S$ are called $S$-birational if they are isomorphic in the category of $S$-schemes with dominant $S$-rational maps.

Prop.(5.2.8.10). The notion of $S$-rational and $S$-birational maps are stable under base change, because a base change of fields is flat locally of f.p. thus open.

Prop.(5.2.8.11)[Faithfully Flat Descent]. Let $X',X,Y \in \text{Sch}_{\text{sep},\text{loc}}^{\text{sep},\text{loc},\text{pf}}/S$ and $\varphi : Y \to S$ an $S$-rational map,

- If $f : X' \to X$ flat, then $\varphi \circ f$ is an $S$-rational map $X' \to Y$, and $\text{dom}(\varphi \circ f) = f^{-1}(\text{dom}(\varphi))$. In particular, if $f$ is f.f. and $\varphi \circ f$ is a morphism, then $\varphi$ is also a morphism.
- If $T \to S$ is flat, then the base change $\varphi_T : X_T \to Y_T$ satisfies $\text{dom}(\varphi_T) = \text{dom}(\varphi) \times_S T$.

Proof: Cf.[BLR90]P58. □

9 Associated Points

Main References are [Sta]Chap30.

Def.(5.2.9.1). For a scheme $X$ and a Qco sheaf $\mathcal{F}$ on $X$, a point is called associated to $\mathcal{F}$ iff $m_x$ is associated to $\mathcal{F}_x$, which is equivalent to $m_x$ are all zero-divisors in $M$ by(4.2.5.18). When $\mathcal{F} = \mathcal{O}_X$, $x$ is called an associated point of $X$.

Prop.(5.2.9.2). If $X$ is locally Noetherian, then an associated prime is equivalent to it is an associated prime of $\Gamma(X,\mathcal{O}_X)$ of $\Gamma(U,\mathcal{F})$ for a nbhd $U$ of $x$.

Proof: Cf.[Sta]02OK. □

Prop.(5.2.9.3). Same results of associated points are parallel to the discussion of associated primes:

- relations of $\text{Ass}(\mathcal{F})$ w.r.t exact sequences(4.2.5.14).
- $\text{Ass}(\mathcal{F}) \subset \text{Supp}(\mathcal{F})(4.2.5.16)$.
- When $X$ is locally Noetherian and $\mathcal{F}$ is coherent, for a quasi-compact open set $U$ of $X$, the number of associated points in $U$ is finite(4.2.5.16).
- When $X$ is locally Noetherian, $\mathcal{F} = 0$ iff $\text{Ass}(\mathcal{F})$ is empty(4.2.5.16).
• When $X$ is locally Noetherian, if $\text{Ass}(\mathcal{F}) \subset$ an open subset $U$, then $\Gamma(X, \mathcal{F}) \to \Gamma(U, \mathcal{F})$ is injective (4.2.5.22).

• If $X$ is locally Noetherian, then the minimal elements (under specialization) of $\text{Supp}(\mathcal{F})$ are associated points of $\mathcal{F}$, in particular, any generic point of an irreducible component of $X$ is an associated points of $X$.

• If $X$ is locally Noetherian, then if a map $\varphi : \mathcal{F} \to \mathcal{G}$ that is injective at all the stalks of $\text{Ass}(\mathcal{F})$, then $\varphi$ is injective.

10 Others

Frobenius

**Def. (5.2.10.1)** [Frobenius]. Let $p \in \mathbb{P}, r \in \mathbb{Z}, q = p^r, k \in \text{Field}, \# k = q, X_0 \in \text{Sch}_k/X, X = X_0 \otimes_k \overline{k},$

- The **absolute Frobenius** for $X$ or $X_0$ is the automorphism $\varphi_{r,X} : X \to X$ that is the $p^r$-th power on $\mathcal{O}_X$.
- $F_X = \text{id}_{X_0} \times_k \varphi_{\overline{k}/k}^{-1}$, called the **arithmetic Frobenius**, which is not $k$-linear!
- $F_{r,X} = \varphi_{X_0} \times_k \text{id}_{\overline{k}} : X \to X$, which is $\overline{k}$-linear, called the **geometric Frobenius**.
- Let $U$ be a $X_0$-scheme, then the **relative Frobenius** $F_{U/X_0,r} : U \to \varphi_{r,X_0}^*(U)$ is defined by the universal property of the base change of $U$ by $\varphi_{X_0}^r$. $F_{U/X_0,1}$ is denoted by $F_{U/X_0}$.

**Prop. (5.2.10.2).** $F_X = \varphi_{r,X} \circ F_X : X \to X$.

*Proof:* Easy. \qed

**Prop. (5.2.10.3).** $F_{U/X_0}$ is a universal homeomorphism. In particular, if $U \to X_0$ is étale, then it is an isomorphism.

*Proof:* Because $U \to X, X \times_{\varphi_{X_0}} U \to X$ are both étale, $F_U/X_0$ is étale. And from the fact both both $\varphi_{X_0}$ and $\varphi_{U_0}$ are universally bijective, we see $F_{U_0/X_0}$ is universally bijective. So it must be an isomorphism? \qed

**Prop. (5.2.10.4).** If $X$ is a scheme over a field $k$ of char $p$, then $X^{(p)}$ is reduced iff $X$ is geometrically reduced. This follows from (5.4.3.2).
5.3 Cohomology on Ringed Sites

Main references are [Sta], [Har77] and [Sheaf Cohomology, Anonymous].

1 Derived Cohomology

Notations(5.3.1.1).
- We use notations defined in Sites, Sheaves and Stacks.

\[ D(\text{Mod}(\mathcal{O})) \]

Def.(5.3.1.2)[Setups]. Let \( (\mathcal{C}, \mathcal{O}) \) be a ringed site, write \( K(\mathcal{O}) = K(\text{Mod}(\mathcal{O})), D(\mathcal{O}) = D(\text{Mod}(\mathcal{O})) \). The Abelian category \( \text{Mod}(\mathcal{O}) \) contains enough injectives by (3.3.2.28) and (3.3.2.24), so we can consider right derived functor for any left exact functor.

1. (Hom) Let \( K \) be a presheaf of sets on \( \mathcal{C} \), then \( \mathcal{F} \mapsto \text{Hom}_{\mathcal{PSh}(\mathcal{C})}(K, \mathcal{F}) \) is a left exact functor \( \text{Mod}(\mathcal{O}) \) to \( \text{Ab} \), thus we denote its derived functors as \( H^i(K, \mathcal{F}) \).

2. (Section) The section functor \( \Gamma(U, \mathcal{F}) \) is the left exact functor \( \text{Mod}(\mathcal{O}) \to \text{Mod}(\mathcal{O}(U)) \) and call the derived functors \( H^i(U, \mathcal{F}) = H^i(R\Gamma(U, \mathcal{F})) \) as the \( i \)-th cohomology of \( \mathcal{F} \) at \( U \). In fact, this functor is just \( \text{Mor}_{\mathcal{PSh}(\mathcal{C})}(h_U, \mathcal{F}) \) defined in (5.3.1.2).

3. (Global Section) Let \( e \) be the final object in \( \mathcal{PSh}(\mathcal{C}) \), then we define the global section functor \( \Gamma(\mathcal{C}, -) \) to be the left exact functor \( \text{Mod}(\mathcal{O}) \to \text{Ab} : \mathcal{F} \mapsto \text{Mor}_{\mathcal{PSh}(\mathcal{C})}(e, \mathcal{F}) = \lim_{\longrightarrow X \in \mathcal{C}_{\text{op}}} \Gamma(X, \mathcal{F}) \), then we define its derived functor \( R\Gamma(\mathcal{C}, \mathcal{F}) \), and call the derived functors \( H^i(\mathcal{C}, \mathcal{F}) = H^i(R\Gamma(\mathcal{C}, \mathcal{F})) \) the \( i \)-th cohomology group of \( \mathcal{F} \) on \( \mathcal{C} \).

4. (Pushforward) Let \( (\mathcal{S}, \mathcal{O}) \to (\mathcal{D}, \mathcal{O}') \) be a morphism of topoi, then \( f_* \) is a left exact functor from \( \text{Mod}(\mathcal{O}) \) to \( \text{Mod}(\mathcal{O}') \)(5.1.2.18), and we call its derived functors \( R^if_* \) the \( i \)-th higher direct images.

5. (Shifification) Let shifification functor \( i : \mathcal{PSh}(\mathcal{C}) \to \mathcal{Sh}(\mathcal{C}) \) is left exact, and we call the derived functors \( H^p(F) \) the sheaf-cohomology presheaves of \( F \).

Def.(5.3.1.3)[G_a, G_m]. Let \( (\mathcal{C}, \mathcal{O}) \) be a ringed site, denote \( G_{a, \mathcal{C}} = \mathcal{O}, G_{m, \mathcal{C}} = \mathcal{O}^* \).

Prop.(5.3.1.4)[Global Section as Pushforward]. For a ringed site \( (\mathcal{C}, \mathcal{O}) \), if we endow \( \mathcal{C} \) with the discrete topology, then there is a functor \( \mathcal{C} \to \text{pt} \) which is cocontinuous, thus induce a morphism of ringed topoi \( \pi : (\mathcal{Sh}(\mathcal{C}), \mathcal{O}) \to (\mathcal{Sh}(\text{pt}) \cong \text{Ab}, \Gamma(\mathcal{C}, \mathcal{O})) \)(5.1.2.20). Then \( \pi_* \) is exactly \( \mathcal{F} \mapsto \Gamma(\mathcal{C}, \mathcal{F}) \), so \( R\pi_* \mathcal{F} = H^i(\mathcal{C}, \mathcal{F}) \).

Prop.(5.3.1.5)[Change of Topologies]. Let \( \mathcal{C}, \mathcal{C}' \) be sites and \( i : \mathcal{C}' \to \mathcal{C} \) is continuous and cocontinuous satisfying the hypothesis of (5.1.2.22), then for \( \mathcal{F} \in \mathcal{Sh}(\mathcal{C}'), \mathcal{G} \in \mathcal{Sh}(\mathcal{C}) \), there are functorial isomorphisms

\[ H^p(\mathcal{C}', U, i^{-1}\mathcal{G}) \cong H^p(\mathcal{C}, U, \mathcal{G}) \]

And if \( i \) satisfies the hypothesis of (5.1.2.24), then moreover there are functorial isomorphisms

\[ H^p(\mathcal{C}', U, F') \cong H^p(\mathcal{C}; U, i_*F') = H^p(\mathcal{C}; i(U), i_*F') \]

Proof: For the first assertion, notice \( g^{-1} \) preserves injectives because it is right adjoint to \( g_! = f^{-1} \) is exact (5.1.2.22).

The second assertion follows immediate from (5.1.2.24).
Calculations

Prop.(5.3.1.6) [Locality of Cohomologies]. Let \((\mathcal{C}, \mathcal{O})\) be a ring site and \(U \in \mathcal{C}\), then for \(\mathcal{F} \in \text{Mod}(\mathcal{O}_X)\), \(H^n(U, \mathcal{F}) = H^n(\mathcal{C}/U, \mathcal{F}|_U)\), by (5.3.1.7) and the composition of derived functors applied to the pullback \(j^* : \mathcal{C}/U \to \mathcal{C}\).

Prop.(5.3.1.7) [Sheaf-Cohomological Presheaves]. The forgetful functor is right adjoint to the exact shiffification functor, the composition of derived functors applied to the functor \(\Gamma(U, -) \circ \iota\) from \(PSh(\mathcal{C})\) to \(Ab\) shows its right derived functor is
\[
\mathcal{H}^p(F) = R^p\iota(F) : U \to H^p(U, F).
\]

Prop.(5.3.1.8) [Higher Direct Image]. For \(f : (\mathcal{C}', \mathcal{O}') \to (\mathcal{C}, \mathcal{O})\) a morphism of ringed topoi and \(\mathcal{F} \in \text{Sh}(\mathcal{C})\), the composition of derived functors applied to the functor \((\mathcal{F} \circ f)^{\text{Sh}} \circ (\mathcal{O})\) (because \(\mathcal{F} \circ f^{\text{Sh}} \circ (\mathcal{O})\) are exact(5.1.2.10)) shows that \(R^p f_* \mathcal{F} = (f_* \mathcal{H}^p(\mathcal{F}))^\#\). So flask sheave thus flabby sheave are right acyclic for \(f_*\).

In particular, \(R^p f_* \mathcal{F}\) can be calculated locally on the base.

Prop.(5.3.1.9) [Relative Leray Spectral Sequence]. Let
\[
(f, f^\sharp) : (\text{Sh}(\mathcal{C}), \mathcal{O}) \to (\text{Sh}(\mathcal{C}'), \mathcal{O}'), \quad (g, g^\sharp) : (\text{Sh}(\mathcal{C}'), \mathcal{O}') \to (\text{Sh}(\mathcal{D}), \mathcal{O}_D)
\]
be morphisms of ringed topoi, then the natural transformation \(R(g \circ f) \to Rg_* \circ Rf_*\) is an isomorphisms, and for any \(\mathcal{F}^\bullet \in K^+(\mathcal{O})\), there is a spectral sequence convergence
\[
E_2^{p,q} = R^p g_* R^q f_* (\mathcal{F}^\bullet) \Rightarrow E^n = R^n (g \circ f)_* (\mathcal{F}^\bullet).
\]

Proof: This is just the Grothendieck spectral sequence(3.4.7.11), where the condition is satisfied by(5.3.1.8) and(5.3.1.12).

Cor.(5.3.1.10) [Leray Spectral Sequence]. Let \(f, f^\sharp) : (\text{Sh}(\mathcal{C}), \mathcal{O}) \to (\text{Sh}(\mathcal{C}'), \mathcal{O}')\) be a morphism of ringed topoi, then for any \(\mathcal{F}^\bullet \in K^+(\mathcal{O})\), then \(R\Gamma(\mathcal{C}, -) \to R\Gamma(\mathcal{C}', -) \circ Rf_*\) is an isomorphism, and there is a spectral sequence convergence
\[
E_2^{p,q} = H^p(\mathcal{C}', R^q f_* (\mathcal{F}^\bullet)) \Rightarrow E^n = H^n(\mathcal{C}, \mathcal{F}^\bullet).
\]

Prop.(5.3.1.11) [Relative Mayer-Vietoris Sequence]. Let \((\mathcal{C}, \mathcal{O})\) be a ringed site and \(U : \{U \to X, V \to X\}\) is a covering s.t. \(U \to X\) is a monomorphism, then for any \(\mathcal{F} \in \text{Sh}(\mathcal{O})\) and any morphism of ringed sites \(f : (\mathcal{C}, \mathcal{O}) \to (\mathcal{O}', \mathcal{O}')\), there is a long exact sequence of sheaves in \(\text{Sh}(\mathcal{O}')\):
\[
0 \to (f|_{X*})(\mathcal{F}|_{X}) \to (f|_{U*})(\mathcal{F}|_{U}) \oplus (f|_{V*})(\mathcal{F}|_{V}) \to (f|_{U \cap V*})(\mathcal{F}|_{U \cap V}) \to R^1(f|_{X*})(\mathcal{F}|_{X}) \to \ldots
\]
that is functorial in \(f\).

Proof: Choose a functorial injection resolution \(\mathcal{F} \to \mathcal{I}^\bullet(3.4.3.9)\), then there is an exact sequence of complexes
\[
0 \to (f|_{X*})(\mathcal{I}^\bullet|_{X}) \to (f|_{U*})(\mathcal{I}^\bullet|_{U}) \oplus (f|_{V*})(\mathcal{I}^\bullet|_{V}) \to (f|_{U \cap V*})(\mathcal{I}^\bullet|_{U \cap V}) \to 0
\]
because injective sheaves are flabby(5.3.4.9) and \((U \times_X V) \times_X f^{-1}W \to V \times_X f^{-1}W\) is a monomorphism for any \(W \in \mathcal{O}'\). Then we take the long exact sequence of cohomology.
Cor. (5.3.1.12) [Mayer-Vietoris Sequence]. Let \((\mathcal{C}, \mathcal{O})\) be a ringed site and \(U : \{U \to X, V \to X\}\) is a covering s.t. \(U \to X\) is a monomorphism, then for any \(\mathcal{F} \in \mathsf{Sh}(\mathcal{O})\), there is a long exact sequence

\[0 \to H^0(X, \mathcal{F}) \to H^0(U, \mathcal{F}) \oplus H^0(V, \mathcal{F}) \to H^0(U \times_X V, \mathcal{F}) \to H^1(X, \mathcal{F}) \to \ldots\]

that is functorial in \(\mathcal{F}\).

Prop. (5.3.1.13) [Compatibility with Algebraic Structures]. Let \((\mathcal{C}, \mathcal{O})\) be a ringed site and \(\mathcal{F} \in \mathsf{Sh}(\mathcal{C})\), \(K \in \mathsf{PSh}(\mathcal{C})\), then \(H^*(K, \mathcal{F})\) is the same calculated as \(\mathcal{O}\)-modules or Abelian sheaves.

Proof: Denote \((C, \mathcal{Z})\) the trivial ringed site and \(ab : (C, \mathcal{O}) \to (C, \mathcal{Z})\) the forgetful functor, then \(ab\) is exact and \(\text{Hom}(K, \mathcal{F}_{ab}) = \text{Hom}(K, \mathcal{F})\), thus we can use the Leray spectral sequence (5.3.1.10). □

Prop. (5.3.1.14) [Direct Products]. Let \((\mathcal{C}, \mathcal{O})\) be a ringed site and \(\mathcal{F}_i\) be a family of sites indexed over a set \(I\), then for any presheaf of sets \(K\) on \(\mathcal{C}\), there is a Leray spectral sequence convergence

\[H^n(K, R^q(\prod_i \mathcal{F}_i)) \to R^n(\prod_i \text{Hom}(K, \mathcal{F}_i))(\mathcal{F}_i) \cong \prod_i H^n(K, \mathcal{F}_i).\]

In particular, \(H^1(K, \prod_i \mathcal{F}_i) \to \prod_i H^1(K, \mathcal{F}_i)\) is injective.

Prop. (5.3.1.15) [Filtered Colimits]. \(H^n(U, -)\) commutes with filtered colimits if \(T\) is a Noetherian topology.

Proof: \(n = 0\) case follows from the fact the colimit presheaf is already a sheaf, because for any finite cover, the Čech complex of the limit sheaf is the filtered colimit of Čech complexes, and filtered colimit is exact.

And a filtered colimits of injective sheaves is flask, because flask need only be checked for finite coverings at this case (because of the fact \(T\) and \(T^f\) have equivalent category of sheaves (5.1.1.3) and definition of flask (5.3.4.8)), and a filtered colimit of exact Čech complexes is exact. So we can choose a functorial injective resolution (3.4.3.9) and use the colimit resolution to calculate the cohomology. □

Prop. (5.3.1.16) [Filtered Colimits]. \(H^1(U, -)\) commutes with direct limits if \(X\) is a qs ringed space and \(U \subset X\) is qc.

Proof: The proof is the same as that of (5.7.1.5). □

Low Dimensions


Prop. (5.3.1.17) [\(H^1\) and Picard Group]. Let \((\mathcal{C}, \mathcal{O})\) be a local ringed site, then there is a canonical isomorphism of Abelian groups

\[H^1(\mathcal{C}, \mathcal{O}^*) = \text{Pic}(\mathcal{O}).\]

Proof: Let \(\mathcal{L}\) be an invertible sheaf, then there exists a subsheaf

\[\mathcal{L}^* : U \mapsto \{s \in \mathcal{L}(U) | s^* : \mathcal{O}(U) \to \mathcal{L}(U)\text{ is an isomorphism}\}.\]
Notice if \( f \in \mathcal{O}^*(U) \) and \( s \in \mathcal{L}^*(U) \), then \( fs \in \mathcal{L}^*(U) \), and any two \( s, s' \in \mathcal{L}^*(U) \) differ by an element of \( \mathcal{O}^*(U) \), so \( \mathcal{L}^* \) is a pseudo-\( \mathcal{O}^* \)-torsor. Moreover, as \( \mathcal{L} \) is locally free of rank 1 by (5.2.5.8), so \( \mathcal{L}^* \) has sections locally, so it is an \( \mathcal{O}^* \)-torsor.

In this way, we get a map
\[
\text{Pic}(\mathcal{O}) \to \text{Tor}(\mathcal{O}_{\mathcal{X}}^*) \cong H^1(X, \mathcal{O}_{\mathcal{X}}^*)(5.3.2.18).
\]
This map is injective: if \( \mathcal{L} \) corresponds to a trivial torsor, then \( \mathcal{L}^* \) has a global section, and then \( \mathcal{L} \) is also trivial. This map is also surjective, because if \( \mathcal{F} \) is an \( \mathcal{O}_{\mathcal{X}}^* \)-torsor, then we can define
\[
\mathcal{L}_1 : U \mapsto [\mathcal{F}(U) \otimes \mathcal{O}(U)]/\mathcal{O}(U)^*,
\]
where the action is given by \( f \cdot (s, g) = (fs, f^{-1}g) \), and \( \mathcal{L}_1 \) is an \( \mathcal{O} \)-module given the addition \( (s, g) + (s', g') = (s, g + \frac{g}{s}g') \), where \( \frac{g}{s} \in \mathcal{O}(U) \) satisfies \( \frac{g}{s} \cdot s = s' \). Then the shifification \( \mathcal{L} \) of \( \mathcal{L} \) is a locally trivial bundle that maps \( \mathcal{F} \).

**Prop. (5.3.1.18) \([H^2 \text{ and Objects of Gerbes}]\)** Let \( \mathcal{C} \) be a site and \( \mathcal{S} \to \mathcal{C} \) be a gerbe whose automorphism sheaves are Abelian. Let \( \mathcal{G} \) be the sheaf defined in (5.1.3.24). If \( U \) is an object of \( \mathcal{C} \) that

- there exists a cofinal system of coverings \( \{U_i \to U\} \) that for any such covering, \( H^1(U_i, \mathcal{G}) = 0 \), \( H^1(U_i \times_U U_j, \mathcal{G}) = 0 \),
- \( H^2(U, \mathcal{G}) = 0 \).

Then \( \mathcal{S}_U \) is non-empty.

**Proof:** By hypothesis, there is a covering \( \{U_i \to U\} \) and \( x_i \) in \( \mathcal{S} \) lying over \( U_i \). By item1, after refining the covering, we may assume \( H^1(U_i, \mathcal{G}) = 0 \) and \( H^1(U_{ij}, \mathcal{G}) = 0 \). Consider the sheaf
\[
\mathcal{F}_{ij} = \text{Isom}(x_i|_{U_{ij}}, x_j|_{U_{ij}})
\]
on \( \mathcal{C}/U_{ij} \), then there is an action \( \mathcal{G}_{U_{ij}} \times \mathcal{F}_{ij} \to \mathcal{F}_{ij} \). Then \( \mathcal{F}_{ij} \) is a pseudo \( \mathcal{G}|_{U_{ij}} \)-torsor and clearly a torsor because any two objects of a gerbe is locally isomorphic.

By (5.3.2.18), these torsors are trivial, thus having a global section. In other words, there are isomorphisms \( \varphi_{ij} : x_i|_{U_{ij}} \to x_j|_{U_{ij}} \). To get an object \( x \) over \( U \), it suffices to manage the choices of \( \varphi_{ij} \) to get a descent datum. For this, use the fact \( H^2(U, \mathcal{G}) = 0 \) and \( H^2(U, \mathcal{G}) \to H^2(U, \mathcal{G}) \) is injective by Cech to Derived spectral sequence (5.3.2.13). \( \square \)

**Others**

**Prop. (5.3.1.19)** Let \( K' \to K \) be a map of presheaves of sets on \( \mathcal{C} \) whose shifification is surjective. Set \( K' = K' \times_K \ldots \times_K K' \), then for any \( \mathcal{F} \in \text{Sh}(\mathcal{C}) \), there is a spectral sequence convergence
\[
E_1^{p,q} = H^q(K'_p, \mathcal{F}) \Rightarrow H^{p+q}(K, \mathcal{F}).
\]

**Proof:** Since shifification is exact, \( (K'_p)^\natural = (K'^\natural)_p \). Then we use (5.1.2.25) to change to a larger site \( \mathcal{C}' \) where the topoi are equivalent and \( K', K \) are objects in \( \mathcal{C}' \) and \( K' \to K \) is a covering, then we use the \( E_1 \) page of the Čech to derived spectral sequence (5.3.2.13). Notice this need modification, the modification goes back to the proof of the Grothendieck spectral sequence, where we choose the natural Čech complex resolution in place of the CE resolution, because we have (5.3.2.3). \( \square \)
Cor. (5.3.1.20)[Čech-Alexander Resolution]. If $C$ is a site with the indiscrete topology, $X$ a weakly final object (3.1.1.20) of $C$, then for any Abelian sheaf $F$ on $C$, the total cohomology $R\Gamma(C, F)$ is represented by the Čech complex

$$F(X) \to F(X \times X) \to F(X \times X \times X) \to \ldots.$$

Proof: By (5.3.4.10), $H^q(X^p, F) = 0$ for $q > 0$. The assumption says $h_X \to \ast$ is surjective, thus the conclusion is a special case of (5.3.1.19).

2 Čech Cohomology

Def. (5.3.2.1)[Čech Complex and Čech Cohomology]. Let $(C, \mathcal{O})$ be a ringed site and $U = \{U \to \ast\}$ be a covering, we have a canonical complex of presheaves $\mathcal{Z}_{U, \bullet}$ defined to be

$$\ldots \to \bigoplus_{i_0, i_1, i_2} j! \mathcal{Z}_{U_{i_0}i_1i_2} \to \bigoplus_{i_0, i_1} j! \mathcal{Z}_{U_{i_0}i_1} \to \bigoplus_{i_0} j! \mathcal{Z}_{U_{i_0}} \to 0.$$

And for any presheaf of $\mathcal{O}_X$-module $F$, the complex

$$\text{Hom}^\bullet_{Psh(C)}(\mathcal{Z}_{U, \bullet} \otimes \mathcal{O}, F) \cong \text{Hom}^\bullet_{P, \text{Ab}}(\mathcal{Z}_{U, \bullet}, F)$$

is called the Čech complex $\check{C}^\bullet(U, F)$ of $F$. The cohomology $\check{H}^\bullet(U, F)$ of $\check{C}^\bullet(U, F)$ is called the Čech cohomology of $F$ w.r.t $U$.

$\mathcal{Z}_{U, \bullet}$ is exact except in degree 0, where the homology is $j! \mathcal{Z}_U$. This is because we have a homotopy: choose a fixed $i_0$, for a $s \in \Gamma(U_{i_1\ldots i_n}, F)$, we map it to $(hs)_{i_1\ldots i_n} = \delta_{i, i_0} s$??. In particular, an injective sheaf is Čech acyclic.

Lemma (5.3.2.2). The Čech complexes $\check{C}^\bullet(U, -)$ induces a functor from $PSh(C)$ to $K^+(\text{Ab})$, which is an exact functor.

Proof: Because in each degree this functor is a sum of functors of the form $F \mapsto F(U)$, which are exact functors on $PSh(C)$.

Prop. (5.3.2.3)[Čech Complex as Derived Functors]. Let $C$ be a site and $U = \{U \to \ast\}$ be a covering, then $\check{H}^0(U, -)$ is left exact, and for $F \in \mathcal{Sh}(C)$, there are functorial quasi-isomorphisms

$$\check{C}^\bullet(U, F) \to R\check{H}^0(U, F)$$

which is functorial in $F$.

Proof: Choose a functorial injective resolution of presheaves $I^\bullet$ of $F$, and consider the double complex $\check{C}(U, I^\bullet)$. There are maps of complexes

$$\check{C}(U, F) \to \text{Tot}(\check{C}(U, I^\bullet)), \quad \check{H}^0(U, I^\bullet) \to \text{Tot}(\check{C}(U, I^\bullet))$$

which are both quasi-isomorphism by an application of spectral sequence and the fact the columns and rows are exact in positive degrees: The columns are exact because of (5.3.2.2) and the rows are exact because $\mathcal{Z}_{U, \bullet}$ is exact in positive degrees (5.3.2.1) and $I^p$ are injective. Then we have the desired quasi-isomorphism, and it is functorial in $F$. 

\[\square\]
Cor. (5.3.2.4) [Čech Cohomologies]. If we take filtered colimit for coverings, \( F \rightarrow \check{H}^0(U, F) = H^0(U, F) \) is a left exact functor from presheaves to sets, the derived complex is just \( \lim_{\rightarrow} \check{\mathcal{C}}^\bullet(U, F) \), and the derived functors are just \( \lim_{\rightarrow} \check{H}^q(U, F) \).

Proof: This is because we can take colimit of the conclusion of (5.3.2.3), because the colimit is filtered by (5.3.2.5) so exact, so the Čech complex also represents the derived complex. \( \square \)

Lemma (5.3.2.5). The refinement morphism of Čech cohomologies of two coverings doesn’t depends on the refinement map chosen.

Proof: For two refinement map, there is a commutative diagram

\[
\begin{array}{ccc}
\prod F(U_i) & \xrightarrow{\delta} & \prod F(U_i \times_U U_j) \\
\downarrow{f-g} & & \downarrow{\Delta^1} \\
\prod F(U'_j) & & 
\end{array}
\]

so it induce the same map on the kernel. \( \square \)

Def. (5.3.2.6) [Alternating Čech Complexes]. Let \((\mathcal{C}, \mathcal{O})\) be a ringed site and \( U : \{U_i \to U\} \in \text{Cov}(\mathcal{C}) \), \( F \in \mathcal{S}_\mathcal{O} \), then the alternating Čech complex \( \check{\mathcal{C}}^\bullet(U, F) \) is defined to be the subcomplex

\[
\check{\mathcal{C}}^\bullet_{\text{alt}}(U, F) = \{ s \in \check{\mathcal{C}}^\bullet(U, F) | s_{i_0, \ldots, i_p} = 0 \text{ if } i_m = i_n, m \neq n, s_{i_{\sigma(0)}, \ldots, i_{\sigma(p)}} = \text{sgn}(\sigma)s_{i_0, \ldots, i_p} \} \subset \check{\mathcal{C}}^\bullet(U, F).
\]

It is truly a subcomplex.

Prop. (5.3.2.7) [Alternating and Usual Complexes]. Let \((\mathcal{X}, \mathcal{O}_X)\) be a ringed space, \( U : \{U_i \to U\} \in \text{Cov}(\mathcal{C}) \), \( F \in \mathcal{S}_\mathcal{O}_X \), then the inclusion \( \check{\mathcal{C}}^\bullet_{\text{alt}}(U, F) \to \check{\mathcal{C}}^\bullet(U, F) \) is a homotopy equivalence.

Proof: Cf.[Sta]01FM. The proof is rather complicated. \( \square \)

Remark (5.3.2.8). WARNING: This is not right for ringed sites, e.g. the étale sites, for example, cf.(6.4.1.23).

Comparison Theorems

Prop. (5.3.2.9). If two coverings are refinements of each other, then their Čech cohomology is isomorphic.

Proof: Because the refinement morphism doesn’t depends on the refinement map(5.3.2.5). \( \square \)

Prop. (5.3.2.10) [Comparison Theorem for Čech Acyclicity]. If there are two coverings \( \mathcal{U}, \mathcal{V} \) and a presheaf \( F \), then we can construct a double Čech complex with the \((p, q)\)-term being \( F(U_{i_1, \ldots, i_p} \cap V_{j_1, \ldots, j_q}) \). Then the vertical and horizontal arrays calculate the Čech cohomology \( \prod_j H^s(U|_{V_{j_1, \ldots, j_q}}, F) \), \( \prod_i H^s(\mathcal{V}|_{U_{i_1, \ldots, i_q}}, F) \) respectively.

So by Spectral sequence(3.4.7.8), if both higher Čech cohomology group \( H^k(U|_{V_{j_1, \ldots, j_q}}, F) \), \( H^k(\mathcal{V}|_{U_{i_1, \ldots, i_q}}, F) \) vanish, i.e., they are both \( F \)-acyclic, then \( H^s(\mathcal{U}, F) \cong H^s(\mathcal{V}, F) \).
Cor. (5.3.2.11). If $\mathfrak{V}$ is a refinement of $\mathfrak{U}$, and $\mathfrak{V}|_{U_{i_1,\ldots,i_p}}$ are all $\mathcal{F}$ acyclic, then $H^*(\mathfrak{U}, \mathcal{F}) \cong H^*(\mathfrak{V}, \mathcal{F}).$

Proof: It suffices to prove $\mathfrak{U}|_{V_{i_1,\ldots,i_q}}$ is $\mathcal{F}$-acyclic. But $\mathfrak{U}|_{V_{i_1,\ldots,i_q}}$ and $\text{id}_{V_{i_1,\ldots,i_q}}$ are refinements of each other, so (5.3.2.9) settles the proof. □

Cor. (5.3.2.12). If $\mathfrak{V}|_{U_{i_1,\ldots,i_p}}$ is $\mathcal{F}$-acyclic, then the covering $H^*(\mathfrak{U} \times \mathfrak{V}, \mathcal{F}) = H^*(\{U_i \cap V_j\}, \mathcal{F}) \cong H^*(\mathfrak{U}, \mathcal{F}).$

Proof: Because $\mathfrak{V}|_{U_{i_1,\ldots,i_p}}$ and $\mathfrak{U} \times \mathfrak{V}|_{U_{i_1,\ldots,i_p}}$ are refinements of each other, so $\mathfrak{U} \times \mathfrak{V}$ refines $\mathfrak{U}$, so (5.3.2.11) can be applied. □

Prop. (5.3.2.13) Čech to Derived. For any $\mathcal{F} \in \text{Sh}(\mathcal{C})$, the Grothendieck spectral sequence applied to $\Gamma(U, -) = H^0(\{U_i \to U\}, -) \circ \iota = \tilde{H}^0(U, -) \circ \iota$ gives us:

$$H^p(\{U_i \to U\}, \mathcal{H}^q(\mathcal{F})) \Rightarrow H^{p+q}(U, \mathcal{F}).$$

$$\tilde{H}^p(U, \mathcal{H}^q(\mathcal{F})) \Rightarrow H^{p+q}(U, \mathcal{F}).$$

Cor. (5.3.2.14) [\tilde{H}^0 of Sheaf-Cohomology Presheaves]. For any $\mathcal{F} \in \text{Sh}(\mathcal{C})$, $\mathcal{H}^p(\mathcal{F})^+ = \mathcal{H}^p(\mathcal{F})^\sharp = 0$ for $p > 0$, so

$$\mathcal{H}^p(\mathcal{F})^+(U) = \tilde{H}^0(U, \mathcal{H}^p(\mathcal{F})) = 0 \quad p > 0.$$  

because $\mathcal{H}^p(\mathcal{F})^+$ is separated by (5.1.2.7). In particular, for any $s \in H^p(U, \mathcal{F})$, $p > 0$, there exists a covering $\mathcal{U}$ of $U$ s.t. $s|_{U_{i_j}} = 0$ for any $i$.

Thus the low degree of Čech to sheaf says (3.4.7.12):

$$0 \to \tilde{H}^1(U, \mathcal{F}) \to H^1(U, \mathcal{F}) \to 0 \to \tilde{H}^2(U, \mathcal{F}) \to H^2(U, \mathcal{F}) \to \tilde{H}^1(U, H^1(\mathcal{F})) \to \tilde{H}^2(U, \mathcal{F}) \to H^3(U, \mathcal{F}).$$

Proof: By Grothendieck spectral sequence applied to forgetful functor and exact $\sharp$ functor, where the condition are satisfied by (5.3.4.3). □

Cor. (5.3.2.15) [Acyclic Covering Calculates Derived Cohomologies]. If we have $H^q(U_{i_1,\ldots,i_p}, \mathcal{F}) = 0, q > 0$, then $H^p(\{U_i \to U\}, \mathcal{F}) = H^p(U, \mathcal{F})$ as $\mathcal{O}_X(U)$-modules.

Proof: Because $H^p(\{U_i \to U\}, \mathcal{H}^q(\mathcal{F}))$ vanish for $q > 0$. □

Prop. (5.3.2.16) Čech Acyclic Čech Comparison. If $\mathcal{C}$ be a ringed site, $\mathfrak{G} \subset \mathcal{C}, \text{Cov} \subset \text{Cov}(\mathcal{C})$ and $\mathcal{F} \in \text{Sh}(\mathcal{C})$ that

- For any $\{U_i \to U\} \in \text{Cov}, U_i, U \in \mathfrak{G}$, and $U_{i_1,\ldots,i_p} \in \mathfrak{G}$.
- $\text{Cov}|_U$ is cofinal in $\text{Cov}(\mathcal{C}/U)$ for any $U \in \mathfrak{G}$.
- $\tilde{H}^q(U, \mathcal{F}) = 0$ for any $U \in \mathfrak{G}$ and $q > 0$.

Then $H^p(X, \mathcal{F}) = \tilde{H}^p(X, \mathcal{F}) = H^p(\{U_i \to X\}, \mathcal{F})$ for any $\{U_i \to X\} \in \text{Cov}$.

Proof: By (5.3.2.15), we only have to show that $H^q(U, \mathcal{F}) = 0$ for $U \in \mathfrak{G}$ and $q > 0$. Use induction on $q$, use Čech to sheaf2: $\tilde{H}^p(U, \mathcal{H}^q(\mathcal{F})) \Rightarrow H^{p+q}(U, \mathcal{F})$. The case $q \neq 0$ is by condition 2, 3, and induction hypothesis. For $p = 0$, use (5.3.2.14). □
Non-Abelian Čech Cohomologies

**Def. (5.3.2.17) [Non-Abelian Cohomology].** Let $\mathcal{C}$ be a site and $\mathcal{G} \in Sh^{sp}(\mathcal{C})$, for any covering $U = \{U_i \to U\} \in Cov(\mathcal{C})$, we can define a non-Abelian Čech cohomology $\check{H}^1(U, \mathcal{G})$ as follows:

Define $Z^1(U, \mathcal{G})=\{\text{sets of families } (c_i) \mid c_i \in \Gamma(U_{ij}, \mathcal{G}) : c_{ijk}c_{ik}^{-1}c_{ij} = 1\}$.

If $c \in Z^1(G, M)$, then for any $g \in \Gamma(U, \mathcal{G})$,

$$c_g = (c_{ij} = g|_{U_i}c_{ij}g|_{U_j})$$

is also in $Z^1(U, \mathcal{G})$. This defines an equivalence relation on $Z^1(U, \mathcal{G})$, the equivalence classes are called $\check{H}^1(G, M)$. This is compatible with the commutative case.

Taking filtered colimit over all coverings of $U$, we can also define $\check{H}^1(U, \mathcal{G})$.

**Prop. (5.3.2.18) [H^1 and Torsors].** Let $\mathcal{C}$ be a site and $\mathcal{H} \in Sh(\mathcal{C})$, then there is a canonical isomorphism of $\mathcal{H}$-torsors(5.1.1.14) and $H^1(\mathcal{C}, \mathcal{H})$.

**Proof:** Cf.[Sta]03AJ. Should have a non-commutative version. \qed

**Prop. (5.3.2.19) [Long Exact Sequence of Non-Abelian Čech Cohomologies].** Let $\mathcal{C}$ be a site and $1 \to A \to B \to C \to 1$ is an exact sequence in $Sh^{sp}(\mathcal{C})$, then for any $U \in \mathcal{C}$, there is a long exact sequence of pointed sets

$$1 \to \Gamma(U, A) \to \Gamma(U, B) \to \Gamma(U, C) \xrightarrow{\delta} \check{H}^1(U, A) \to \check{H}^1(U, B) \to \check{H}^1(U, C) \xrightarrow{\Delta} \check{H}^2(U, A)$$

the last term is defined only when $A$ is in the center of $B$ and $U$ satisfies: For any covering $U$ and a refinement $\mathcal{W} \to U \times U$, there exists a refinement $U' \to U$ s.t. $U' \times U'$ is a refinement of $\mathcal{W}$.

$\delta$ is defined as follows: for $c \in \Gamma(\mathcal{C}, C)$, by taking a covering $\{U_i \to U\}$, we may assume that $c_{ij} = b_i \in \Gamma(U_i, B)$, then $a_{ij} = b_i^{-1}b_j$ is a cocycle, and a different choice differ by a cocycle, so this is well-defined.

$\Delta$ is defined as: for any covering $U$ of $U$ and $c = (c_{ij})$ a cocycle in $\check{H}^1(U, \mathcal{C})$, by passing to a refinement, we may assume that $c_{ij} \in \Gamma(U_{ij}, B)$, then $\delta(c)$ is represented by the 2-cocycle $a_{ijk} = c_{jk}c_{ik}^{-1}c_{ij} \in \Gamma(U, A)$.

**Proof:** The verification of well-definedness of $\Delta$ is checked at [Serre Local Fields P124].

For the exactness at $C^G$, the definition of $\delta$ shows that $\delta(c) = 1$ iff there is an inverse image $b$ that $b^{-1}\sigma(b) = 1$ for all $\sigma$.

For the exactness at $H^1(G, A)$, $a_\sigma = b^{-1}\sigma(b)$ if $a_\sigma$ is in the image of $\delta$. Conversely, the image of $b$ in $C$ is in $C^G$, so it is in the image of $\delta$.

For the exactness at $H^1(G, B)$, one way is clear, and for the other, if $\pi(b_\sigma) = c^{-1}\sigma(c)$, then if $t$ is an inverse image of $c$, then $tb_\sigma\sigma(t)^{-1}$ is a cocycle in $A$ cohomologous to $b_\sigma$.

For the exactness at $H^1(G, C)$, one way is clear, and if $b_\sigma$ is an inverse image of $b_\sigma$ and $a_{\sigma, \tau} = b_\sigma\sigma(b_\tau)b_\sigma^{-1}$ is a coboundary, then it is $a_\sigma\sigma(a_\tau)a_{\sigma, \tau}^{-1}$, so we change $b$ to $a_\sigma^{-1}b_\sigma$, as $A$ is in the center of $B$, this lifts $c$ to a cocycle in $B$. \qed

**Prop. (5.3.2.20) [Hilbert’s Theorem 90].** For $L/K$ a Galois extension, $H^1(\text{Gal}(L/K), GL_n(L)) = 1$, where $L$ is equipped with the discrete topology.
Proof: We prove any cocycle is a coboundary, for this, notice any cocycle factor through a finite quotient, and the images of it is contained in a finite extension of \( K \), hence it reduce to the case of \( L/K \) finite.

By definition, this is equivalent to any \( B \)-semi-linear representation of \( G \) free of finite rank is trivial, which is by(14.2.4.4). \( \square \)

Cor.(5.3.2.21) \[ semi-linear \ representations \]. The proposition implies that any semi-linear \( L \)-representation of \( G_{L/K} \) is trivial.

Cor.(5.3.2.22). \( H^1(G/L/K), SL_n(L) = 1 \). This is seen from the exact sequence 1 → SL\(_n\)(L) → GL\(_n\)(L) → \( L^\times \) → 1.

3 Derived Homology

K-Flat Complexes

Def.(5.3.3.1)[K-flat Complexes]. Let \((\mathcal{C}, \mathcal{O})\) be a ringed site, a complex \( \mathcal{K}^\bullet \) of \( \mathcal{O} \)-modules is called K-flat if for any acyclic complex \( \mathcal{F}^\bullet \) of \( \mathcal{O} \)-modules, the total complex \( \text{Tot}^\oplus(\mathcal{F}^\bullet \otimes_\mathcal{O} \mathcal{K}^\bullet) \) is acyclic, or equivalently, tensoring with \( \mathcal{K}^\bullet \) maps quasi-iso to quasi-iso, by the long exact sequence and the fact tensoring is an exact functor of triangulated categories(3.3.6.4).

Prop.(5.3.3.2). If \( K, K' \) are K-flat complexes of \( \mathcal{O} \)-modules,

\begin{itemize}
  \item \( \text{Tot}^\oplus(\mathcal{K} \otimes_\mathcal{O} \mathcal{K}') \) is K-flat.
  \item If \( (K_1, K_2, K_3) \) is a distinguished triangle in \( K(\mathcal{O}) \), if two of them is K-flat, then the third is also K-flat.
  \item Any bounded above complex of flat \( \mathcal{O} \)-modules is K-flat.
  \item Any filtered colimits of K-flat complexes are K-flat.
\end{itemize}

Proof: 1: This follows from(3.3.6.2).
3: use(3.3.6.4), and the long exact sequence.
4: Cf.[Sta]06YQ.
5: because we are taking termwise-colimit, and Tot and tensor all commute with filtered colimits. \( \square \)

Prop.(5.3.3.3)[K-Flat Resolutions]. Any complex \( \mathcal{P}^\bullet \) of \( \mathcal{O} \)-modules has a K-flat resolution \( \mathcal{K}^\bullet \rightarrow \mathcal{P}^\bullet \), moreover, each term of \( \mathcal{K}^\bullet \) is a flat \( \mathcal{O} \)-module and \( \mathcal{K}^\bullet \rightarrow \mathcal{P}^\bullet \) is termwise surjective.

Proof: Cf.[Sta]06Y4. \( \square \)

Lemma(5.3.3.4). Let \( P \rightarrow Q \) be a quasi-isomorphism of K-flat complexes of \( \mathcal{O} \)-modules, then for any complex \( L \) of \( \mathcal{O} \)-modules, \( \text{Tot}(L \otimes P) \rightarrow \text{Tot}(L \otimes Q) \) is a quasi-isomorphism.

Proof: Choose a K-flat resolution(5.3.3.3) \( K \) of \( L \), then notice

\[
\text{Tot}(L \otimes P) \cong \text{Tot}(K \otimes P) \cong \text{Tot}(K \otimes Q) \cong \text{Tot}(L \otimes Q)
\]

by definition of K-flatness(5.3.3.1). \( \square \)

Prop.(5.3.3.5)[Pullback of K-Flat is K-Flat]. Let \( f : (\text{Sh}(\mathcal{C}'), \mathcal{O}_{\mathcal{C}'}) \rightarrow (\text{Sh}(\mathcal{C}), \mathcal{O}_{\mathcal{C}}) \) be a morphism of ringed topoi, then \( f^* \) maps K-flat complexes to K-flat complexes.

Proof: Cf.[Sta]0G7E. \( \square \)
Derived Tensor Product and Tor

Def. (5.3.3.6) [Derived Tensor Product]. Let \( A \to B \) be a homomorphism of sheaves of rings over a site \( \mathcal{C} \), then the functor \( \text{Tot}^\oplus(- \otimes_{\mathcal{O}} -) \) is a bi-exact bifunctor of triangulated categories \( K(A) \times K(B) \to D(B) \) by (3.6.3.4)(3.4.1.8), and the class of K-flat complexes in \( K(A) \) and K-flat complexes in \( K(B) \) satisfies the condition of (the dual of)?? by (5.3.3.1) and (5.3.3.3), so we get a left derived functor

\[- \otimes^L_A - : D(A) \times D(B) \to D(B),\]

called the derived tensor product. And if any of \( M^\bullet, N^\bullet \in K(A) \) is K-flat, the natural map \( M^\bullet \otimes^L_A N^\bullet \to \text{Tot}^\oplus(M^\bullet \otimes_A N^\bullet) \) is an isomorphism in \( D(B) \).

Prop. (5.3.3.7). Let \( A \to B \) be a homomorphism of sheaves of rings over a site \( \mathcal{C} \). Let \( N^\bullet \) be a \( B \)-module, then for \( M^\bullet \in D(A) \), there are a functorial isomorphisms

\[M^\bullet \otimes^L_A N^\bullet \cong (M^\bullet \otimes^L_A B) \otimes^L_B N^\bullet.\]

Proof: Consider both sides as right derived functors of the multi-exact multifunctor. As this is true for \( \text{Tot}^\oplus \), these follow from the universal property and (3.4.4.14), the conditions are satisfied by (5.3.3.3)(5.3.3.4)(5.3.3.5).

Cor. (5.3.3.8) [Commutative Monoidal Structure]. If \( A = B = \mathcal{C} = \mathcal{O} \) and \( K, L, M \in K(\mathcal{O}) \), there are natural isomorphisms

\[K \otimes^L L \cong L \otimes^L K, \quad (K \otimes^L L) \otimes^L M \cong K \otimes^L (L \otimes^L M).\]

Thus \( D^*(\mathcal{O}) \) has a commutative monoidal structure.

Remark (5.3.3.9) [WARNING]. If \( M, N \) are two \( A \)-modules, then we can define \( M_R \otimes^L_R N \) and \( M \otimes^L_R N_R \), but there are no reason for them to be isomorphic.

Prop. (5.3.3.10). Let \( A \to B \to \mathcal{C} \) be homomorphism of sheaf of rings on a site \( \mathcal{C} \), then for \( M^\bullet \in K(A), N^\bullet \in K(B) \) and \( K^\bullet \in K(C) \), there are functorial isomorphisms

\[(M \otimes^L_A N) \otimes^L_B K = M \otimes^L_A (N \otimes^L_B K) = (M \otimes^L_A C) \otimes^L_C (N \otimes^L_B K)\]

called

\[(M \otimes^L_A N) \otimes^L_B K \cong (M \otimes^L_A K) \otimes^L_B (N \otimes^L_B C)\]

Proof: Consider both sides as right derived functors of the multi-exact multifunctor. As these are true for \( \text{Tot}^\oplus \), these follow from the universal property and (3.4.4.14), the conditions are satisfied by (5.3.3.3)(5.3.3.4)(5.3.3.5).

Def. (5.3.3.11) [Tor Modules]. Let \( \mathcal{F}, \mathcal{G} \) be \( \mathcal{O} \)-modules, then the Tor modules \( \text{Tor}_p^\mathcal{O}(\mathcal{F}, \mathcal{G}) \) is defined to be \( H^{-p}(\mathcal{F} \otimes^L_\mathcal{O} \mathcal{G}) \).

Prop. (5.3.3.12) [Flatness and Tor]. Let \( (\mathcal{C}, \mathcal{O}) \) be a ringed site, and \( \mathcal{F} \) is an \( \mathcal{O} \)-module. Then \( \mathcal{F} \) is a flat \( \mathcal{O} \)-modules iff \( \text{Tor}_1^\mathcal{O}(\mathcal{F}, \mathcal{G}) = 0 \) for any \( \mathcal{O} \)-module \( \mathcal{G} \).

Proof: If \( \mathcal{F} \) is flat, then clearly \( \text{Tor}_1^\mathcal{O}(\mathcal{F}, \mathcal{G}) = 0 \) for any \( \mathcal{O} \)-module \( \mathcal{G} \). Conversely, use the long exact sequence associated to \( \mathcal{F} \otimes^L_\mathcal{O} \) (3.3.6.4).
**Def. (5.3.3.13) [Relative Cup Product].** Let \( f : (\mathcal{Sh}(\mathcal{C}), \mathcal{O}_\mathcal{C}) \to (\mathcal{Sh}(\mathcal{D}), \mathcal{O}_\mathcal{D}) \) be a morphism of ringed topoi, then for any \( K, L \in D(\mathcal{O}_\mathcal{C}) \), there is a canonical functorial **relative cup product**

\[
Rf_*K \otimes^L_{\mathcal{O}_\mathcal{D}} Rf_*L \to Rf_*(K \otimes^L_{\mathcal{O}_\mathcal{C}} L)
\]

in \( D(\mathcal{O}_\mathcal{D}) \) that is the adjunction map of the map

\[
Lf^*(Rf_*K \otimes^L_{\mathcal{O}_\mathcal{D}} Rf_*L) \to Lf^*Rf_*K \otimes^L_{\mathcal{O}_\mathcal{C}} Lf^*Rf_*L \to K \otimes^L_{\mathcal{O}_\mathcal{C}} L
\]

by (5.3.3.15). This map is symmetric and associative.

In particular, if \( (\mathcal{Sh}(\mathcal{D}), \mathcal{O}_\mathcal{D}) = (\mathcal{Sh}(\text{pt}), \Gamma(\mathcal{C}, \mathcal{O}_\mathcal{C}) = A) \) (5.3.1.4), we get a map

\[
R\Gamma(\mathcal{C}, K) \otimes^L_A R\Gamma(\mathcal{C}, L) \to \Gamma(\mathcal{C}, K \otimes^L_{\mathcal{O}_\mathcal{C}} L).
\]

**Derived Pullback**

**Def. (5.3.3.14) [Derived Pullback].** Let \( f : (\mathcal{Sh}(\mathcal{C}'), \mathcal{O}') \to (\mathcal{Sh}(\mathcal{C}), \mathcal{O}) \) be a morphism of ringed site, define the **derived pullback**

\[
Lf^* : D(\mathcal{O}) \to D(\mathcal{O}') : \mathcal{F}^* \mapsto f^{-1}\mathcal{F}^* \otimes^L_{f^{-1}\mathcal{O}} \mathcal{O}'(5.3.3.6).
\]

In particular, if \( \mathcal{F}^* \) is K-flat, then there are natural isomorphisms \( Lf^*\mathcal{F}^* \cong f^*\mathcal{F}^* \).

Moreover, \( Lf^* \) is also naturally isomorphic to the left derived functor of the pullback morphism \( f^* \), by composition of derived functors applied to the \( f^* = \text{Tot}(\cdot \otimes_{f^{-1}\mathcal{O}} \mathcal{O}') \circ f^{-1} \) where \( f^{-1} \) is exact. In particular, \( Lf^* \) only depends on the underlying map \( f^* \) of ringed topoi.

**Prop. (5.3.3.15).** Let \( f : (\mathcal{Sh}(\mathcal{C}), \mathcal{O}_\mathcal{C}) \to (\mathcal{Sh}(\mathcal{D}), \mathcal{O}_\mathcal{D}), \ g : (\mathcal{Sh}(\mathcal{D}), \mathcal{O}_\mathcal{D}) \to (\mathcal{Sh}(\mathcal{E}), \mathcal{O}_\mathcal{E}) \) be a morphism of ringed topoi, then

- There is a natural isomorphism \( L(g \circ f)^* \cong Lf^* \circ Lg^* \). In particular, as localizing map \( j^* \) is exact, \( Lf^* \) can be calculated locally on the base.

- For \( \mathcal{F}^*, \mathcal{G}^* \in \text{Mod}_{\mathcal{O}_\mathcal{D}}, \) there are natural functorial isomorphisms

\[
Lf^*(\mathcal{F}^* \otimes^L_{\mathcal{O}_\mathcal{D}} \mathcal{G}^*) \cong Lf^*\mathcal{F}^* \otimes^L_{\mathcal{O}_\mathcal{C}} Lf^*\mathcal{G}^*.
\]

In particular, as localizing map \( j^* \) is exact, the derived tensor product can be calculated locally on the base.

- For \( \mathcal{F}^* \in \text{Mod}_{\mathcal{O}_\mathcal{C}}, \mathcal{G}^* \in \text{Mod}_{\mathcal{O}_\mathcal{D}}, \) there are natural functorial isomorphisms

\[
\mathcal{F}^* \otimes^L_{\mathcal{O}_\mathcal{C}} Lf^*\mathcal{G}^* \cong \mathcal{F}^* \otimes^L_{f^{-1}\mathcal{O}_\mathcal{D}} f^{-1}\mathcal{G}'
\]

- For \( \mathcal{F}^*, \mathcal{G}^* \in \text{Mod}_{\mathcal{O}_\mathcal{D}}, \) the natural isomorphisms satisfy a commutative diagram

\[
\begin{array}{ccc}
Lf^*(\mathcal{F}^* \otimes^L_{\mathcal{O}_\mathcal{D}} \mathcal{G}^*) & \longrightarrow & Lf^* \text{Tot}^\oplus(\mathcal{F}^* \otimes_{\mathcal{O}_\mathcal{D}} \mathcal{G}^*) \\
\downarrow & & \downarrow \\
Lf^*\mathcal{F}^* \otimes^L_{\mathcal{O}_\mathcal{C}} Lf^*\mathcal{G}^* & \longrightarrow & f^* \text{Tot}^\oplus(f^*\mathcal{F}^* \otimes_{\mathcal{O}_\mathcal{C}} f^*\mathcal{G}^*),
\end{array}
\]
Proof: 1, 2, 3: These follow from (5.3.3.10).

4: By a universal argument, \((\mathcal{F}^\bullet, \mathcal{G}^\bullet) \mapsto LF^*(\mathcal{F}^\bullet \otimes_{\mathcal{O}_D} \mathcal{G}^\bullet)\) is the derived functor of the bi-exact bifunctor

\[ F : K(\mathcal{O}_D) \times K(\mathcal{O}_D) \to D(\mathcal{O}_C) : (\mathcal{F}^\bullet, \mathcal{G}^\bullet) \mapsto f^* \text{Tot}^2(\mathcal{F}^\bullet \otimes_{\mathcal{O}_D} \mathcal{G}^\bullet). \]

Then by the universal property, both natural transformations corresponds to a natural transformation \(\theta_i : LF \to LF\). So it suffices to show that they are isomorphic. But K-flat morphisms are essentially surjective in \(D(\mathcal{O}_D)\), thus it suffices to prove the diagram is commutative for \(\mathcal{F}, \mathcal{G}\) K-flat. But in this case, there are commutative diagrams

\[
\begin{align*}
LF(\mathcal{F}^\bullet, \mathcal{G}^\bullet) & \xrightarrow{\eta(\mathcal{F}, \mathcal{G})} F(\mathcal{F}^\bullet, \mathcal{G}^\bullet) \\
\downarrow \theta_1 & \downarrow \text{id} \\
LF(\mathcal{F}^\bullet, \mathcal{G}^\bullet) & \xrightarrow{\eta(\mathcal{F}, \mathcal{G})} F(\mathcal{F}^\bullet, \mathcal{G}^\bullet)
\end{align*}
\]

and \(\eta(\mathcal{F}, \mathcal{G})\) is an isomorphism, so \(\theta_1 = \theta_2\). \(\square\)

**Prop. (5.3.3.16) [Adjunction].** \(LF^*\) is left adjoint to \(Rf_*\), by (3.4.4.15) and (5.2.2.9).

**Prop. (5.3.3.17) [Base Change Map].** Let

\[
(\text{Sh}(C'), \mathcal{O}_{C'}) \xrightarrow{g'} (\text{Sh}(C), \mathcal{O}_C) \\
\downarrow \mathbb{f}' \quad \downarrow \mathbb{f} \\
(\text{Sh}(D'), \mathcal{O}_{D'}) \xrightarrow{g} (\text{Sh}(D), \mathcal{O}_D)
\]

be a commutative diagram of ringed topoi, then for any \(K \in D(\mathcal{O}_C)\), there is a canonical base change map

\[ LG^*Rf_*K \to R(f')_*L(g')^*K \]

functorial in \(K\), and this map is compatible with composition of diagrams.

**Proof:** By adjunction (5.3.3.16), this follows from the canonical map

\[ Rf_*K \to Rg_*R(f')_*L(g')^*K = Rf_*R(g')_*L(g')^*K, \]

which comes from the adjunction map \(K \to R(g')_*L(g')^*K\). \(\square\)

**Cor. (5.3.3.18) [Flat Base Change Morphism].** Let

\[
(\text{Sh}(C'), \mathcal{O}_{C'}) \xrightarrow{g'} (\text{Sh}(C), \mathcal{O}_C) \\
\downarrow \mathbb{f}' \quad \downarrow \mathbb{f} \\
(\text{Sh}(D'), \mathcal{O}_{D'}) \xrightarrow{g} (\text{Sh}(D), \mathcal{O}_D)
\]

be a commutative diagram of ringed sites. Assume both \(g, g'\) are flat, then for any \(\mathcal{F}^\bullet \in K^+(\mathcal{O}_C)\), there is a canonical base change map

\[ g^*Rf_*\mathcal{F}^\bullet \to Rf'_*(g')^*\mathcal{F}^\bullet. \]

and when \((\text{Sh}(D'), \mathcal{O}_D) = (\text{Sh}(C/U), \mathcal{O}_U)\) is the localizing site, then this map is an isomorphism

\[ (Rf_*\mathcal{F}^\bullet)_U \cong Rf'_*(\mathcal{F}^\bullet)_U. \]
Proof: The last assertion follows from the fact the restriction of a K-injective is also a K-injective \((5.3.4.2)\).

**Def. (5.3.3.19) [Projection Map].** Let \( f : (\mathcal{Sh}(\mathcal{C}), \mathcal{O}_\mathcal{C}) \to (\mathcal{Sh}(\mathcal{D}), \mathcal{O}_\mathcal{D}) \) be a morphism of ringed topoi, then for any \( E \in D(\mathcal{O}_\mathcal{C}) \) and \( K \in D(\mathcal{O}_\mathcal{D}) \), there is a canonical functorial projection map

\[
R f_* E \otimes_{\mathcal{O}_\mathcal{D}} K \to R f_* (E \otimes_{\mathcal{O}_\mathcal{C}} L f^* K)
\]

which is the adjunction of the map

\[
L f^* (R f_* E \otimes_{\mathcal{O}_\mathcal{D}} K) \cong L f^* R f_* E \otimes_{\mathcal{O}_\mathcal{C}} L f^* K \to E \otimes_{\mathcal{O}_\mathcal{C}} L f^* K
\]

by \((5.3.3.15)\).

**Prop. (5.3.3.20) [Projection Formula].** In situation \((5.3.3.19)\), if \( K \) is perfect \((5.3.4.17)\), then the projection map is an isomorphism.

Proof: To check it is an isomorphism, it suffice to find a covering \( \{ U_i \to V \} \) for each \( V \in \mathcal{C} \) that this map is an isomorphism on \( U_i \). (To see this, look at \( H^1 \), and notice \( U \mapsto \text{Mod}(\mathcal{O}_U) \) is a stack.) Then we may assume \( K \) is a finite complex of \( \mathcal{O}_U \)-modules consisting of finite free \( \mathcal{O}_U \)-modules. And then we use truncation to reduce to the case \( K \) is discrete, in which case it is trivial. \( \square \)

**Inner Hom**

**Def. (5.3.3.21) [Sheaf Hom Complexes].** Let \( (\mathcal{C}, \mathcal{O}) \) be a ringed site and \( P^\bullet, Q^\bullet \in K(\mathcal{O}) \), we define the sheaf hom complex \( \mathcal{H}om^\bullet(P^\bullet, Q^\bullet) \) to be

\[
\mathcal{H}om^n(P^\bullet, Q^\bullet) = \prod_i \mathcal{H}om_{\mathcal{O}}(P^i, Q^{n+i})(5.2.3.1),
\]

with the differential giving by \( d(\{ f_k \}_i) = \{ df_i - (-1)^i f_{i+1} d \} \) and suitable signatures.

It is clear that

\[
\Gamma(U, \mathcal{H}om_\mathcal{O}(P^\bullet, Q^\bullet)) = \text{Hom}_{\mathcal{O}_{\mathcal{U}}}(P^\bullet|_U, Q^\bullet|_U), \quad \Gamma(\mathcal{C}, \mathcal{H}om_\mathcal{O}(P^\bullet, Q^\bullet)) = \text{Hom}_{\mathcal{O}}(P^\bullet|_U, Q^\bullet|_U)
\]

and

\[
H^n(\Gamma(\mathcal{C}, \mathcal{H}om^\bullet(P^\bullet, Q^\bullet))) = \text{Hom}_{K(\mathcal{O}_U)}(P^\bullet|_U, Q^\bullet|_U[n]), \quad H^n(\Gamma(\mathcal{C}, \mathcal{H}om^\bullet(P^\bullet, Q^\bullet))) = \text{Hom}_{K(\mathcal{O})}(P^\bullet, Q^\bullet[n]).
\]

**Prop. (5.3.3.22) [Adjunction].** For \( K^\bullet, M^\bullet, L^\bullet \in K(\mathcal{O}) \), there is a canonical functorial isomorphism:

\[
\mathcal{H}om^\bullet(K, \mathcal{H}om^\bullet(L, M)) = \mathcal{H}om^\bullet(\text{Tot}(K \otimes_R L), M).
\]

Proof: Cf. [Sta]0A5Y. \( \square \)

**Prop. (5.3.3.23).** For \( K^\bullet, M^\bullet, L^\bullet \in K(\mathcal{O}) \), there are canonical functorial morphisms:

- \( \text{Tot}(\mathcal{H}om(K^\bullet, L^\bullet) \otimes_{\mathcal{O}} K^\bullet) \to L^\bullet \),
- \( \text{Tot}(\mathcal{H}om^\bullet(L, M) \otimes_{\mathcal{O}} \mathcal{H}om^\bullet(K, L)) \to \mathcal{H}om^\bullet(K, M) \),
- \( \text{Tot}(\mathcal{H}om^\bullet(L, M) \otimes_{\mathcal{O}} K) \to \mathcal{H}om^\bullet(\mathcal{H}om^\bullet(K, L), M) \),
- \( \text{Tot}(K \otimes_{\mathcal{O}} \mathcal{H}om^\bullet(M, L)) \to \mathcal{H}om^\bullet(M, \text{Tot}(K \otimes_{\mathcal{O}} L)) \),
• $\mathcal{K} \to \mathcal{H}om^\bullet(L, \text{Tot}(\mathcal{K} \otimes \mathcal{O} L))$.

**Proof:** All these are consequences of (5.3.3.22). \hfill \Box

**Lemma (5.3.3.24).** Let $(\mathcal{C}, \mathcal{O})$ be a site and $(\mathcal{I}^\bullet)' \to \mathcal{I}^\bullet$ be a quasi-isomorphism of K-injective $\mathcal{O}$-modules and $(\mathcal{L}^\bullet)' \to \mathcal{L}^\bullet$ be a quasi-isomorphism of $\mathcal{O}$-modules, then the natural map

$\mathcal{H}om^\bullet((\mathcal{L}^\bullet)'(\mathcal{I}^\bullet)') \to \mathcal{H}om^\bullet((\mathcal{L}^\bullet)'(\mathcal{I}^\bullet))$

is a quasi-isomorphism.

**Proof:** $H^n(\mathcal{H}om^\bullet((\mathcal{L}^\bullet)'(\mathcal{I}^\bullet)'))$ is the the sheaf $U \to \text{Hom}_{K(\mathcal{O}_U)}((\mathcal{L}^\bullet)'_U,(\mathcal{I}^\bullet)_U^[[n]])$, and $(\mathcal{I}^\bullet)_U^[[n]]$ is K-injective by (5.3.4.2). \hfill \Box

**Def. (5.3.3.25) [Internal Hom].** Let $(\mathcal{C}, \mathcal{O})$ be a ringed site, $K(\mathcal{O})$ has enough K-injectives, thus by (3.4.4.13), we can define the internal Hom

$R\mathcal{H}om : D(\mathcal{O})^{\text{op}} \times D(\mathcal{O}) \to D(\mathcal{O})$

as the right derived functor of the bi-exact bifunctor $\mathcal{H}om^\bullet : K(\mathcal{O})^{\text{op}} \times K(\mathcal{O}) \to D(\mathcal{O})$, where the conditions are satisfied by (5.3.3.24).

**Prop. (5.3.3.26) [Internal Hom and Localization].** Let $(\mathcal{C}, \mathcal{O})$ be a ringed site, for any $\mathcal{G}, \mathcal{F} \in K(\mathcal{O})$ and $U \in \mathcal{C}$, the natural transformation

$R\mathcal{H}om(\mathcal{F}, \mathcal{G}) \mid_U \to R\mathcal{H}om(\mathcal{F} \mid_U, \mathcal{G} \mid_U)$

is an isomorphism. In particular, we can calculate $\mathcal{E}xt$ locally.

**Proof:** This follows from (5.3.3.21)(5.3.4.2) and trivial Grothendieck duality applied to restrictions. \hfill \Box

**Prop. (5.3.3.27) [Derived Hom and Internal Hom].** For a ringed site $(\mathcal{C}, \mathcal{O})$ and $\mathcal{F}, \mathcal{G} \in D(\mathcal{O})$, $U \in \mathcal{C}$,

$$R\Gamma(\mathcal{C}, R\mathcal{H}om(\mathcal{F}, \mathcal{G})) = R\text{Hom}(\mathcal{F}, \mathcal{G}), \quad R\Gamma(U, R\mathcal{H}om(\mathcal{F}, \mathcal{G})) = R\text{Hom}_{\mathcal{O}_U}(\mathcal{F} \mid_U, \mathcal{G} \mid_U).$$

In particular,

$$\Gamma(U, R\mathcal{H}om(\mathcal{F}, \mathcal{G})) = \text{Hom}_{D(\mathcal{O}_U)}(\mathcal{F} \mid_U, \mathcal{G} \mid_U),$$

and

$$H^0(\mathcal{C}, R\mathcal{H}om(\mathcal{F}, \mathcal{G})) = \text{Hom}_{D(\mathcal{O})}(\mathcal{F}, \mathcal{G}), \quad H^p(\mathcal{C}, R\mathcal{H}om(\mathcal{F}, \mathcal{G})) = \text{Ext}^p_{\mathcal{O}}(\mathcal{F}, \mathcal{G})$$

by (5.3.3.21)(5.3.4.2)(5.3.4.13) and the composition of derived functors.

**Prop. (5.3.3.28).** If $\mathcal{K}, \mathcal{L}, \mathcal{M} \in D(\mathcal{O})$, then there is a natural isomorphism

$R\mathcal{H}om_{\mathcal{O}}(\mathcal{K}, R\mathcal{H}om(\mathcal{L}, \mathcal{M})) \cong R\mathcal{H}om_{\mathcal{O}}(\mathcal{K} \otimes_{\mathcal{O}} \mathcal{L}, \mathcal{M}).$

**Proof:** Consider both sides as the derived functor of the triple-exact triple-functor

$$K(\mathcal{O})^{\text{op}} \times K(\mathcal{O})^{\text{op}} \times K(\mathcal{O}) \to D(\mathcal{O}) : (\mathcal{K}^\bullet, \mathcal{L}^\bullet, \mathcal{M}^\bullet) \mapsto \text{Tot}^\oplus(\mathcal{K}^\bullet \otimes_{\mathcal{O}} \text{Tot}^\oplus(\mathcal{L}^\bullet \otimes_{\mathcal{O}} \mathcal{M}^\bullet)),$$

the conditions are satisfied by (5.3.4.13)(5.3.3.3). As this is true for $\text{Tot}$ by (5.3.3.22), this follows from the universal properties and (3.4.4.14). \hfill \Box
5.3. COHOMOLOGY ON RINGED SITES

Cor. (5.3.3.29) [Adjunction]. By (5.3.3.28), taking $H^0(R\Gamma(C, -))$, we get:

$$\text{Hom}_{D(O)}(K, R\text{Hom}(L, M)) = \text{Hom}_{D(O)}(K \otimes L, M).$$

that is, derived tensor is left adjoint to internal hom.

Prop. (5.3.3.30). Given complexes $K, L, M \in D(O)$, there are canonical functorial morphisms:

- $\text{Hom}(K, L) \otimes_M K \to L$,
- $R\text{Hom}(L, M) \otimes_M R\text{Hom}(K, L) \to R\text{Hom}(K, M)$,
- $R\text{Hom}(L, M) \otimes_M K \to R\text{Hom}(R\text{Hom}(K, L), M)$,
- $K \otimes_M R\text{Hom}(M, L) \to R\text{Hom}(M, K \otimes_M L)$,
- $K \to R\text{Hom}(L, K \otimes_M L)$.

Proof: These are direct consequences of (5.3.3.29).

Prop. (5.3.3.31). Let $(\text{Sh}(C), O) \to (\text{Sh}(C'), O')$ be a morphism of ringed site and $K, L \in D(O)$, there is a natural morphism

$$Rf_* R\text{Hom}_O(L, K) \to R\text{Hom}_{O'}(Rf_* L, Rf_* K).$$

Proof: This follows from the adjunction (5.3.3.28) (5.3.3.30) and the relative cup product (5.3.3.13).

Def. (5.3.3.32) [Internal Ext Groups]. For any $G, F \in K(O)$, we define the internal Ext groups

$$\text{Ext}^n_O(G, F) = H^i(R\text{Hom}(G, F)) \in \text{Mod}(O).$$

Prop. (5.3.3.33). For $E, F, L \in \text{Mod}(O_X)$ and $L$ finite locally free,

$$\text{Ext}^i(F \otimes L, G) \cong \text{Ext}^i(F, L^\vee \otimes G) \cong \text{Ext}^i(F, G) \otimes L^\vee$$

because there are maps between them (5.2.5.2), and Ext is local, so check locally. In particular,

$$\text{Ext}^i(F \otimes L, G) = \text{Ext}^i(F, L^\vee \otimes G).$$

Prop. (5.3.3.34) [Spectral Sequences for Internal Ext]. Let $(C, O)$ be a ringed site and $K^\bullet \in K^-(O), F^\bullet \in K^+(O)$, then there are spectral sequence convergence

$$E^{i+j}_2 = \text{Ext}^i_O(H^{-j}(K^\bullet), F^\bullet) \implies \text{Ext}^{i+j}_O(K^\bullet, F^\bullet).$$

$$E^{i+j}_1 = \text{Ext}^i_O(K^{-i}, F^\bullet) \implies \text{Ext}^{i+j}_O(K^\bullet, F^\bullet)$$

$$E^{i+j}_2 = H^i(C, \text{Ext}^j_O(K^\bullet, F^\bullet)) \implies \text{Ext}^{i+j}_O(K^\bullet, F^\bullet)$$

Proof: 1, 2: Choose a (bounded below) injective resolution $I^\bullet$ of $F^\bullet$, and these are the two spectral sequences associated to the double complex $\text{Hom}_{O_X}(K^\bullet, I^\bullet)$.

3: Use Grothendieck spectral sequence on (5.3.3.27).
4 Acyclic Sheaves

Prop. (5.3.4.1) [Pushforward of Injectives]. Let $f : (\text{Sh}(C), O_C) \to (\text{Sh}(D), O_D)$ be a flat map of ringed topoi, then $f$ preserves injectives, as $f^*$ is exact.

Prop. (5.3.4.2) [Restriction of (K-)Injectives]. Let $(C, \mathcal{O})$ be a ringed site, $U \in C$, then
- If $K^\bullet$ be a K-injective complex $\mathcal{O}$-modules, then $(K^\bullet)|_U$ is a K-injective complex of $\mathcal{O}_U$-modules.
- If $\mathcal{I}$ is an injective $\mathcal{O}$-module, then $\mathcal{I}|_U$ is an injective $\mathcal{O}_U$-module.

Proof: Use (3.4.3.6) and the fact $j^*_U$ is right adjoint to the exact shifification functor. □

Prop. (5.3.4.3). If $I \in \text{Sh}(C)$ is injective, then $I$ is also injective in $\text{PSh}(C)$.

Proof: Because restriction is right adjoint to the exact shifification functor. □

Prop. (5.3.4.4). For an injective sheaf $F$ on a site $(C, \mathcal{O})$, $F(U)$ is injective Abelian group for every $U \in C$.

Proof: This is because for the morphism $i : \text{pt} \to C : \text{pt} \mapsto U$, $i_p$ is exact($i_p A(V) = \oplus_{\text{Hom}(V,U)} A$), hence $i^p$ preserves injectives. □

Flask Sheaves

Def. (5.3.4.5) [Totally Acyclic Sheaves]. A totally acyclic sheaf on a ringed site $(C, \mathcal{O})$ is an object in $\text{Sh}(C)$ that is acyclic for any functor $\text{Hom}_{\text{PSh}(C)}(K, -)$.

Prop. (5.3.4.6) [Characterization of Totally Acyclic Sheaves]. Let $\mathcal{C}$ be a site and $F \in \text{Sh}(\mathcal{C})$, then $F$ is totally acyclic iff
- $F$ is acyclic for $\mathcal{I}(U, -)$ for any $U \in \mathcal{C}$.
- For every surjection $K' \to K$ of sheaves of sets the extended Čech complex
  
  $$0 \to H^0(K, F) \to H^0(K', F) \to H^0(K' \times_K K', F) \to \ldots$$

  is exact.


Prop. (5.3.4.7). A totally acyclic sheaf is acyclic for any map of ringed topoi $f : (\text{Sh}(C), O_C) \to (\text{Sh}(D), O_D)$.

Proof: This follows from the description of $R^i f_*$ in (5.3.1.8). □

Def. (5.3.4.8) [Flask Sheaves]. A flask sheaf on a ringed site $(C, \mathcal{O})$ is an object of $\text{Sh}(C)$ that satisfies the following equivalent conditions:
- It is acyclic for $\mathcal{I}$.
- It is acyclic for any $\check{H}^0(\{U_i \to U\}, -)$
- It is acyclic for all $\mathcal{I}(U, -)$.

In particular a totally acyclic sheaf is flask.

A flabby sheaf is an object of $\text{Sh}(C)$ that for any monomorphism $U \to V$, $F(V) \to F(U)$ is surjective;
5.3. COHOMOLOGY ON RINGED SITES

Proof:  1 ⇐⇒ 3 is by (5.3.1.7),
3 → 2: use Čech to sheaf1 (5.3.2.13), notice the \( q > 0 \) terms vanish, thus \( \check{H}^p(\{U_i \to U\}, \mathcal{F}) = H^p(U, \mathcal{F}) = 0. \)
2 → 3 follows from (5.3.2.16).

Prop. (5.3.4.9). Injective sheaves are flabby. Flabby sheaves on a ringed space are flasque.

Proof: For the first assertion, use (5.2.2.9) and the fact \( j_! \mathcal{O}_U \to j_! \mathcal{O}_V \) is a monomorphism for \( V \to U \) a monomorphism by definition (5.2.2.9).
For the last assertion, use (3.4.2.29): Injectives are flabby, so it is sufficiently large. For an exact sequence \( 0 \to \mathcal{F} \to \mathcal{G} \to \mathcal{H} \to 0 \) of sheaves, if \( \mathcal{F} \) is flabby, then \( \mathcal{H} \) is just the presheaf cokernel. (It reduces to \( \check{H}^1(\{U_i \to U\}, \mathcal{F}) = 0 \), and this is done by Zorn’s lemma). Thus if \( \mathcal{F} \) is flabby, \( \mathcal{G} \) is flabby iff \( \mathcal{H} \) is flabby (by five lemma).

Prop. (5.3.4.10). On a discrete site, all sheaves is flasque, because \( \iota \) is the identity functor.

Prop. (5.3.4.11). Filtered colimits of flabby sheaves is flabby. (This is because filtered colimits are exact).
Filtered colimits of injective sheaves over a Noetherian topological space is injective. (Use Baer criterion, then notice every sub-object of \( \mathbb{Z}_U \) is finitely generated because it has only f.m. connected component (3.8.3.4) so it maps to some \( F_\alpha \)).

Prop. (5.3.4.12) [Pushforward of Totally Acyclic/Flask Sheaves]. Let \( f : (\mathcal{S}(\mathcal{C}), \mathcal{O}_C) \to (\mathcal{S}(\mathcal{D}), \mathcal{O}_D) \) be a map of ringed topoi (resp. ringed site), then \( f_* \) maps totally acyclic (resp. flask) sheaves to totally acyclic (resp. flask) sheaves (5.3.4.5)(5.3.4.8). In particular, it maps injectives to totally acyclic sheaves.

Proof: By (5.2.1.3) we may assume \( f \) is a map of ringed sites, and \( K = h_U \) for some \( U \in \mathcal{C} \). Then we notice \( H^i(\{U_i \to U\}, f_* \mathcal{F}) = H^i(\{f^{-1}(U_i) \to f^{-1}(U)\}, \mathcal{F}) \), then we can use (5.3.2.16) to show \( f_* \mathcal{F} \) is totally acyclic.

Prop. (5.3.4.13) [Technical Lemma]. If \( \mathcal{K}^* \) is \( K \)-flat \( \mathcal{O} \)-modules and \( \mathcal{I}^* \) is \( K \)-injective \( \mathcal{O} \)-modules, then \( \mathcal{H}om^*(\mathcal{K}^*, \mathcal{I}^*) \) is \( K \)-injective.

Proof: Use definitions (5.3.3.1)(3.4.3.1) and (5.3.3.22).

Prop. (5.3.4.14). If \( \mathcal{I} \) is an injective \( \mathcal{O}_X \)-module, then for a coherent locally free sheaf \( \mathcal{L} \), \( \mathcal{L} \otimes \mathcal{I} \) is also injective, because tensoring with \( \mathcal{L} \) is adjoint to tensoring with \( \mathcal{L}^\vee \) (5.2.5.2), which is exact.

Pseudo-Coherent Sheaves

Def. (5.3.4.15) [Strictly Perfect Complexes of Modules]. Let \( (\mathcal{C}, \mathcal{O}) \) be a ringed site, a strictly perfect complex of \( \mathcal{O} \)-modules is a finite complex of \( \mathcal{O} \)-modules that each term is a direct summand of a finite free \( \mathcal{O} \)-module.

Def. (5.3.4.16) [Pseudo-Coherent Complexes of Modules]. Let \( (\mathcal{C}, \mathcal{O}) \) be a ringed site, then \( \mathcal{K} \in D(\mathcal{O}_X) \) is called an \( m \)-pseudo-coherent \( \mathcal{O}_X \)-module if for any \( U \in \mathcal{C} \), there exists a covering \( \{U_i \to U\} \) s.t. for any \( i \), there are strictly perfect object \( E_i \in D(\mathcal{O}_{U_i}) \) and a morphism \( E_i \to \mathcal{K}|_{U_i} \) that induces isomorphisms on \( H^i \) for \( i > m \) and surjection on \( H^m \).

\( \mathcal{K} \in D(R) \) is called a pseudo-coherent \( \mathcal{O}_X \)-module if it is \( m \)-pseudo-coherent for any \( m \).
Perfect Sheaves

Def.(5.3.4.17)[Perfect Complexes of Modules]. Let $(\mathcal{C}, \mathcal{O})$ be a ringed site, a perfect complex of $\mathcal{O}$-modules is an object $E$ in $D(\mathcal{O})$ that for any $U \in \mathcal{C}$ there is a covering $\{U_i \to U\}$ that $E|_{U_i}$ is can be represented by a strictly perfect complexes (5.3.4.15).

Prop.(5.3.4.18). Every mapping from a strictly perfect complex to an acyclic complex has a cover of open sets that on each open set the map is nullhomotopic.

Proof: This is true for a single direct summand of a finite free sheaf, and we can use induction to prove, Cf.[Sta]08C7.

Cor.(5.3.4.19). The strictly perfect complexes are fake "$K$-projective" objects in $K(\mathcal{O}_X)$. Note it is note technically $K$-projective, but it has all the properties of $K$-projective when proven, noticing the fact it is irrelevant when taken shifification.

Def.(5.3.4.20)[Perfect Sheaves]. Let $(\mathcal{C}, \mathcal{O})$ be a ringed site, an object $K^\bullet$ in $K(\mathcal{O})$ perfect if there is a covering $\mathcal{U}$ that on each $U_i$ there is a quasi-iso $K_i^\bullet \to K^\bullet|_{U_i}$ with $K_i^\bullet$ strictly perfect.

This is equivalent to $K^\bullet$ is locally represented by perfect objects in $D(\mathcal{O})$ by the fact that perfect object is fake $K$-projective.

Prop.(5.3.4.21). When $X$ is local ringed space, perfectness is equivalent to the fact that it is locally a finite free $\mathcal{O}_{U_i}$-module.

Proof: This is because direct summand of a finite free module is free, Cf.[Sta]0BCI.

Prop.(5.3.4.22)[Strictly Perfect Modules are “Acyclic” for $\text{Hom}^\bullet$]. If $(\mathcal{C}, \mathcal{O})$ is a ringed site and $\mathcal{E}^\bullet, \mathcal{F}^\bullet \in K(\mathcal{O})$, then $\mathcal{R}\text{Hom}(\mathcal{E}^\bullet, \mathcal{F}^\bullet)$ can be calculated directly by $\text{Hom}^\bullet(\mathcal{E}, \mathcal{F})$ in the following cases:

• $\mathcal{E}^\bullet$ is strictly perfect.
• $\mathcal{E}^\bullet \in D^-(\mathcal{O}_X), \mathcal{F}^\bullet \in D^+(\mathcal{O}_X)$, and each term $\mathcal{E}^n$ is a direct summand of a finite free $\mathcal{O}_X$-module.

Proof: Cf.[Sta]08I5, 08DM.

Prop.(5.3.4.23)[Duals]. Let $K$ be a perfect object in $D(\mathcal{O})$, then

• $K^\vee = \mathcal{R}\text{Hom}(K, \mathcal{O})$ is also a perfect object, and $(K^\vee)^\vee \cong K$.
• For any $M \in D(\mathcal{O})$, there are functorial isomorphisms

$$M \otimes^L K^\vee \cong \mathcal{R}\text{Hom}(K, M), \quad H^0(\mathcal{C}, M \otimes^L K^\vee) \cong \text{Hom}_{D(\mathcal{O})}(K, M).$$

Proof: Cf.[Sta]08JJ.

Def.(5.3.4.24)[Relative Perfect Modules]. Let $(X, \mathcal{O}_X) \to (S, \mathcal{O}_S)$ be a morphism of ringed sites that is flat and locally of f.p., then $E \in D(\mathcal{O}_X)$ is called a perfect object relative to $S$ if $E$ is pseudo-coherent and $E$ locally has finite tor dimension as an object in $D(f^{-1}\mathcal{O}_S)$. Cf.[Sta]08CG.

5 Topological Sheaves

References are [Sheaf Cohomology, Anonymous].

A topological space can be seen as a ringed site, so the theory of ringed sites applies to topological spaces.
5.3. COHOMOLOGY ON RINGED SITES

**Acyclic sheaves**

**Def. (5.3.5.1).** An Abelian sheaf on a paracompact Hausdorff topological space $X$ is called

- **soft** iff is and $\forall$ closed $V, \mathcal{F}(X) \to \mathcal{F}(V)$ is surjective. A flabby sheaf is soft.
- **fine** iff the sheaf of rings $\text{Hom}(\mathcal{F}, \mathcal{F})$ is soft.

Fine and soft are local properties (Use Zorn’s lemma to construct one-by-one).

**Prop. (5.3.5.2).** For a sheaf of unital rings over a paracompact Hausdorff space $X$, the following are equivalent,

1. it is a soft sheaf.
2. for any disjoint closed sets $V, W$, there is a section of $X$ that is 0 on $V$, and 1 on $W$.
3. it possesses a partition of unity.
4. it is a fine sheaf.

Note any soft sheaf possesses a partition of unity.

**Proof:** $1 \iff 2$ is easy and $1 \to 3$ is the to choose a closed locally finite subcover and use Zorn’s lemma to construct one-by-one. For $3 \to 1$, notice a closed section can extend to a slightly larger nbhd.

Because for a sheaf of rings $\mathcal{F}$, a partition of unity is equivalent to a partition of unity $\text{Hom}(\mathcal{F}, \mathcal{F})$, so $34$ are equivalent because $13$ are equivalent.

**Cor. (5.3.5.3).**

- Note that a fine sheaf possesses a decomposition of section because the previous proposition applies to $\text{Hom}(\mathcal{F}, \mathcal{F})$, and a partition of unity in $\text{Hom}(\mathcal{F}, \mathcal{F})$ yields a decomposition of section in $\mathcal{F}$. Thus a fine sheaf is soft. (extend to a small nbhd and use partition of unity).
- The sheaf of modules over a soft sheaf of rings is soft, by partition of unity.
- The continuous function sheaf on a paracompact Hausdorff space or the smooth function sheaf on a smooth manifold is fine, thus any smooth module is fine (Use bump function).

**Prop. (5.3.5.4).** Soft sheaf, e.g. fine sheaf is adapted to $\Gamma(X, -)$. (Similar as in (5.3.4.9), notice flabby is soft and the others are the same as before).

**Prop. (5.3.5.5).** Let $X$ be a locally compact space of finite compact dimension, when $S$ is a soft sheaf, and one of $S$ and $\mathcal{F}$ is flat, then $S \otimes_k \mathcal{F}$ is soft. Cf.[Cohomology of Sheaves Iversen P319].

**Prop. (5.3.5.6).** Over a locally compact space of finite dimension, any flat sheaf $\mathcal{F}$ on $X$ has a resolution of soft flat sheaves.

**Proof:** Cf.[Gelfand P232].

**Lemma (5.3.5.7).** A constant sheaf on an irreducible topological space is flabby, thus flask.

**Basics**

**Prop. (5.3.5.8).** If $i : Z \to X \in \text{Top}$ is a closed immersion, then for any $\mathcal{F} \in \mathcal{S}h(Z)$, $H^*(Z, \mathcal{F}) = H^*(Z, i_* \mathcal{F})$.

**Proof:** This is because $i_*$ is exact (5.2.6.7), so we can apply the Leray spectral sequence (5.3.1.10).
Comparison Theorems

**Prop. (5.3.5.9) [Singular].** For any locally contractible topological space $X$ and $G \in \mathcal{A}b$, there are canonical isomorphisms

$$H^*_\text{sing}(X, G) \cong H^*(X, G).$$

**Proof:** Shiffification of the singular cochain complex is a flabby presheaf resolution of $G$ because it is locally contractible, check on stalks. Then we only have to prove $C^\bullet(X) \to (C/V)^\bullet(X)$ is quasi-isomorphism, where $V$ is the presheaf of locally vanishing cochain. It suffice to prove $V^\bullet(X)$ is exact.

For any $i$-cocycle $\varphi$, for any $i-1$-complex $\sigma$, use barycentric subdivision, we can construct a $c_\sigma$ whose boundary is $\sigma$ and other simplexes on which $\phi$ vanishes, so we have the coboundary of $\eta : \sigma \to \varphi(c_\sigma)$ is $\varphi$. □

**Lemma (5.3.5.10) [Poincaré].** For a smooth manifold $X$ of dimension $n$, there is an exact sequence

$$0 \to \mathbb{R}^X \xrightarrow{d} \Omega^0 \xrightarrow{d} \Omega^1 \xrightarrow{d} \ldots \xrightarrow{d} \Omega^n \to 0$$

**Proof:** □

**Prop. (5.3.5.11) [DeRham].** For any smooth manifold $X$,

$$H^*_d\text{R}(X, \mathbb{R}^X) \cong H^*(X, \mathbb{R})$$

Where the right is constant sheaf cohomology.

**Proof:** Use the fact that smooth sheaf is fine so adapted to sheaf cohomology (5.3.5.4), and Poincaré lemma (5.3.5.10). □

**Prop. (5.3.5.12) [Period Maps].** For a smooth manifold $X$, by a similar method as (5.3.5.9), we can define a **differentiable singular cohomology** $H^*_{\text{sing,} \infty}(X)$, and prove a canonical isomorphism

$$H^*_{\text{sing,} \infty}(X, \mathbb{R}) \cong H^*(X, \mathbb{R}).$$

Then combining with (5.3.5.11), we get a canonical isomorphism

$$H^*_d\text{R}(X, \mathbb{R}^X) \cong H^*_{\text{sing,} \infty}(X, \mathbb{R})$$

which can be described as follows: there is a map of sheaves

$$\Omega^k \to C^*_\text{sing,} \infty(X)$$

that is locally defined to be $\omega \mapsto \sigma \mapsto \int_\sigma \omega$, then this map gives a map of complexes

$$\Omega^\bullet \to C^*_\text{sing,} \infty(X)$$

that induces the isomorphism.

**Proof:** ? Cf. [Warner, P206]. □

**Lemma (5.3.5.13) [\overline{\partial}-Poincaré Lemma].** If $X$ is a complex manifold of dimension $n$, there is an exact sequences:

$$0 \to \Omega^p_{\text{hol}} \xrightarrow{\overline{\partial}} \Omega^{p,1}_{\text{hol}} \xrightarrow{\overline{\partial}} \ldots \xrightarrow{\overline{\partial}} \Omega^{p,n-p}_{\text{hol}} \to 0$$
5.3. COHOMOLOGY ON RINGED SITES

Proof: Cf.[Sheaf Cohomology P21].

Cor. (5.3.5.14). If $X$ is a complex manifold of dimension $n$, there are exact sequences:

$$0 \to \mathbb{C}_X \xrightarrow{d} \mathcal{O}_X \xrightarrow{d} \Omega^1_{\text{hol}} \xrightarrow{d} \ldots \xrightarrow{d} \Omega^n_{\text{hol}} \to 0$$

Proof: This follows from the Poincare lemma (5.3.5.10) and $\bar{\partial}$-Poincare lemma (5.3.5.13), by applying the spectral sequence (I mean in the category of sheaves).

Prop.(5.3.5.15)[Holomorphic Cohomology]. For a complex manifold $X$,

$$H^p(X, \mathbb{C}) = H^p(X, \Omega^\bullet_{\text{hol}}).$$

Prop.(5.3.5.16)[Dolbeault]. For a complex bundle $\mathcal{E}$ on a complex manifold $X$,

$$H^{p,q}_\bar{\partial}(X, \mathcal{E}) \cong H^q(M, \Omega^p_{\text{hol}} \otimes \mathcal{O}_X \mathcal{E}),$$

where the left is Dolbeault cohomology and the right is sheaf cohomology. (Use the fact that smooth sheaf is fine so adapted to sheaf cohomology (5.3.5.4), and $\bar{\partial}$-Poincare lemma (5.3.5.13)).

Moreover, there is a spectral sequence of

$$E^1_{pq} = H^p_{\bar{\partial}}(X) \Rightarrow E^n = H^n_{\text{dR}}(X, \mathbb{R}) \times \mathbb{R} \mathbb{C}.$$

Prop.(5.3.5.17)[Cartan]. The class of Coh-Acyclic subsets of an analytic space is exactly the class of Stein manifolds.

Proof:

Prop.(5.3.5.18)[Čech and Sheaf Cohomology]. For a paracompact Hausdorff space $X$, there are isomorphisms

$$\check{H}^i(X, \mathbb{Z}) \cong H^i(X, \mathbb{Z}).$$

Proof: Cf.[Godement, Prop5.10.1].

Cohomology with Proper Support

References are [Cohomology of Sheaves Iversen].

Prop.(5.3.5.19). Soft sheaf is adapted to $f_!$ when $X, Y$ are locally compact. Cf.[Gelfand P226]. So we can use soft resolution to define $R^i f_!$, in particular, when $Y = \text{pt}$, we denote it by $H^i_c(X, \mathcal{F})$.

Using (5.2.6.2), we get the stalk of $R^i f_!(\mathcal{F})$ at $y$ is just $H^i_c(f^{-1}(y), \mathcal{F}|_{f^{-1}(y)})$.

Def.(5.3.5.20). The compact dimension of a locally compact topological space is the smallest $n$ that $H^i_c(X, \mathcal{F}) = 0$ for $i > n$. It is also the maximal length of minimal soft resolution.

$
\dim_c \mathbb{R}^n = n$, and when $Y$ is an open or closed subset of $X$, $\dim_c Y \leq \dim_c X$. $\dim_c$ is local in the sense if every point has a nbhd of dimension $\leq n$, then $\dim_c X \leq n$. Cf.[Iversen].

Prop.(5.3.5.21)[Proper Pushforward Commutes with Pullback]. For a pullback diagram

$$
x \times_Y Z \xrightarrow{\tau'} X \xrightarrow{\pi} X$$

we have $\tau^{-1}(\pi_! \mathcal{F}) = \pi'_!(\tau'^{-1} \mathcal{F})$.

Proof:
Cohomology on Noetherian Spaces

There are three basic objects, the derived functor for $f_*$ as an Abelian sheaf, $f_*$ as a $O_X$-module, $\Gamma(U,-)$ as an Abelian sheaf. Notice that an Abelian group is just a $\mathbb{Z}$-module.

**Prop.(5.3.5.22) [Grothendieck Vanishing].** The sheaf cohomology of an Abelian sheaf over a Noetherian topological space of dimension $n$ vanish for $k > n$.

**Proof:** Use (5.2.6.10) and (5.3.5.8) and long exact sequence, we can reduce to the case of $X$ irreducible. Then we induct on dimension. Notice first any sheaf is a filtered colimits of sheaf generated by f.m sections, thus we can use (5.3.1.15) to reduce to f.m sections case. And notice $\mathcal{F}_\alpha' \to \mathcal{F}_\alpha \to \mathcal{G}$, then $\mathcal{G}$ is generated by at most $|\alpha| - |\alpha'|$ elements, so reduce to the one section case.

Now it is a quotient sheaf of $\mathbb{Z}$, look at the kernel $R$. If the kernel is $d\mathbb{Z}$ at the generic pt, then $R|_V \cong \mathbb{Z}$ on some nbhd, and $R|_V/\mathbb{Z}$ supports on a lower dimension set, then we only need to consider the pushout of constant sheaf $\mathbb{Z}_U$.

Now there is an exact sequence $0 \to \mathbb{Z}_U \to \mathbb{Z} \to \mathbb{Z}_Y \to 0$ (5.2.6.10), $\mathbb{Z}$ is flabby (5.3.5.7) so flask, and the conclusion follows by induction.

Cf. [Sta]02UU. \qed

**Prop.(5.3.5.23).** For $f : X \to Y$, if $\mathcal{I}$ is an injective module on $X$, then $\check{H}^p(\{U_i \to U\}, f_*\mathcal{I}) = 0$ for every open cover for an open subset $U$ (5.3.4.8). This is because Čech cohomology is a derived functor. (Notice $f_*\mathcal{I}$ may not be injective when $f$ is not flat).

**Cor.(5.3.5.24) [Mayer-Vietoris].** For $X = U \cup V$, there is a long exact sequence

$$0 \to H^0(X,\mathcal{F}) \to H^0(U,\mathcal{F}) \otimes H^0(V,\mathcal{F}) \to H^0(U \cap V,\mathcal{F}) \to H^1(X,\mathcal{F}) \to \cdots$$

derived from the Čech to sheaf1 because it has only two column, just wrap out the definition.
5.4 Properties of Schemes

Main References are [Har77], [Sta], [?]nd [Tin20].

1 Basic Scheme Properties

Affine Local Properties of Schemes

Lemma (5.4.1.1) [Nike’s Trick]. In a scheme $X$ and $x \subset \text{Spec } A \cap \text{Spec } B$, $x$ has an open nbhd in $\text{Spec } A \cap \text{Spec } B$ that are distinguished in both $\text{Spec } A$ and $\text{Spec } B$.

Proof: Choose a nbhd of $x$ that is distinguished in $\text{Spec } A$ that is contained in $\text{Spec } A \cap \text{Spec } B$, then because distinguished of distinguished is distinguished, we may assume $i : \text{Spec } A \subset \text{Spec } B$. Now let $f \in B$ be an element that $D(f) \subset \text{Spec } A$, then I claim $D(i^\sharp(f)) = D(f)$, this will finish the proof, but this is equivalent to $i^{-1}(\text{Spec } B_f) = \text{Spec } A_{i^\sharp(f)}$, which is true for ideal-theoretical reason. □

Prop. (5.4.1.2) [Affine Communication Theorem]. A property $P$ of affine open subsets is called affine local if: $\text{Spec } (A)$ has $P$ $\Rightarrow$ all $\text{Spec } (A_f)$ has $P$, and any cover of $\text{Spec } (A_f)$ has $P$ $\Rightarrow$ $\text{Spec } (A)$ has $P$. Notice a stalk-wise property is obviously affine-local.

Now if we call $X$ has $\tilde{P}$ if $X = \bigcup_i \text{Spec } A_i$ that $A_i$ has $P$. Then the following is equivalent:

1. any open affine subscheme of $X$ has $P$.
2. any open subscheme of $X$ has $\tilde{P}$.
3. $X$ has a cover of open subschemes that has $\tilde{P}$.
4. $X$ has $\tilde{P}$.

Proof: $1 \rightarrow 2 \rightarrow 3 \rightarrow 4$ is obvious. It suffices to prove $4 \rightarrow 1$: if $X = \bigcup \text{Spec } A$, for any open affine subscheme of $X$, by (5.4.1.1), it can be covered by distinguished opens that are also distinguished in some $\text{Spec } A_i$, so by hypothesis it has $P$. □

Remark (5.4.1.3). When proving locality of morphism properties using affine communication theorem, one usually resort to Local Properties.

Prop. (5.4.1.4) [List of Stalkwise Properties]. All properties defined by a stalkwise ring-theoretic property that is stalkwise. (4.1.4.2)

Prop. (5.4.1.5) [List of properties affine local on the target]. (All the property besides the $H$-projectiveness is local on the target).

1. Because affineness is local on the target (5.1.5.26), all properties defined by a ring-theoretic property local on the target is local on the target (4.1.4.4).
2. All properties that is stalkwise.
3. All properties that satisfies faithfully flat descent (5.1.5.26)
4. Locally projective morphism.

Prop. (5.4.1.6) [List of properties affine local on the source]. (not complete)

1. All properties defined to be local ring map property local on the source (4.1.4.4)
2. Openness.

Proof:
1. Trivial.
2. Trivial.

Irreducible

Def. (5.4.1.7) [Irreducible Schemes]. A scheme is called irreducible if its underlying topological space is irreducible.

Prop. (5.4.1.8) [Nearly Affine Local]. For a scheme, the following are equivalent:
1. It is irreducible.
2. There is an affine cover $U_i$ of $X$ that $U_i$ are all irreducible and $U_i \cap U_j \neq \emptyset$.
3. Every affine open subset of $X$ is irreducible.

Proof: A scheme is sober (5.2.7.11), if $X$ is irreducible, then $X$ has a unique generic pt $\eta$ that $\{\eta\} = X$, then 2, 3 all holds. If 2 holds, then for a decomposition $X = Z_1 \cup Z_2$, any $U_i$ belongs to $Z_1$ or $Z_2$, so it is easy to see $Z_1 = X$ or $Z_2 = X$. If 3 holds, then choose an affine cover $U_i$ of $X$, then $U_i \cap U_j \neq \emptyset$, otherwise $U_i \coprod U_j$ is affine and not irreducible, contradiction, so 2 holds. □

Cor. (5.4.1.9). The fiber product of irreducible schemes is irreducible, because.

Reducedness

Def. (5.4.1.10) [Reduced Schemes]. A scheme is called reduced if $\mathcal{O}_X(U)$ is reduced for every open set $U$. Reduced is a stalk-wise property (5.4.1.5), it suffices to check reducedness at closed pts.

Prop. (5.4.1.11). For a reduced scheme $X$, $\Gamma(X, \mathcal{O}_X) \to \prod_{x \in X} k(x)$ is injective.

Prop. (5.4.1.12). If $X$ is locally Noetherian, the set of points with reduced stalk is open in $X$.

Proof: This set is just the set of points $x$ that $\mathcal{N}_x = 0$, where $\mathcal{N}$ is the sheaf of nilradicals, which is coherent, so it has closed supports (5.5.1.38). □

Prop. (5.4.1.13) [Reduction]. There is a $X_{\text{red}} \to X$ associated tot every scheme, it is $\text{Spec}(\mathcal{O}_X/\mathcal{N})$ where $\mathcal{N}$ is the sheaf of nilpotent elements. This construction is right adjoint to the forgetful functor by the adjoint property of $\text{Spec}(5.2.7.12)$. $X_{\text{red}} \to X$ is an closed immersion.

It’s useful to change to $X_{\text{red}}$ when the proposition only involve topology because $X_{\text{red}}$ has the same topology as $X$. A map can induce a map on their reduced structure.

Prop. (5.4.1.14) [Induced Reduced Scheme Structure]. Let $Z$ be a locally closed subset of a scheme $X$. There is a unique reduced subscheme $Z_{\text{red}}$ of $X$ with underlying topological space $Z$, called the induced reduced scheme structure of $Z$. It has the universal property that any morphism from a reduced scheme $Y$ to $X$ that has image in $Z$ factors through this subscheme (By virtue of reducedness).

In particular, there is a closed subscheme structure $X_{\text{red}}$ of $X$, called the underlying reduced subscheme of $X$.

Proof: The uniqueness is clear by the universal property. The existence is clear when $X$ is affine and $Z$ is closed in $X$. Then we can use the uniqueness to glue them to a global subscheme structure. □
Integral

Def. (5.4.1.15) [Integral Schemes]. A scheme $X$ is called integral if $\mathcal{O}_X(U)$ are all integral. This is equivalent to reduced and irreducible. So a scheme is integral iff there is an integral open affine cover that are pairwise-intersect (5.4.1.7).

The category of integral schemes is denoted by $\text{Sch}^{\text{int}}$.

Proof: If $X$ is irreducible and reduced, then so does any affine subscheme $\text{Spec} R$, so $R$ is integral as $(0)$ is the generic prime, because it has only one minimal prime consisting of nilpotent elements. Conversely, if $X$ is reduced, then any affine subscheme $\text{Spec} R$ is integral so reduced, and is irreducible by the presence of prime $(0)$. □

Cor. (5.4.1.16). The projective space over an integral scheme is integral. (Check the affine covers are dense). The projective space $\mathbb{P}_\mathbb{Z}^n$ is integral.

Prop. (5.4.1.17) [Integral is Almost Stalkwise]. Let $X$ be a non-empty and connected scheme, then $X$ is integral if all the

Def. (5.4.1.18) [Function Field]. Let $X$ be an integral scheme with generic point $\eta$, then $R(X) \cong \mathcal{O}_X,\eta$ is a field (5.2.8.2), called the function field of $X$, denoted by $K(A)$. Then any rational function on $X$ is defined on an open dense subset of $X$.

Prop. (5.4.1.19). If $X$ is an integral scheme and $Z_1, Z_2$ are closed subschemes of $X$ with generic points $\eta_1, \eta_2$, then $\mathcal{O}_{X,\eta_1} \not\subseteq \mathcal{O}_{X,\eta_2}$. In particular, if $Z = \{x\}$ consists of a closed point, then there is a rational function defined near $x$ that is not in $\mathcal{O}_{X,\eta_2}$.

Proof: [Sta]02NF. □

Noetherian

Def. (5.4.1.20) [Noetherian Scheme]. A scheme is called locally Noetherian if it can be covered by open affine schemes of noetherian rings. It is called Noetherian if moreover it is quasi-compact. (Locally)Noetherian is affine local (5.4.1.5).

Prop. (5.4.1.21) [Noetherian Scheme is Noetherian]. The underlying space of a Noetherian scheme is a Noetherian space.

Proof: By (3.8.3.3), we are reduced to the affine case. Now it is clear from the definition. □

Prop. (5.4.1.22). Any locally closed subscheme of a (locally)Noetherian scheme is (locally)Noetherian. In particular, an subset of a Noetherian scheme is quasi-compact.

Proof: This is because any localization and quotients of a Noetherian ring is Noetherian (4.1.1.40), and any subset of a Noetherian space is quasi-compact (3.8.3.2) (5.4.1.21). □

Prop. (5.4.1.23) [Finitely Many Irreducible Components]. For a closed subscheme in a locally Noetherian space, the collection of its irreducible components is locally finite in $X$, because a Noetherian space has f.m. irreducible components (3.8.3.4).

In particular, a locally Noetherian space is locally connected.

Prop. (5.4.1.24). Let $k'/k$ be a f.g. field extension, then a scheme $X$ over $k$ is locally Noetherian iff $X_{k'}$ is locally Noetherian.

Proof: Locally Noetherian is affine local, so the problem is totally ring-theoretic. If $X_{k'}$ is Noetherian, then so does $X$ by ff descent (4.4.2.1). If $X$ is Noetherian, then so does $X_{k'}$ by (4.1.1.44). □
Jacobson

Def. (5.4.1.25). An scheme is called Jacobson iff its underlying topological space is Jacobson (3.8.3.21). In particular, an affine scheme Spec $R$ is Jacobson iff $R$ is Jacobson (4.2.6.5).

So by (3.8.3.22), being Jacobson is a local property.

Prop. (5.4.1.26)[Locally Algebraic Scheme is Jacobson]. For a scheme locally algebraic over a field $k$, the set of closed points $X_0$ is dense in every closed subset of $X$, because it is a Jacobson space by (3.8.3.22) and (4.2.6.10). Equivalently, every locally closed subset of $X$ contains a closed point.

Moreover, the residue field of a closed point is finite over $k$ by (4.2.6.10), and the converse is also true. In particular, by (5.2.7.9), the closed points of $X$ are just the geometric points.

Proof: For the converse, because $k \subset A/p_x \subset k(x)$ are finite hence integral extensions, by (4.2.1.3) $A/p_x$ is a field, thus $x$ is a closed point. □

Cor. (5.4.1.27) [Algebraic Scheme Preserves Closed Points]. A morphism between algebraic schemes over a field $k$ maps closed points to closed points.

Remark (5.4.1.28). When $X$ is geo.reduced, a stronger statement shows the set of separable closed points of $X$ is dense in $X$, Cf. (5.4.3.3).

Cor. (5.4.1.29) [Check Surjectiveness on Closed Points]. If a morphism of locally algebraic schemes over a field $k$ is surjective on closed points, then it is surjective.

Proof: By Chevalley theorem (5.6.1.5), the image is a locally constructible set, thus the supplement set is also locally constructible. Now if it is not surjective, then there is an open closed subset $U \cap Z$ not in the image. But this set contains a closed point by (5.4.1.26), which is a contradiction. □

Cohen-Macaulay

Def. (5.4.1.30) [Cohen-Macaulay Schemes]. A Cohen-Macaulay scheme of a C.M. scheme is a scheme $X \in \text{Sch}$ s.t. all its stalks is C.M. local. Thus being C.M. is a stalkwise property.

Catenary Schemes

Def. (5.4.1.31) [Catenary Schemes]. A catenary scheme is a scheme that its underlying space is catenary. A scheme $S$ is called universally catenary if $S$ is locally Noetherian and every scheme locally of f.t. over $S$ is catenary.

(Universally) catenary is a stalkwise property, by (4.1.4.2).

Prop. (5.4.1.32) [Catenary and Dimension Functions]. Let $X \in \text{Sch}$ be locally Noetherian, then $X$ is catenary iff locally around every point there is a dimension function, by (3.8.3.39).

Example (5.4.1.33) [Universally Catenary Schemes]. The following are some examples of universally catenary schemes, by (4.2.4.7).

- A scheme locally of f.t. over a universally catenary scheme.
- A C.M. scheme.
- Spectrum of a 1-dimensional Noetherian domains,
- Spectrum of a fields.
5.4. PROPERTIES OF SCHEMES

Japanese & Nagata Schemes

Def. (5.4.1.34) [Japanese & Nagata Schemes]. A (universally) Japanese scheme is a scheme that can be covered by open affine spectrum of (universally) Japanese rings (4.3.8.1). A Nagata scheme is a scheme that can be covered by open affine spectrum of Nagata rings (4.3.8.1).

Prop. (5.4.1.35). Being (universally) Japanese or Nagata is a local property, and are stable under taking open subschemes, by (4.3.8.1).

Prop. (5.4.1.36). Let $X$ be a locally Noetherian scheme, then $X$ is Nagata iff every integral closed subscheme $Z$ of $X$ is Japanese.

Proof: One direction is clear. If every integral closed subscheme $Z$ of $X$ is Japanese, let $U = \text{Spec } A \subset X$ be an affine open subscheme and $Z = V(p) \subset U$, we need to show $A/p$ is Japanese. Consider $Z$ with the reduced induced structure is an integral closed subscheme of $X$ and $Z$ is an open subscheme of $Z$, thus $Z$ is Japanese and so is $Z$ by (5.4.1.34). □

2 Normal & Regular

Def. (5.4.2.1) [Normal & Regular Schemes]. A scheme is called normal if all its stalks are normal domains (4.3.5.1), or equivalently all its affine sections are normal rings. In particular, a normal scheme is reduced.

A locally Noetherian scheme is called regular iff all its stalk are regular local rings (4.3.5.17), i.e. all affine opens are regular rings. Regular only have to be checked at close pt by (4.3.5.17).

Def. (5.4.2.2). Let $X$ be a locally Noetherian scheme, the points $x$ that $\mathcal{O}_{X,x}$ is a regular local ring is called the regular locus of $X$, and the complement of the regular locus is called the singular locus of $X$.

Prop. (5.4.2.3) [Noetherian and Integral]. Let $X$ be a locally Noetherian scheme, then $X$ is normal iff it is a disjoint union of integral normal schemes.

Proof: It suffices to show that a connected locally Noetherian scheme is integral. Thus it suffices to show it is irreducible. Suppose there are several irreducible components, and let $p$ be a intersection point, then we may assume $X$ is affine, then this follows from (4.3.5.4). □

Cor. (5.4.2.4). A normal scheme is integral iff it is connected.

Prop. (5.4.2.5). If $X$ is an integral normal scheme, then $\Gamma(X, \mathcal{O}_X)$ is a normal ring.

Proof: If $X$ is integral, then $R = \Gamma(X, \mathcal{O}_X)$ is integral. If $f = a/b \in K(R)$ that is integral over $R$, then for any affine open $U \subset X$, $b|_U$ is non-zero as $X$ is integral, thus $f|_U$ is integral over $\mathcal{O}_X(U)$ thus $f|_U \in \mathcal{O}_X(U)$, thus $f \in R$. □

Prop. (5.4.2.6) [Normalization]. For an integral scheme $X$, there is a $X_{\text{nom}} \rightarrow X$ which is $\text{Spec}(\mathcal{O}_{X,\text{nom}})$, any dominant morphism $f$ from a normal integral scheme to $X$ will factor through $X_{\text{nom}}$. (Use the adjointness for $\text{Spec}$ and notice $f$ maps generic to generic).

Proof: □

Prop. (5.4.2.7) [Normalization is not flat]. Non-trivial normalization is never flat.
Proof: Use (5.6.2.6). □

Prop. (5.4.2.8) [Regular and Normal]. Regular scheme is C.M and locally factorial, hence normal, by (4.3.5.21) and (4.3.5.19). A Normal scheme is regular in codimension 1, by (4.3.5.32).

Cor. (5.4.2.9). A regular connected scheme $X$ is irreducible, by (5.4.2.4).

Prop. (5.4.2.10). For a locally Noetherian scheme of dimension $\leq 1$, normal is equivalent to regular, by (10.3.3.4).

**Factorial Schemes**

Def. (5.4.2.11) [Factorial Schemes]. A factorial scheme is a scheme that all the local rings are UFD.

Prop. (5.4.2.12). If $A$ is a UFD, then $\text{Spec } A$ is factorial.

**Dedekind Scheme**

Def. (5.4.2.13) [Dedekind Scheme]. A Dedekind scheme is an integral Noetherian normal scheme of dimension 1.

Prop. (5.4.2.14). Let $X$ be a Dedekind scheme and $x \in X$ is a closed pt, let $\hat{X} = \text{Spec} (\hat{O}_{X,x}) \rightarrow X$ be the completion of $X$ at $x$, then there is a pullback of categories:

$$
\begin{array}{ccc}
\text{Bun}_X & \rightarrow & \text{Bun}_{X \setminus \{x\}} \\
\downarrow & & \downarrow \\
\text{Bun}_{\hat{X}} & \rightarrow & \text{Bun}_{\hat{X} \setminus \{x\}}
\end{array}
$$

Proof: We may study locally near $x$, then we can assume that $X$ is affine. Now shrink $X$ even more, we can assume that $x$ is defined by a single $f \in A$ (localized at the maximal ideal defined by $x$), then we finish by (4.4.2.12). □

3 Geometrical properties

Def. (5.4.3.1) [Geometric Properties over Fields].

- A scheme $X$ is called geometrically integral/reduced/separated/irreducible... over a field $k$ iff for any field extension $k'/k$, $X_{k'}$ is integral/reduced/separated/....

- A locally Noetherian scheme is called geometrically regular iff for any f.g. field extension $K/k$, $X_K$ is regular. It is stalkwise by (5.4.3.18).

**Geo.reducedness**

Prop. (5.4.3.2) [Geo.Reduced]. For a scheme $X$ over a field $k$, the following are equivalent:

1. $X$ is geometrically reduced.
2. For every reduced $k$-scheme $Y$, the product $X \otimes_k Y$ is reduced.
3. All stalks are geometrically reduced ring.
4. $X$ is reduced and for every maximal point $\eta$ of $X$, the residue field $k(\eta)$ is separable over $k$.
5. $X_{\text{geo}}$ is reduced.
6. $X_K$ is reduced for every finite purely inseparable field extension $K/k$.
7. $X_{K^{1/p}}$ is reduced.

In particular, if $k$ has characteristic 0, then geo.reduced $\iff$ reduced.

Proof: As reduced is local, these all follows from (4.3.6.2).

Prop.(5.4.3.3) [Geo.Reduced and Arithmetic Points]. Let $X$ be a locally algebraic geo.reduced scheme over a field $k$, then the set of closed points with finite separable field extensions $k(x)/k$ is dense in $X$.

Proof: Combine (5.6.4.19) and (5.6.4.21).

Def.(5.4.3.4) [Density of Points]. Let $X$ be an algebraic scheme over a field $k$, and $k'/k$ be a field extension, then a subset $S \subset X(k')$ is said to be schematically dense in $X$ if the only closed subscheme $Z \subset X$ over $k$ that $S \subset Z(k')$ is $X$ itself.

? Should merge with the definition of scheme-theoretical image.

Prop.(5.4.3.5) [Schematically Dense Subset]. Let $X$ be an algebraic scheme over a field $k$, $S \subset X(k)$ be a subset. Then the following are equivalent:
1. $S$ is schematically dense in $X$.
2. $X$ is reduced and $S$ is dense in $|X|$.
3. The family of homomorphisms $O_X \to k : f \mapsto f(s)$ is jointly injective.

Proof: 1 $\to$ 2: Let $\overline{S}$ be the induced reduced structure of the closure $S$ in $X(5.4.1.14)$, then $\overline{S} = X$, so $X$ is reduced with $X = \overline{S}$.

2 $\to$ 3: ? Cf.[Milne Algebraic Groups, P10].

Cor.(5.4.3.6). A schematically dense subset remains schematically dense after field base changes.

Cor.(5.4.3.7). The schematic closure of a subset commutes with base change.

Proof: Use the third definition in (5.4.3.5), notice that the valuation maps are also jointly injective because $k'/k$ is flat.

Cor.(5.4.3.8). If $X$ admits a schematically dense subset $S$, then $X$ is geo.reduced.

Prop.(5.4.3.9). If $X(k')$ is dense in $X$, then $X$ is reduced. Conversely, if $X(k')$ is dense in $|X_{k'}|$ and $X$ is geo.reduced, then $X(k')$ is dense in $X$.

Proof: $X$ is reduced because $X_{\text{red}}(k') = X(k')$. Conversely if $Z \subset X$ is a closed subscheme that $Z(k') = X(k')$, then $|Z_{k'}| = |X_{k'}|$ by condition, and then $Z_{k'} = X_{k'}$ as $X_{k'}$ is reduced. Thus $Z = X$ by flatness.

Cor.(5.4.3.10) [Geometric Points Schematically Dense]. If $X$ is locally algebraic and geo.reduced, then $X(k')$ is schematically dense in $X$ for any separably closed field $k'$ containing $k$. 
Proof: \( X(k') \) is dense in \( |X_{k'}| \) by (5.4.3.3), thus it is schematically dense in \( X \) by the proposition. □

Cor. (5.4.3.11). If \( Z, Z' \) are closed subvarieties of a locally algebraic algebraic scheme \( X \) over \( k \) that \( Z(k') = Z'(k') \subset X(k') \) for some separably closed field \( k' \) containing \( k \), then \( Z = Z' \). In other words, a closed subvariety of \( X \) is determined by the subset \( Z(k^s) \subset X(k^s) \).

\[ \text{Proof:} \quad \text{The closed subscheme } Z \cap Z' \text{ satisfies } Z \cap Z'(k') = Z(k'), \text{ so } Z \cap Z' = Z \text{ by (5.4.3.10).} \]

Similarly, \( Z \cap Z' = Z' \).

Geo. Connected and Geo. Irreducible

Prop. (5.4.3.12)[Geo. Connectedness]. For a scheme \( X \) over a field \( k \), the following are equivalent:

- For every connected \( k \)-scheme \( Y \), the product \( X \otimes_k Y \) is connected.
- \( X \) is geometrically connected.
- \( X_{K^s} \) is connected.
- \( X_K \) is connected for any finite separable extension \( K/k \).

\[ \text{Proof:} \quad \text{Cf. [Sta]0385, 0389.} \]

Prop. (5.4.3.13)[Invariance of Base Change]. Let \( X \) be a scheme over a field \( k \) and \( k'/k \) a field extension, then \( X \) is geo. connected iff \( X_{k'} \) is geo. connected.

\[ \text{Proof:} \quad \text{Cf. [Sta]054N.} \]

Prop. (5.4.3.14). Let \( T \to X \) be a map of schemes over a field \( k \), if \( T \) is geo. connected and \( X \) is connected, then \( X \) is geo. connected.

\[ \text{Proof:} \quad \text{Cf. [Sta]056R.} \]

Cor. (5.4.3.15)[Connected with a Rational Point]. Let \( X \) be a scheme over a field \( k \). Assume \( X \) is connected and has a point \( x \) that \( k \) is alg. closed in \( k(x) \), then \( X \) is geo. connected. In particular, if \( X \) is connected and has a rational point, then \( X \) is geo. connected.

\[ \text{Proof:} \quad \text{Cf. [Sta]04KV.} \]

Prop. (5.4.3.16)[Geometrically Irreducible]. For a scheme \( X \) over a field \( k \), the following are equivalent:

- For every irreducible \( k \)-scheme \( Y \), the product \( X \otimes_k Y \) is irreducible.
- \( X \) is geometrically irreducible.
- \( X_{K^s} \) is irreducible.
- \( X \) is irreducible and if \( \eta \) is the generic pt of \( X \), then \( k \) is separably closed in \( k(\eta) \).
- \( X_K \) is irreducible for any finite separable extension \( K/k \).

\[ \text{Proof:} \quad \text{Cf. [Gortz P136].} \]

□
Geo.Integral

Cor. (5.4.3.17)[geometrically Integral]. For a scheme $X$ over a field $k$, the following are equivalent:

- For every integral $k$-scheme $Y$, the product $X \otimes_k Y$ is integral.
- $X$ is geometrically integral.
- $X_K$ is irreducible for any finite extension $K/k$.
- $X_k$ is integral.
- $X$ is integral and if $\eta$ is the generic pt of $X$, then $k$ is alg. closed in $k(\eta)$ and $k(\eta)/k$ is separable.

Proof: $1 \to 2 \to 3 \to 4$ is easy, Cf.[Gortz P136]. □

Geometrically Regular

Prop. (5.4.3.18). Let $X$ be a locally Noetherian scheme over a field $k$, then $X$ is geometrically regular iff the local ring $\mathcal{O}_{X,x}$ is geometrically regular over $k$. Thus it suffice to check for finite purely inseparable field extensions $k'/k$, by(4.3.6.6).

Proof: For a finite purely inseparable field extension, $\mathcal{O}_{X,x} \otimes_k k'$ is also a local ring because their spectra are the same(4.1.7.26), so $\mathcal{O}_{X,x}$ is geometrically regular by(4.3.6.6).

Conversely, if $\mathcal{O}_{X,x}$ is geo.regular, then for any field extension $k'/k$, stalks of $X_{k'}$ are localization of $\mathcal{O}_{X,x} \otimes_k k'$, so it is regular by(4.3.5.17). □

Cor. (5.4.3.19). A geometrically regular ring is geometrically reduced, by(4.3.5.19) and(5.4.3.2).

Prop. (5.4.3.20)[Partially Invariance Under Base Change]. If $k'/k$ is a f.g. field extension, then $X_{k'}$ is geo.regular over $k'$ iff $X_k$ is geo.regular over $k$.

In fact, this is true for any field extension $k'/k$ if $X$ is locally algebraic over $k$, because in this case geo.regular is equivalent to smoothness.

Proof: One direction is trivial, for the other, Cf.[Sta]038W?. □

4 Basic Morphism Properties

Main references are [Sta]02WE.

Base Change Trick

Prop. (5.4.4.1)[Base Change Trick]. If a property $P$ of morphisms satisfy:

- Closed immersion has $P$.
- Stable under base change and composition.

Then

- it is stable under product.
- $g \circ f : X \to Y \to Z$ has $P$ and $g$ separated implies $f$ has $P$.
- it is stable under $f_{red}$. (Notice $X_{red} \to X$ is closed immersion).
Proof: For the product, we may assume one of them is identity and use composition, but then the product is just base change, so it has \( P \).

For the second, factorize \( f : X \rightarrow X \times_Z Y \rightarrow Y \), the first is base change of \( \Delta : Y \rightarrow Y \times_Z Y \), so it satisfies \( P \) because \( g \) is separable, and the second map is a base change of \( X \rightarrow Z \), so it satisfies \( P \), so \( f \) satisfies \( P \).

\( X_{\text{red}} \rightarrow X \rightarrow Y = X_{\text{red}} \rightarrow Y_{\text{red}} \rightarrow Y \) has \( P \) because \( X_{\text{red}} \rightarrow X \) is closed immersion, and \( Y_{\text{red}} \rightarrow Y \) is separable because closed immersion is separable (checked directly), so by what has been proved, \( X_{\text{red}} \rightarrow Y_{\text{red}} \) has \( P \). \( \square \)

Prop. (5.4.4.2). Lists of properties satisfying the base change trick (5.4.4.1) (not complete):
1. Universal closed/universal injective morphisms.
2. Affineness.
3. Morphisms (locally) of finite type.
4. Finite Morphisms.
5. Integral Morphisms.
6. Morphisms (locally) of finite presentation.
7. Quasi-affine morphisms.
8. Closed Immersions.
10. (Quasi-)Separatedness.
11. Proper.
12. Unramified.
14. (Locally) Quasi-finiteness.
15. H-projectiveness.

Proof:
1. Trivial.
2. Because affineness is local on the target (5.4.1.5), this follows from (5.2.7.17) and (5.2.7.14).
3. Trivial.
4. Trivial.
5. 

6. By (4.3.7.9).
7. Affine morphism is quasi-compact: because quasi-compactness is local on the target, we can reduced to the affine case, thus it is quasi-compact, by (5.4.4.26). To show a base change of quasi-compact morphism is quasi-compact, because quasi-compactness is local on the target (5.4.1.5), then we can choose a cover by affine opens that the image is contained in an affine open, thus it reduces to show a map between affine schemes is quasi-compact, which is (5.4.4.26).
8. For closed immersions, use (5.2.7.16) and check locally, for open immersions, use (5.2.7.16).

9. It suffices to show an affine map is quasi-compact.

10. Closed immersion is separated is checked directly. Composition: For \( X \to Y \to Z \), the diagonal map decomposes as \( X \to X \times_Y X \to X \times_Z X \), the second one is closed immersion (or quasi-compact) by (5.4.4.78), so this follows from that of closed immersion and qc. Base change: The diagonal commutes with base change (3.1.1.48), so this follows from that of closed immersion and qc.

11. Because universally closed, f.t. and separatedness both do (5.4.4.2).

12.

13.

14. □

**Injectivity and Monomorphisms**

**Def.(5.4.4.3)** [Injectivity and Monomorphisms]. A morphism of schemes is called **injective** if it is injective topologically. A morphism of schemes is called a monomorphism if it is a monomorphism in the category of schemes.

**Prop.(5.4.4.4)** [Universally Injective]. For a morphism of schemes \( X \to S \), the following are equivalent:

- It is universally injective.
- It is injective and the residue field extension are all purely inseparable.
- The diagonal map is surjective.
- For any field \( K \), \( \text{Hom}(\text{Spec} \, K, X) \to \text{Hom}(\text{Spec} \, K, S) \) is injective.

In particular, any monomorphism is universally injective.

**Proof:**

1 \to 4: For \( s \in \text{Hom}(\text{Spec} \, K, S) \), a \( x \in \text{Hom}(\text{Spec} \, K, X) \) mapping to \( s \) is a section of the injective map \( X \times_S \text{Spec} \, K \to \text{Spec} \, K \), which is unique if it exists.

4 \to 1: If \( S' \to S \) is a morphism, \( X' = X \times_S S' \), and \( x, x' \in X' \) map to the same point \( s' \in S' \), then we can choose a common field extension \( K/k(s') \) of \( k(x)/k(s) \) and \( k(x')/k(s) \). Then we get two elements in \( \text{Hom}(\text{Spec} \, K, X') \), and the hypothesis says they map to the same element in \( \text{Hom}(\text{Spec} \, K, X) \). Thus they are the same, as \( X' \) is the fiber product.

1 \to 2: It the residue field extension is not purely inseparable, then tensoring with this field extension, we get two points mapping to the same, contradiction.

2 \to 4: It the residue field extension is purely inseparable, then \( k(x) \to K \) is determined by the composition, \( k(s) \to k(x) \to K \), which means 4 is true.

1 \to 3: If \( X \to S \) is universally injective, then \( X \times_S X \to X \) is injective, and \( \Delta_{X/S} \) is a section of this map, thus it must be surjective.

3 \to 1: If \( \Delta_{X/S} \) is surjective, then for any base change \( S' \to S \), \( \Delta_{X'/S'} \) is surjective, thus \( X' \to S' \) is injective, thus 1 holds. □

**Prop.(5.4.4.5)** [Monomorphism and Injectivity]. A morphism of schemes \( j : X \to Y \) is a monomorphism if \( j \) is an injective map and for any \( x \in X \), \( \mathcal{O}_{Y,j(x)} \to \mathcal{O}_{X,x} \) is surjective.
Proof: First check topologically, then check the local ring map. □

Cor. (5.4.4.6). For any scheme $X$ and a point $x$, $\text{Spec} \mathcal{O}_{X,x} \to X$ is a monomorphism.

Closed Map

Prop. (5.4.4.7) [Universal Closed]. Universal closedness is local on the basis and satisfies the base change trick (5.4.4.2).

Prop. (5.4.4.8). If $g$ is surjective, then $f \circ g$ is universally closed iff $f$ is universally closed (because surjective is S.u.B).

Prop. (5.4.4.9) [Closed Map and Specialization]. The image of a quasi-compact morphism is closed iff it is stable under specialization. And it is a closed map iff specializations lift along $f$.

Proof: For the first, the question is local, so reduce to $Y$ affine, and then $X$ is qc $= \bigcup U_i$, then we can replace $X$ by an affine $\bigcap U_i$, then reduce to the affine case (4.1.7.14).

For the second, for any closed subset of $X$ with its induced reduced structure, the restriction to it is still qc and specialization lifts, so we prove the image is closed. Now the image is stable under specialization, so the result follows from the first assertion. □

Affine Map

Prop. (5.4.4.10). $X$ is affine if there is a finite set of elements $f_i \in \Gamma(X, \mathcal{O}_X)$ that generate the unit ideal and $X_{f_i}$ is affine.

Proof: First prove that $X_{f_i} \cap X_{f_j} = X_{f_if_j}$ is affine because affine intersect $X_{f_i}$ is affine. Second, prove $\Gamma(X_f, \mathcal{O}_X) = \Gamma(X, \mathcal{O}_X)_f$, finally glue them to get a map $X \to \text{Spec}(A)$ and use the fact isomorphism is local on the target (5.4.4.5). $X$ is affine scheme if $X \to \text{Spec}(\Gamma(X))$ is affine. □

Cor. (5.4.4.11). Affineness is affine local on the target, and it satisfies the base change trick (5.4.4.2).

Lemma (5.4.4.12) [Serre Criterion of Affineness].

- A qc scheme $X$ is isomorphic to an affine scheme iff $H^1(X, \mathcal{I}) = 0$ for every Qco sheaf of ideals $\mathcal{I}$.

- If $X$ is qcqs, then it suffices to show $H^1(X, \mathcal{I}) = 0$ for every Qco sheaf of ideals $\mathcal{I}$ of f.t..

- If $f : X \to Y$ is a quasi-compact morphism between quasi-separated schemes, then $f$ is affine iff for any Qco sheaf of ideals $\mathcal{I}$ on $X$, $R^1f_*\mathcal{I} = 0$.

Proof: Cf. [Sta]01XF.

The case of affine scheme is proven by (5.7.1.1) and (5.7.1.2). The converse: For every point $p$, choose an open affine nbhd $U$, let $Y = X - U$, by the exact sequence

$$0 \to \mathcal{I}_{Y \cup \{p\}} \to \mathcal{I}_Y \to k(P) \to 0,$$

we have a surjective map $\Gamma(X, \mathcal{I}_Y) \to \Gamma(X, k(P))$ thus there is a $f \in A = \Gamma(X, \mathcal{O}_X)$ that $P \in X_f \subset U$ is affine. So using (5.4.4.10), we only have to show that for f.m $f_i$, they generate $\Gamma(X, \mathcal{O}_X)$. This is by considering the kernel $F$ of $\mathcal{O}_X^* \to \mathcal{O}_X : (a_1, \ldots, a_r) \to \sum f_ia_i$, and there is a filtration on $F$, the quotient of which are all coherent sheaves because kernel and cokernel are Qco, and there by induction and hypothesis, $H^1(X, F) = 0$, thus the result.
2: In the qcqs case, by (5.7.1.5), we can use filtered colimit to show that \( H^1(X, \mathcal{I}) = 0 \) for any Qco sheaf of ideals.

3: For any affine open \( U \) of \( Y \), the inclusion \( U \to Y \) is qc, thus \( f^{-1}(U) \to X \) is also qc. Now any Qco sheaf of ideals \( \mathcal{I} \) on \( U \) extends to a Qco sheaf of ideals on \( X \) by (5.5.1.8), then we can use Leray spectral sequence to conclude that \( H^1(f^{-1}(U), \mathcal{I}) = 0 \), so \( f^{-1}(U) \) is affine.

\[ \square \]

**Cor. (5.4.4.13).** For a Noetherian scheme \( X \), \( X \) is affine iff \( X_{\text{red}} \) is affine.

**Proof:** The canonical exact sequence (5.2.6.10) reads: \( 0 \to N \mathcal{F} \to \mathcal{F} \to i_* i^* \mathcal{F} \to 0 \), so iff \( X_{\text{red}} \) is affine, then we have \( H^i(\mathcal{F}) \cong H^i(N \mathcal{F}) \), and notice \( N^k = 0 \) for some \( k \).

\[ \square \]

**Cor. (5.4.4.14).** For a Noetherian reduced scheme \( X \), \( X \) is affine iff each irreducible component is affine. (The same as the above, notice that \( \prod p_i = 0 \), for the minimal primes of \( A \)). (The reducedness can be dropped by the last proposition).

**Lemma (5.4.4.15).** If a morphism \( X \to Y \) is a homeomorphism onto a closed subset of \( Y \), then \( f \) is affine.

**Proof:** Cf. [Sta]04DE.

**Quasi-affine**

**Def. (5.4.4.16)[Quasi-Affine Morphism].** A scheme is called quasi-affine iff it is isomorphic to a qc open subscheme of an affine scheme. A morphism is called quasi-affine iff the inverse of any affine scheme is quasi-affine.

**Prop. (5.4.4.17).** Quasi-affine is local on the target and satisfies the base change trick.

**Proof:** Cf. [Sta]01SN.

\[ \square \]

**Prop. (5.4.4.18).** Any qc immersion \( i \) of a quasi-affine scheme is quasi-affine.

**Proof:** As \( i \) is qc, \( i \) factors through a map \( Z \to U \to X \), where \( U \) is a quasi-compact open subset of \( X \). Thus it suffices to consider the closed immersion case, which is clear.

\[ \square \]

**Prop. (5.4.4.19).** A morphism \( f : X \to S \) is quasi-affine iff \( \mathcal{O}_X \) is \( f \)-ample. In particular, A scheme is quasi-affine iff \( \mathcal{O}_X \) is ample.

**Proof:** Cf. [Sta]01QE.

\[ \square \]

**Cor. (5.4.4.20).** Let \( X \) be a quasi-affine scheme and \( H^p(X, \mathcal{O}_X) = 0 \) for \( p > 0 \), then \( X \) is affine.

**Proof:** By (5.4.4.19) \( \mathcal{O}_X \) is ample, then by (5.5.4.18), \( X \) is affine.

\[ \square \]

**Prop. (5.4.4.21)[Descent].** Let \( X \) be a scheme over a field \( k \) and \( K/k \) be a field extension, then \( X \) is quasi-affine iff \( X_K \) is quasi-affine.

**Proof:** Cf. [Sta]0BDD.
Dominant

**Prop. (5.4.4.22).** Let \( f : X \to S \) be a map of schemes.
- If every generic point of irreducible components of \( S \) is in the image of \( f \), then \( f \) is dominant.
- If \( f \) is quasi-compact, then the converse is also true. More precisely, if a generic point \( \eta \) is not in the image, then it is not in the closure of the image.
- If \( X \) has only f.m. irreducible component, then the converse is also true.

**Proof:** Cf.[Sta]Chap28.8.

**Prop. (5.4.4.23)[Dominant Map between Integral Schemes].** If \( f : X \to S \) is a map between integral schemes, then the following are equivalent:
- \( f \) is dominant.
- \( f(\eta_X) = \eta_Y \).
- for some(all) affine open subset \( U \subset X, V \subset Y \) with \( f(U) \subset V \), the ring map \( O_Y(V) \to O_X(U) \) is injective.
- for some(all) \( x \in X \), the local ring map \( O_{Y,f(x)} \to O_{X,x} \) is injective.

**Proof:** Cf.[Sta]0CC1.

**Def. (5.4.4.24)[Dominant Rational Maps].** A rational map between irreducible schemes is called a **dominant map** if it maps the generic point to the generic point.

Quasi-Compact

**Prop. (5.4.4.25)[Quasi-Compact Morphism].** A morphism \( f : X \to S \) of schemes is quasi-compact iff the inverse image of any quasi-compact open subsets is quasi-compact, because affine opens form a basis of \( X \).

**Prop. (5.4.4.26).** A map between affine schemes is quasi-compact.

**Proof:** Because quasi-compactness is local on the target(5.4.1.5), it suffices to show the inverse image of a distinguished open subset is quasi-compact, and this is true.

**Prop. (5.4.4.27).** Let \( f : X \to Y, g : Y \to Z \). If \( g \circ f \) is quasi-compact and \( g \) is qs, then \( f \) is qc.

**Proof:** Factor it through \( X \to X \times_Z Y \to Y \). The second map is a base change of \( X \to Z \) hence qc, the first map is a section of \( X \times_Z Y \to X \), which is a base change of \( Y \to Z \), hence qs, so by(14.5.3.19), the first map is also qc.

**Prop. (5.4.4.28).** Any map between Noetherian schemes is quasi-compact, by(5.4.1.22).

Finite Type

**Def. (5.4.4.29)[Morphisms of Finite Type].** A morphism \( f : X \to S \) is called of **locally of finite type** if for there exists an affine open cover \( \{\text{Spec}(B_i)\} \) of \( S \) that \( f^{-1}(U_i) \) has an affine open cover of spec of finite generated \( B_i \)-algebras. It is called **finite type** if moreover it is quasi-compact.
5.4. PROPERTIES OF SCHEMES

Let \( k \in \text{Field} \), then \( S \in \text{Sch} / k \) is called (locally) algebraic iff \( S \) is (locally) of finite type over \( \text{Spec} \ k \).

For \( S \in \text{Sch} \), denote \( \text{Sch}_{\text{loc.ft}} / S(\text{Sch}^{\text{ft}} / S) \) the full subcategory of \( \text{Sch} / S \) consisting of (locally) of finite type schemes over \( S \).

(Locally) Finite type is affine local on the target and on the source, and satisfies the base change trick (5.4.4.2).

Prop. (5.4.4.30) [Closed Subschemes Descending Chain Stablizes]. The closed subschemes of an algebraic scheme \( X \) over a field \( k \) satisfy the descending chain condition.

Proof: As \( X \) is Noetherian, the topological chain \( |Z_1| \supset |Z_2| \supset \ldots \) stabilizes, so we may assume \( |X| = |Z_1| = |Z_2| = \ldots \). Now choose a finite affine cover \( \text{Spec} \ A_i \) of \( X \), then \( Z_i \) corresponds to ideals \( I_i \) of \( A_i \), so they stabilize, as \( A_i \) are Noetherian.

Cor. (5.4.4.31). Arbitrary intersection of closed subschemes of an algebraic scheme \( X \) is well-defined.

Prop. (5.4.4.32) [Algebraic Schemes of Dimension 0]. Let \( X \) be a locally algebraic variety over a field \( k \) of dimension 0, then \( X \) is a disjoint union of f.d. local Artinian \( k \)-algebras.

Proof: Cf. [Sta]06LH.

Prop. (5.4.4.33) [Dimensions for Locally Algebraic \( k \)-Schemes]. Let \( k \) be a field and \( X \) is a locally algebraic \( k \)-scheme.

if \( X \) is irreducible, then \( \dim X = \dim U \) for any nonempty open \( U \subset X \).

Proof: It suffices to show any two affine open subsets \( U, U' \) of \( X \) have the same dimension, then use (3.8.3.26). Now \( U \cap U' \neq \emptyset \) as \( X \) is irreducible, and then it contains a maximal pt \( x \) by Hilbert's Nullstellensatz, and then \( \dim U = \dim(\mathcal{O}_{X,x}) = \dim U' \) because f.g. algebras over a field is catenary.

Integral & Finite Map

Def. (5.4.4.34) [Finite and Integral Map]. A morphism \( f : X \to S \) is called integral if it is affine and there is a affine open covering \( U_i = \text{Spec} \ A_i \) of \( S \) that \( f^{-1}(U_i) = \text{Spec} \ B_i \) and \( A_i \to B_i \) is integral.

A morphism \( f : X \to S \) is called finite if it is affine and there is a affine open covering \( U_i = \text{Spec} \ A_i \) of \( S \) that \( f^{-1}(U_i) = \text{Spec} \ B_i \) and \( B_i \) are finite modules over \( A_i \).

A morphism \( f : X \to S \) is called (locally) quasi-finite if it is (locally) of f.t. and the inverse of a point is a discrete set.

Prop. (5.4.4.35) [Integral Morphism is Closed]. Specialization lifts along an integral morphism. In particular, an integral morphism is closed, by (5.4.4.9).

Proof: If \( f(x) = y, y \to y' \), then we can choose an open affine \( U \) containing \( y' \), which also contains \( y \). So we can choose an open affine containing \( x \) mapping into \( U \), then it reduces to the affine case (4.1.7.13).

Prop. (5.4.4.36) [Chevalley]. If \( f : Y \to X \) is integral surjective, \( Y \) is affine, then \( X \) is affine.
**Proof:** Cf.[Sta]05YU.

**Lemma (5.4.4.37).** If \( f : Y \to X \) is finite surjective, \( Y \) is affine, then \( X \) is affine.

**Proof:**

**Prop. (5.4.4.38) [Finite and Integral].** A morphism is finite iff it is integral of f.t..

**Prop. (5.4.4.39) [Integral and Affine u.c.].** Integral map is equivalent to u.c. and affine.

**Proof:** Integral is stable under base change. And if it is integral, then it is closed by (4.2.1.5).

Conversely, we need to prove if \( \text{Spec } B \to \text{Spec } A \) is u.c., then \( A \to B \) is integral. For any \( a \in B \), let \( J \) be the kernel of \( A[X] \to B[X]/(aX - 1) \), then if \( f \in J \), then \( f(X) = (aX - 1)q(X) \), and \( X^\deg(f) f(\frac{1}{X}) = (a - X)X^\deg(q)q(\frac{1}{X}) \) vanishes at \( a \), so it suffices to find a \( f \in J \) with constant term 1. It suffices to show that \( \text{Spec}(A[X]/J + (x)) \) is empty:

As \( f \) is universally closed, \( \text{Spec } B[X] \to \text{Spec } A[X] \) is closed, thus the image of \( \text{Spec}(B[X]/(aX - 1)) \) is closed in \( \text{Spec } A \), which is the underlying set of \( \text{Spec } A/J \), by (5.4.4.64). Now notice \( T = \text{Spec}(A[X]/J + (x)) \times_{\text{Spec } A[X]/J} \text{Spec}(B[X]/(aX - 1)) \) is empty, because \( (A[X]/J + (x)) \otimes_{A[X]/J} (B[X]/(aX - 1)) = \text{Spec } A \otimes \text{Spec } A/X \text{Spec}(B[X]/(aX - 1)) = 0 \), as \( X \) is invertible in \( B[X]/(aX - 1) \) but vanish in \( A \). But \( T \to \text{Spec}(A[X]/J + (x)) \) is surjective, as a base change of \( \text{Spec}(B[X]/(aX - 1)) \) to \( \text{Spec } A/J \), thus we are done.

**Def. (5.4.4.40) [Degree of Finite Morphisms at a Point].** Suppose \( \pi : X \to Y \) is a finite morphism, then \( \pi_* \mathcal{O}_X \) is a \( \mathcal{O}_Y \)-module of f.t.. Let \( p \in Y \), then the **degree of \( \pi \) at \( p \)** is the rank of this sheaf on \( Y \) (5.5.1.11), which is an upper-semicontinuous function (5.5.1.41).

**Prop. (5.4.4.41).** The degree of a finite morphism \( \pi : X \to Y \) at \( p \) is the dimension over \( k(p) \) of the fiber of \( \pi \) at \( p \). In particular, the degree is zero iff \( \pi^{-1}(p) = 0 \).

**Proof:** Look affine locally.

**Lemma (5.4.4.42).** For \( f : Y \to X \) finite surjective and \( X \) locally Noetherian, for every integral subscheme \( Z \) of \( X \) with generic point \( \xi \), there is a coherent sheaf \( \mathcal{F} \) on \( Y \) that the support of \( f_* \mathcal{F} \) is \( Z \) and \( (f_*Z)_\xi \) is annihilated by \( \mathfrak{m}_\xi \).

**Proof:** Consider an inverse image of \( \xi = \xi' \), and let \( Z' = \frac{\xi}{\mathcal{F}} \) with the induced reduced structure, then let \( \mathcal{F} = i_* \mathcal{O}_{Z'} \) on \( Y \), \( \mathcal{F} \) is coherent, then we need to show that \( (f_* \mathcal{F})_\xi \) is annihilated by \( \mathfrak{m}_\xi \). This is because it factors through \( Z \). Cf.[Sta]01YO.

**Quasi-Finiteness**

**Def. (5.4.4.43) [Quasi-Finite Morphisms].**

(Locally)Quasi-finite morphisms are local on the target and satisfies base change trick.

**Prop. (5.4.4.44) [Characterization of Quasi-Finiteness].** Let \( f : X \to S \) be a morphism, then the following are equivalent:

- \( f \) is quasi-finite.
- \( f \) is locally quasi-finite and quasi-compact.
- \( f \) is locally of f.t., quasi-finite and has finite fibres.
5.4. PROPERTIES OF SCHEMES

Proof: Cf.[Sta]01TJ, 02NH.

Prop.(5.4.4.45). Immersions are locally quasi-finite.

Prop.(5.4.4.46). Let \( f : X \to S \) be a morphism of schemes and \( s \in S \). Assume that \( f \) is locally of f.t. and \( f^{-1}(s) \) is a finite set, then \( X_s \) is a finite discrete topological space, and \( f \) is quasi-finite at every point of \( f^{-1}(s) \).

Proof: Cf.[Sta]02NG.

Prop.(5.4.4.47)[Zariski’s Main Theorem]. Let \( f : Y \to X \) be an affine morphism of f.t.. Let \( Y \xrightarrow{f'} X' \xrightarrow{\nu} X \) where \( X' \) is the normalization of \( X \) in \( Y \), then there exists an open subscheme \( U' \subset X' \) that \( (f')^{-1}(U) \to U \) is an isomorphism and \( (f')^{-1}(U) \) is the set of points at which \( f \) is quasi-finite.

Proof: Cf.[Sta]03GT.

Prop.(5.4.4.48)[Quasi-Finite Locus is Open]. Let \( f : X \to S \) be a morphism of schemes, then the set of points of \( X \) that \( f \) is quasi-finite is an open subset \( U \subset X \), and \( U \to S \) is locally quasi-finite.

Proof: Cf.[Sta]01T1.

Prop.(5.4.4.49)[Zariski’s Main Theorem]. For a morphism \( X \to S \) that is quasi-finite and separated, if \( S \) is qcqs, Then there is a factorization \( X \to T \to S \) that \( X \to T \) is a qc open immersion and \( T \to S \) is finite.

Proof: Cf.[Sta]05K0.

Prop.(5.4.4.50). If \( f : Y \to X \) is a quasi-finite morphism of schemes, and \( T \subset Y \) is nowhere dense, then \( f(T) \subset X \) is also nowhere dense.

Proof: Cf.[Sta]03J2.

Generically Finiteness

Def.(5.4.4.51)[Generically Finite Morphisms]. A generically finite morphism is a morphism \( f : X \to Y \) locally of f.t. and there exists a dense open subset \( U \subset X \) s.t. \( U \to Y \) is locally quasi-finite.

Lemma(5.4.4.52). Let \( R \to S \) be a ring map of f.t., if \( p \subset R \) is a minimal prime that there are f.m. primes in \( S \) lying over \( p \), then there is a \( g \in R \), \( g \notin p \) that \( R_g \to S_g \) is finite.

Proof: The condition means \( S_p/pS_p \) has only f.m. primes and \( pS_p \) is locally nilpotent. Then \( \kappa(p) \to S_p/pS_p \) if finite. Let \( x_i \) generate \( S \) over \( R \), then there are polynomials \( P_i \in R[X] \) that \( P_i(x_i) = 0 \in S_p/pS_p \), and thus \( P_i^e(x_i) = 0 \in S_p \). Now choose \( g \notin p \) that \( g \) divides the common divisors of the coefficients of \( P_i \) and \( P_i^e(x_i) = 0 \in S_p \), then \( R_g \to S_g \) is finite.

Prop.(5.4.4.53)[Generically Finiteness]. Let \( f : X \to Y \) be a morphism of finite type. If \( \eta \in Y \) is a generic point, then:

- \( f^{-1}(\eta) \) is a finite set iff there are affine opens \( U_i \subset X, i = 1, \ldots, n \) and \( V \subset Y \) that \( f(U_i) \subset V, \eta \in V \) and \( f^{-1}(\eta) \subset \cup U_i \) and \( U_i \to V \) are finite.
• If $f$ is qs, then we can further restrict to $n = 1$.
• If $f$ is qcqs, then we can further restrict to $U_1 = f^{-1}(V)$.

Proof: These are local on $Y$, so we can change $Y$ to an affine open subscheme containing $\eta$.

1: If these affine opens exist, then $\# f^{-1}(\eta) < \infty$ because finite maps are quasi-finite (5.4.5.5).

If $f^{-1}(\eta) = \{\xi_1, \ldots, \xi_n\}$, choose affine opens $U_i$ around each $\xi_i$, then we reduce to the affine case (5.4.4.52).

2: Cf. [Sta]02NW.

3: □

Prop. (5.4.4.54) [Extension of Fraction Fields]. Let $f : X \rightarrow Y$ be a dominant morphism locally of f.t. between integral schemes, then the following are equivalent:
• $\text{tr.deg } K(X)/K(Y) = 0$.
• $K(X)/K(Y)$ is finite.
• there exists non-empty affine opens $U \subset X, V \subset Y$ s.t. $f(U) \subset V$ and $U \rightarrow V$ is finite.
• the generic point of $X$ is the only point mapping to the generic point of $Y$.
• If $f$ is qc or qs, we can assume $U = f^{-1}(V)$.

Proof: Cf. [Sta]02NX. □

Def. (5.4.4.55) [Degree Generically Finite Morphisms]. Let $f : X \rightarrow Y$ be a dominant morphism of f.t. between integral schemes, then by (5.4.4.23), $f$ induces an injective map of function fields $K(Y) \rightarrow K(X)$, the degree of $[K(X) : K(Y)]$ is called the degree of $f$, denoted by $\deg(f)$. It is a positive integer or $\infty$.

When $\deg(f)$ is finite (i.e. the conditions of (5.4.4.54) hold), it is called a separable/purely inseparable morphism if the field extension $K(X)/K(Y)$ is separable/purely inseparable. And also we can define the separable, inseparable degree of $f$.

Immersions

Def. (5.4.4.56) [Immersions]. A closed immersion of schemes is a closed immersion of local ringed spaces (5.2.6.15). A closed subscheme of a scheme $X$ is a closed sub-ringed space (5.2.6.15) that is also a scheme.

An open immersion of schemes is an open immersion of local ringed spaces (5.2.6.15). An open subscheme of a scheme $X$ is an open subspace (5.2.6.15) that is also a scheme.

Open and closed immersions are affine local on the target (5.4.1.5).

An immersion is a morphism that is a closed immersion of an open immersion.

Lemma (5.4.4.57) [Closed Immersion for Schemes]. Let $f : Y \rightarrow X$ be a morphism of schemes that induces a homeomorphism of $Y$ onto a closed subset of $X$, and $f^\sharp : \mathcal{O}_X \rightarrow f_\ast \mathcal{O}_Y$ is surjective, then it is a closed immersion (5.2.6.15).

Proof: It suffices to show that the kernel of $f^\sharp$ is Qco. For this, notice that $f$ is quasi-compact, and it is a monomorphism by (5.4.4.5), in particular separated by (5.4.4.86). Then (5.5.1.6) shows $f_\ast \mathcal{O}_Y$ is Qco. Then the kernel is Qco by (5.5.1.3). □

Prop. (5.4.4.58) [Closed Subschemes of Affine Schemes]. The closed sub-ringed spaces of $X = \text{Spec } A$ are all closed subschemes, and they corresponds to ideals $I \subset A$:
5.4. PROPERTIES OF SCHEMES

- If $I \subset A$ is an ideal, then the morphism $Z = \text{Spec } A/I \to \text{Spec } A$ is a homeomorphism of $Z$ onto a closed subspace $V(I)$ of $X$, and also the stalk map at a point $p \subset Z$ is $R_p \to (R/I)_p = R_p / I R_p$, which is surjective. So this is a closed immersion by (5.4.4.57).

- By (5.2.6.17), for any closed subscheme $Z$ of $X$ with sheaf of ideals $\mathcal{I}$, $Z$ is isomorphic to the closed subscheme of $X$ defined by $\mathcal{I}$. Now $\mathcal{I}$ is locally generated by sections, so the quotient sheaf $\mathcal{O}_X / \mathcal{I}$ is a Qco sheaf, so it is of the form $\widetilde{S}$ for some $A$-module $S$, by (5.5.1.2). Then $\mathcal{I}$, as the kernel of $\mathcal{O}_X \to \widetilde{S}$, is also Qco (5.5.1.3), so it equals $\widetilde{I}$ for some ideal $I \subset A$. Thus $S = R \ wedge I$, and we are done.

Prop. (5.4.4.59) [Closed Subscheme of Schemes]. The closed sub-ringed spaces of a scheme $X$ are all closed subschemes, and they correspond to Qco $\mathcal{O}_X$-sheaves of ideals via the ideal sheaf (5.2.6.15):

Proof: Let $i : Y \to X$ be a closed immersion, for any $x \in X$, choose an open affine nbhd $U$ of $x \in X$, then $i : i^{-1}(U) \to U$ is also a closed immersion, so it corresponds to $\text{Spec } A/I \to \text{Spec } A$ for some ideal $I$ by (5.4.4.58). So $Z$ is a scheme, and the ideal sheaf $\mathcal{I}$ is Qco. □

Prop. (5.4.4.60). Closed immersion satisfies the base change trick (5.4.4.2). Open immersion are stable under base change and composition. Immersions are stable under base change and composition.

Proof: For immersion, shrink the open subset. □

Remark (5.4.4.61). A open immersion followed by a closed immersion can be written as a closed immersion followed by an open immersion, but not reversely. The reverse happens if the immersion is quasi-compact or the source is reduced (use the reduced induced structure).

Def. (5.4.4.62) [Scheme-Theoretical Image]. For a morphism $f : X \to Y$, there is a closed scheme called scheme-theoretic image that is the smallest closed subscheme of $Y$ that $f$ factors through $Z$.

For an immersion of schemes, the scheme-theoretic image of the immersion is called the scheme-theoretic closure.

Proof: Consider the kernel of the structural map, and the kernel contains a maximal Qco sheaf of ideals $\mathcal{I}$ by (5.5.1.12). □

Prop. (5.4.4.63). If $X_1 \overset{f_1}{\to} Y_1 \quad \downarrow \quad \downarrow$

be a commutative diagram of schemes and $Z_i \subset Y_i$ be the scheme-theoretic image of $f_i$, then it induces a commutative diagram $X_1 \overset{f_1}{\to} Z_1 \overset{f_1}{\to} Y_1$

$X_2 \overset{f_2}{\to} Z_2 \overset{f_2}{\to} Y_2$

Proof: It suffices to show $Z_1$ factors through the closed subscheme $Z_2 \times_{Y_2} Y_1$ of $Y_1$, which follows from the universal property of $Z_1$. □

Prop. (5.4.4.64). Let $f : X \to Y$ be a qc morphism of schemes and $Z$ be the scheme-theoretical image, then

- the kernel $\mathcal{I} = \ker(\mathcal{O}_Y \to f_* \mathcal{O}_X)$ is Qco, thus $Z$ is the closed subscheme determined by $\mathcal{I}$.

- For any open subscheme $U \subset Y$, the scheme-theoretical image of $f|_{f^{-1}(U)}$ is equal to $Z \cap U$. 

• \( f(X) \) is dense in \( Z \).

**Proof:** 1: As being Qco is local, it suffices to show for \( Y \) affine. Then \( X = \bigcup U_i \) is a finite union of affine schemes. Now take \( X' = \bigsqcup U_i \), then there are maps \( X' \xrightarrow{f'} X \rightarrow Y \). Then \( \mathcal{O}_X \) is a subsheaf of \( f'_*\mathcal{O}_X \). So \( \mathcal{I} = \ker(\mathcal{O}_Y \to f_*f'_*\mathcal{O}_X) \). Now \( f \circ f' \) is qcqs, thus by (5.5.1.6), \( f_*f'_*\mathcal{O}_X \) is Qco, thus also \( \mathcal{I} \) is Qco.

2 follows from 1 as the formation of \( \mathcal{I} \) commutes with restriction to open subschemes.

3 follows from 2 as the scheme-theoretical image of empty set is empty. \( \qed \)

**Prop.(5.4.4.65).** If \( f : X \to Y \) is a morphism and \( X \) is reduced, then the scheme-theoretical image of \( f \) is the induced-reduced structure (5.4.1.14) of \( f(X) \subset Y \).

**Proof:** This is clear. \( \qed \)

**Def.(5.4.4.66) [Scheme-Theoretically Dense].** An open subscheme \( U \subset X \) is called **scheme-theoretically dense** if for any open subscheme \( V \) of \( X \), the scheme-theoretical closure of \( U \cap V \) in \( V \) is equal to \( V \).

**Prop.(5.4.4.67).** If the inclusion \( U \to X \) is qc, then \( U \) is scheme-theoretically dense in \( X \) iff the scheme-theoretical closure of \( U \) is \( X \), by (5.4.4.64).

**Prop.(5.4.4.68).** Let \( j : U \to X \) be an open immersion of schemes, then \( U \) is scheme-theoretically dense in \( X \) iff \( \mathcal{O}_X \to j_*\mathcal{O}_U \) is injective.

**Proof:** If it is not injective, then we can find an open subscheme \( V \) of \( X \) that the kernel is non-zero, thus it contains a non-zero Qco ideal sheaf, which means the scheme-theoretical closure of \( U \cap V \) is not \( V \). \( \qed \)

**Cor.(5.4.4.69).** If \( U, V \) are open subschemes of \( X \) scheme-theoretically dense in \( X \), then \( U \cap V \) is also scheme-theoretically dense in \( X \).

**Proof:** \( \mathcal{O}_X \to \mathcal{O}_X(U) \to \mathcal{O}_X(U \cap V) \) is injective. \( \qed \)

**Prop.(5.4.4.70) [Scheme-Theoretical Image of Immersions].** Let \( f : Z \to X \) be an immersion and either \( f \) is qc or \( Z \) is reduced. Let \( Z \) be the scheme-theoretically image of \( f \), then the morphism \( Z \to Z \) is an open immersion that identifies \( Z \) with a scheme-theoretical dense open subscheme of \( Z \), and also \( Z \) is dense in \( Z \).

**Proof:** Cf. [Sta]01RG. \( \qed \)

**Prop.(5.4.4.71) [Immersion to be Closed].** An immersion \( f \) is a closed immersion iff the image is closed.

**Proof:** Let \( i : Y \to U \) be a closed immersion where \( j : U \subset X \) is an open subscheme, then \( i \) is associated to an ideal sheaf \( \mathcal{I} \) of \( \mathcal{O}_U \). Now because \( \mathcal{I}|_{U \setminus j(Y)} = \mathcal{O}_{U \setminus j(Y)} \), we can glue \( \mathcal{I} \) and \( \mathcal{O}|_{X \setminus j(Y)} \) to a sheaf of ideals \( \mathcal{J} \subset \mathcal{O}_X \). Now \( j^*\mathcal{O}_X/\mathcal{J} = \mathcal{O}_U/\mathcal{I} \cong i_*\mathcal{O}_Y \), thus \( \mathcal{O}_X \to f_*\mathcal{O}_Y = j_*j^*(\mathcal{O}_X/\mathcal{J}) \) is surjective, because \( \mathcal{O}_U/\mathcal{I} \) is supported on a closed subset of \( U \). Thus \( f \) is a closed immersion by (5.4.4.57). \( \qed \)

**Prop.(5.4.4.72) [Immersions are Monomorphisms].** An immersion is a monomorphism.

**Proof:** It is easy to check (5.4.4.5) for both open and closed immersions. \( \qed \)
Prop. (5.4.4.73) [Equivalent Definitions of Closed Immersion]. The following are equivalent for a morphism $f$:

- $f$ is a closed immersion.
- $f$ is a proper monomorphism.
- $f$ is proper, unramified and u.i..
- $f$ is a u.c., unramified monomorphism.
- $f$ is u.c., unramified and u.i..
- $f$ is u.c., locally of f.t. and a monomorphism.
- $f$ is u.c., locally of f.t. and formally unramified.

Proof: $4-7$ are equivalent by (5.6.5.13). For the rest, Cf. [Sta], 04XV.

Universal Homeomorphism

Prop. (5.4.4.74). A morphism is a universally homeomorphism iff it is integral, surjective and universally injective.

Proof: A universally homeomorphism is affine by (5.4.4.15). It is clearly u.c, so it is integral by (5.4.4.39). Conversely, it is integral hence u.c, and universally bijective, so it is universally homeomorphism.

Cor. (5.4.4.75). The reduction $X_{\text{red}} \to X$ is a universal homeomorphism, as closed immersion is u.c.

Separatedness

Def. (5.4.4.76) [Separatedness]. A map $f : X \to Y$ is called separated if the diagonal $\Delta : X \to X \times_Y X$ is a closed immersion. It is called quasi-separated if the diagonal is quasi-compact.

In fact $\Delta$ is always an immersion because maps between affine scheme is separated so $\Delta(X)$ is closed in $\bigcup U_{ij} \otimes_{V_i} U_{ij}$ where $U,V$ are affine open, hence it suffice to check the image is closed.

Prop. (5.4.4.77). (Quasi-)Separatedness is local on the target because closed immersion and quasi-compact is local on the target (5.4.1.5).

(Quasi-)Separatedness satisfies base change trick by (5.4.4.2).

Prop. (5.4.4.78) [Graph]. By (3.1.1.50), for $X \to S$ and $Y \to S$, the map $X = X \times_Y Y \to X \times_S Y$ is an immersion. It is closed immersion if $Y \to S$ is separated, and it is qc if $Y \to S$ is quasi-separated.

Cor. (5.4.4.79). for $X \to Y$ is a morphism of schemes over $S$, the map $X = X \times_Y Y \to X \times_S Y$ is an immersion. It is closed immersion if $Y \to S$ is separated, and it is qc if $Y \to S$ is quasi-separated.

Cor. (5.4.4.80). If $s : S \to X$ is a section of $f : X \to S$, the above proposition applies to this case, because $S = S \times_X X \to S \times_S X = X$.

Prop. (5.4.4.81) [Characterization of Separatedness]. A morphism is quasi-separated iff for any two affine open that mapped into an affine open, their intersection is quasi-compact. This is because quasi-compact is local on the target.

A morphism is separated iff for any two affine open that mapped into an affine open, their intersection is affine and $\mathcal{O}(U) \otimes_{\mathcal{O}(W)} \mathcal{O}(V) \to \mathcal{O}(U \cap V)$ is surjective. This is because closed immersion is local on the target (5.4.1.5).
578  CHAPTER 5. ALGEBRAIC GEOMETRY I: SCHEME THEORY

Cor. (5.4.4.82). A locally Noetherian scheme is quasi-separated.

Cor. (5.4.4.83). If \( g \circ f \) is (quasi-)separated, then so is \( f \).

Cor. (5.4.4.84). If \( X \) is (quasi-)separated, then \( X \to Y \) is (quasi-)separated.

Prop. (5.4.4.85) [Injective Maps are Separated]. Injective maps of schemes are separated.

Proof: Let \( f : X \to Y \) be an injective map. Firstly \( X \times_Y X \) is a union of affine subschemes of the form \( U \times_Y U \) where \( U, V \) are affine and \( f(U) \subset V \); let \( z \in X \times_Y X \), then \( \pi_1(z) = \pi_2(z) \), because they map to the same point in \( Y \), thus we can choose affine nbhds \( U, V \) of \( \pi_1(z) \) and \( f(\pi_1(z)) \). Now for each of these \( U \times_Y U \), \( \Delta : U \to U \times_Y U \) is closed immersion, thus \( \Delta_X \) is also closed immersion (5.4.1.5). \( \square \)

Cor. (5.4.4.86). monomorphisms are separated because they are universal injective (5.4.4.4), and immersions are separated.

Prop. (5.4.4.87). (Quasi-)Affine morphism is separated (Check closed immersion directly).

Prop. (5.4.4.88). if \( f : X \to S \) is affine, \( h : Y \to S \) is separated, and \( g : X \to Y \) is a morphism over \( S \), then \( g \) is affine.

Proof: Decompose \( g \) as \( X \to X \times_S Y \to Y \), where the first map is base change of \( \Delta_Y \) and the second map is base change of \( f \), so they are both affine. \( \square \)

Prop. (5.4.4.89) [Scheme-Theoretic Equalizer]. If \( X, Y \) are schemes over \( S \) and \( a, b : X \to S \) are morphisms, then there is a largest locally closed subscheme \( Z \) of \( X \) that \( a|_Z = b|_Z \). And if \( Y/S \) is separated, \( Z \) is a closed subscheme of \( X \).

Proof: By definition, \( Z \) should be the fibered product:

\[
\begin{align*}
Z & \longrightarrow X \\
\downarrow & \downarrow^{(a,b)} \\
Y & \Delta_Y \times_S Y
\end{align*}
\]

then the theorem follows from the definition and base change trick of locally closed morphisms. \( \square \)

Prop. (5.4.4.90) [Qsqc Lemma]. Let \( X \) be a qcqs scheme and \( s \in \Gamma(X, \mathcal{O}_X) \), then there is a natural isomorphism \( \Gamma(X, \mathcal{O}_X)_s \cong \Gamma(X_s, \mathcal{O}_X) \).

Proof: Firstly this is true for \( X \) affine by definition (5.2.7.1). In general, let \( U_i \) be an affine open cover of \( X \) that \( U_i \cap U_j = \cup_{k=0}^c U_{ijk} \) be a finite cover by affine opens, then there is an exact sequence

\[
\Gamma(X, \mathcal{O}_X) \to \prod_i \Gamma(U_i, \mathcal{O}_X) \to \prod_{ijk} \Gamma(U_{ijk}, \mathcal{O}_X).
\]

Then we can take localization by \( s \) to get an exact sequence

\[
\Gamma(X, \mathcal{O}_X)_s \to \prod_i \Gamma(D(s, U_i), \mathcal{O}_X)_s \to \prod_{ijk} \Gamma(D(s, U_{ijk}), \mathcal{O}_X)_s.
\]

but \( D(s, U_i) \) is an open cover of \( X_s \) with \( D(s, U_i) \cap D(s, U_j) = \cup_k D(s, U_{ijk}) \), thus we get a natural isomorphism \( \Gamma(X, \mathcal{O}_X)_s \cong \Gamma(X_s, \mathcal{O}_X) \). \( \square \)
5 Proper & Projective

Prop.(5.4.5.1)[Proper]. A morphism that is separated, of finite type and universally closed is called proper.

Properness is local on the target, because all these three properties do(5.4.1.5). Properness satisfies the base change trick(5.4.4.2).

Prop.(5.4.5.2). The class of proper morphisms satisfies the base change trick(5.4.4.1), by valuation criterion(5.4.5.13) and fibered products tricks.

Proof: Closed immersion is proper because it is f.t. and is affine so separated(5.4.4.76), and it is universally closed because immersions are stable under base change(5.4.4.60). □

Prop.(5.4.5.3)[Image of Proper Map]. If \( f : X \to Y \) is morphism between separated schemes f.t over \( S \), then if \( X \) is proper, then \( f \) is proper(by base change trick) thus the image is closed, and is proper over \( S \) in its scheme-theoretic structure.

Proof: Notice proper is qc, so by(5.4.4.62), the scheme-theoretic closure has the same underlying space as the image. Then use(5.4.4.8) to show it is u.c.. □

Cor.(5.4.5.4)[Connected Proper to Affine Constant]. A morphism from a connected proper scheme to an Noetherian affine scheme \( \text{Spec} A \) is constant.

Proof: Because the image is proper, by(5.7.4.12), the global section of its image is a finite module over \( k \) thus Artinian(4.1.3.4) so has finitely many points and is discrete. But \( X \) is connected, thus it is constant. □

Prop.(5.4.5.5)[Chevalley]. Let \( f : X \to Y \) be a morphism of schemes, the following are equivalent:

- \( f \) is finite.
- \( f \) is proper and affine.
- \( f \) is proper with finite fibers.
- \( f \) is proper and locally quasi-finite.
- \( f \) is separated, u.c., locally of f.t. and has finite fibres.

Proof: The fiber of \( f : X \to S \) is \( \text{Spec}(k(y) \otimes_A B) \), which is Artinian(4.1.3.4), so it has finitely many primes and they are all closed. Finite morphism is proper because it is integral(5.4.4.39).

The converse follows from Zariski’s main theorem(5.4.4.49).

Cf.[Sta]02LS. □

Cor.(5.4.5.6)[Quasi-Affine+Proper imply Affine]. Let \( f : X \to \text{Spec} A \) be a quasi-affine and proper map, then \( f \) is affine.

Proof: This follows from(5.7.2.8)(5.4.4.20) and the fact \( H^p(X, \mathcal{O}_X) = 0 \) for \( p > 0 \). □

Prop.(5.4.5.7)[Quasi-Finite+Proper Imply Finite]. Let \( f : X \to S \) be a proper morphism of schemes and \( s \in S \) that \( f^{-1}(s) \) is a finite set, then there exists a nbhd \( V \) of \( s \in S \) that \( f^{-1}(V) \to V \) is finite.

Proof: By(5.4.4.46), \( f \) is quasi-finite at the points of \( f^{-1}(s) \). By(5.4.4.48) the set \( U \) of points that \( f \) is quasi-finite is open. Denote \( Z = X \setminus U \), then \( f(Z) \) is closed in \( S \) and doesn’t contain \( s \). Then \( V = S \setminus f(Z) \) satisfies the requirement by(5.4.5.5). □
**Prop. (5.4.5.8) [Generically Finite + Proper Imply Finite]**. Let $f : X \to S$ be a proper morphism of locally Noetherian schemes and $y \in Y$ satisfies $\dim \mathcal{O}_{Y,y} \leq 1$, and if one of the following holds:

- For every generic point $\eta$ of $X$ s.t. $f(\eta)$ generalizes $y$, $k(\eta)/k(f(\eta))$ is algebraic.
- $f$ is quasi-finite at every generic point of $x$.
- $f$ is quasi-finite on a dense subset of $X$.

then there exists an open nbhd $V$ of $y \in Y$ s.t. $f^{-1}(V) \to V$ is finite.

**Proof**: Cf. [Sta]0AB7.

**Prop. (5.4.5.9)**. If $X$ is a separated scheme over a field $k$ of dimension $> 0$ and $x \in X$ is a closed point, then $X \setminus \{x\}$ is not proper over $k$.

**Proof**: Cf. [Sta]0A24.

**Def. (5.4.5.10) [Modification and Alteration]**. A modification of $X \in \text{Sch}$ is a scheme $X'$ together with a proper birational map $X' \to X$.

A alteration of $X$ is a scheme $X'$ together with a proper dominant morphism $f : X' \to X$ that for some non-empty open $U$ of $X$, $f^{-1}(U) \to U$ is finite.

**Prop. (5.4.5.11)**. Let $Y \to X \in \text{Sch}$ be an alteration, then it can be decomposed into $Y \to W \to X$ where $Y \to X$ is a modification and $W \to X$ is finite surjective.

**Proof**: ?

**Valuation Criteria**

**Lemma (5.4.5.12) [Valuation Criteria Lemma]**. If $X$ is a scheme and $x \to y$ is a specialization of pts, then for any field extension $K/k(x)$, there is a valuation ring $A \subset K$ and a morphisms $\text{Spec} A \to X$ that maps the generic pt $\eta$ to $x$ and the unique closed pt to $y$.

Moreover, if $X$ is locally Noetherian, then $A$ can be chosen to be a DVR.

**Proof**: There is a morphism $\mathcal{O}_{X,y} \to k(x) \to K$, so there is a valuation ring $A$ with field of fractions $K$ that dominate the image of $\mathcal{O}_{X,y}$ by (10.3.2.1), which is also a local ring (4.1.1.9). Then this is what we desire.

For the locally Noetherian case, add (10.3.3.7).

**Prop. (5.4.5.13) [Valuation Criteria]**. The valuation criterion for $\text{Spec} K \to \text{Spec} R$ where $R$ is a valuation ring with field of fractions $K$: Given a morphism $f : X \to S$,

1. If it is qc, then it is universally closed iff there is at least one lifting.

2. it is separated iff it is quasi-separated and there is at most one lifting.

3. it is proper iff it is finite type, quasi-separated and lifting exists uniquely.

Moreover, if $S$ is locally Noetherian and $f$ is locally of f.t., then it suffices to check for discrete valuation rings. **Proof**:

1. Firstly, in this case, by (5.4.4.9), it suffices to prove that: specializations lift along any base change of $f$ iff it has at least one lifting. If specializations lift along any base change of $f$, change $S$ to $\text{Spec} A$ and $X$ to $X \times_S \text{Spec} A$. Let $x'$ be the image of $\text{Spec} K \to X$, then by hypothesis there is a specialization $x' \to x$ where $x$ maps to the closed pt of $\text{Spec} A$. Then we
get a map \( A \to \mathcal{O}_{X,x} \to k(x') \to K \), which is exactly the quotient map \( A \to K \). So the image of \( \mathcal{O}_{X,x} \) in \( K \) dominates \( A \), which means it is just \( A \). Thus we get a map \( \mathcal{O}_{X,x} \to A \), which gives a map \( \text{Spec } A \to X \) that commutes \( \text{Spec } K \).

Conversely, if \( f \) has at least one lifting, then any base change of \( f \) also has at least one lifting by categorial reason. Thus it suffices to show specializations lift along \( f \). Let \( s' \to s \) be a specialization in \( S \) and \( x' \in X \) maps to \( s' \), we can apply (5.4.5.12) to \( k(s') \subset k(x') = K \), then we get a lifting diagram, and the image of the closed pt of \( \text{Spec } A \) under the lifting is a point mapping to \( s \).

2. If it is separated, then if there are two lifting, then consider their equalizer, it is a closed subscheme of \( \text{Spec } A \) by (5.2.7.18), and it contains the generic pt, so it equals \( \text{Spec } A \), as desired.

Conversely, if there are at most one lifting, then we want to prove the diagonal is closed. But by (5.4.4.76) and (5.4.4.71) and the valuation criterion for u.c., it suffices to prove the existence of a lifting for the diagonal map (5.4.5.13). But in fact, a valuation digram for the diagonal correspond to two lifting of a valuation criterion for \( X \to S \), then they are the same, and \( \text{Spec } A \to X \times_S X \) lifts along the diagonal.

3. follows from the above two.

\[ \square \]

**Prop. (5.4.5.14) [Extension of Rational Maps]**. Let \( X, Y \) be schemes over \( S \), \( X \) is locally Noetherian and \( Y/S \) is proper. If there is a morphism from an open subset \( U \) of \( X \) to \( Y \), and there is a point \( x \) in the closure of \( U \) with the stalk being a valuation ring, then the morphism can be extended to an open set containing \( x \).

**Proof**: We can replace \( X \) by an affine open nbhd of \( X \). By (4.4.6.1), we assume \( X \) is affine and \( \Gamma(X, \mathcal{O}_X) \subset \mathcal{O}_{X,x} \). In particular \( X \) is integral with generic pt \( \xi \) with residue field \( K \). Then \( U \) contains \( \xi \). By the valuation criterion (5.4.5.13), the morphism \( \text{Spec } K \xrightarrow{\xi} U \to Y \) can be lifted to a morphism \( \text{Spec } \mathcal{O}_{X,x} \to Y \), thus lemma (5.4.6.2) shows there is a morphism on a nbhd \( V \) of \( X \) spreading this morphisms.

Now because \( Y/S \) is separated, the equalizer of this morphism and \( f \) on their intersection is a closed subscheme by (5.4.4.89), but it contains \( \xi \), so they coincide on the intersection, so we are done. \[ \square \]

**Prop. (5.4.5.15) [Singularity in Codimension 1]**. Let \( \varphi : X \to X' \) be a rational map of a locally Noetherian scheme \( X/K \) regular in codimension 1 to a proper scheme \( X'/K \) with maximal domain \( U \), then

\[ \text{codim}(X \setminus U, X) \geq 2. \]

In particular, if \( X \) is non-singular curve, then \( \varphi \) is a morphism.

**Proof**: Use (5.4.5.14), noticing that the stalk at a point of codimention 1 is a DVR (4.3.5.20). \[ \square \]

**Projective Morphism**

**Def. (5.4.5.16) [Projective Morphism]**. A projective morphism \( X \to Y \) is a closed immersion \( X \to \text{Proj}(\mathcal{E}) \) for some \( \mathcal{O}_Y \)-f.t. module \( \mathcal{E} \) over \( Y \).

An \( H \)-projective morphism \( X \to Y \) is a closed immersion \( X \to \mathbb{P}_Y^n \).
An $H$-quasi-projective morphism is a $H$-projective morphism composed with a quasi-compact open immersion.

A locally projective morphism $f : X \to Y$ is a morphism $f$ that there exists a covering $U_i$ of $Y$ that $f^{-1}(U_i) \to U_i$ is projective.

Some proposition about projective is written before the language of Hartshorne so I may not have changed them to the more general notion of projectiveness yet.

**Prop. (5.4.5.17).** For a morphism $f : X \to S$, the following are equivalent:

- $f$ is locally projective.
- There is a covering $U_i$ of $S$ that $f^{-1}(U_i) \to U_i$ is $H$-projective.

**Proof:** Clearly 2 implies 1, and for the converse, it suffices to show that projective morphism is locally $H$-projective. Locally on each affine open nbhd $U = \text{Spec } R$, $X_U$ is isomorphic to a closed subscheme of $P(\mathcal{E})$ for some f.t. $\mathcal{E}$ of $\mathcal{O}_U$-modules. Write $\mathcal{E} = \hat{M}$ for some f.t. $R$-module $M$, which induces a surjection of graded $R$-algebra $R[x_0, \ldots, x_n] \to \text{Sym}_R(M)$, then the corresponding morphism $P(\mathcal{E}) \to \mathbb{P}^n$ is a closed immersion, so $f^{-1}(U)$ is a $H$-projective scheme over $U$. □

**Prop. (5.4.5.18).** $H$-(quasi-)projectiveness is stable under base change and composition. (because Segre embedding is closed). Disjoint union of f.m. projective morphisms is projective (embed into the Segre embedding).

**Proof:** [Sta]01WE. □

**Cor. (5.4.5.19) [Projective Maps are Proper].** Projective morphisms are locally projective and locally projective morphisms are proper. Thus a quasi-projective morphism is locally of f.t. and separated (5.4.4.86).

**Proof:** Because locally projective and proper are both local on the base (5.4.4.2), it suffices to show that $H$-projective morphism is proper by (5.4.5.17).

Because properness satisfies base change trick (5.4.4.2), it suffices to show $\mathbb{P}^n_S \to S$ is proper. Also this is base change of $\mathbb{P}^n_Z \to Z$, it suffices to check this one. $\mathbb{P}^n_Z$ is clearly separated by (14.5.3.20) (looking at the natural affine covering), and qc. Finally we show it is u.c. using valuation criterion (5.4.5.13):

\[
\begin{array}{ccc}
\text{Spec } K & \longrightarrow & X \\
\downarrow & & \downarrow \\
\text{Spec } R & \longrightarrow & \text{Spec } Z \\
\end{array}
\]

Let $\varphi : k(\xi_1) \to K$. Let $f_{ij}$ be the image of $x_i/x_j$ under $\varphi$, and choose $k$ which $f_{k0}$ has the minimal valuation, then $f_{ik} \in R$ for any $i$, which means the there is a map

\[
\mathbb{Z}[x_0/x_k, \ldots, x_n/x_k] \to R
\]

compatible with $\varphi$, or equivalently a map $\text{Spec } R \to D(x_k) \subset X$ commuting the diagram. □

**Prop. (5.4.5.20) [Descent for Projectiveness].** Let $X$ be a scheme over a field $k$, and $K/k$ is a field extension, then $X_K$ is (quasi-)projective iff $X_K$ is (quasi-)projective.

**Proof:** This follows from (5.5.4.19) and f.f. descent. □
Prop. (5.4.5.21). $H$-Projective scheme over Spec $A$ is of the form Proj $S$ where $S_0 = A$ and $S$ is f.g over $S_0$ by $S_1(5.5.2.11)$.

Proof: □

Prop. (5.4.5.22) [Projective Morphisms and Closed Embeddings]. Let $k$ be an alg.closed field and $\pi : X \to Y$ is a projective morphism of algebraic schemes over $k$ that is injective on closed points and injective on tangent vectors at closed points, then $\pi$ is a closed embedding.

Proof: Cf. [Vak17]P506. □

Prop. (5.4.5.23) [Chow’s Lemma]. Let $X \to S$ be separated of f.t over a qcqs $S$, then there is a birational, H-projective map $\pi : X' \to X$ over $S$ that $X'$ is quasi-projective over $S$.

If $X$ is proper, then $X'$ is projective over $S$. And if $X$ is integral/irreducible/reduced over $S$, $X'$ can also be chosen to be so.

Proof: We only prove for $S$ Noetherian, for the general case, Cf. [Sta]0203.

In this case all schemes here are Noetherian. Suppose $X_i, i \le r$ are irreducible components of $X$ with generic points $\eta_i$, by (5.4.6.5) and the fact $X$ is qc we can find a finite affine cover $X = \cup U_i$ that each $U_i$ contains all the generic points of $X$, thus $U = U_1 \cap \ldots \cap U_n$ is dense in $X$. Let $X^*$ be the schematic-closure of $U$ in $X$, and $U_i^* = U_i \cap X^*$, then we may replace $X$ by $X^*$ and assume that $U$ is schematically dense in $X$ by (5.4.4.67) as $X$ is qs. By (5.5.4.22) and (5.4.4.19), there are immersions $U_i \to \mathbb{P}_{S_i}^{n_i}$ together with a closed subscheme $Z_i \subset \mathbb{P}_{S_i}^{n_i}$ that $U_i \to Z$ is a scheme-theoretically dense open immersion (5.4.4.70).

Consider the map $(j_1, \ldots, j_m) : U \to \mathbb{P}_{S_i}^{n_i} \times \ldots \times \mathbb{P}_{S_i}^{n_m}$ with scheme-theoretic image $Z$, and the commutative diagrams

$\begin{array}{c}
\mathbb{P}_{S_i}^{n_i} \times \ldots \times \mathbb{P}_{S_i}^{n_m} \\
\downarrow \pi_i \\
\mathbb{P}_{S_i}^{n_i}
\end{array}$

which induces a map $p_i : Z \to Z_i(5.4.4.63)$ which is proper.

Consider $p_i^{-1}(j_i(U_i)) = V_i$ and $X' = \cup_i V_i$ which is an open subscheme of $Z \subset \mathbb{P}_{S_i}^{n_i} \times \ldots \times \mathbb{P}_{S_i}^{n_m}$ thus quasi-projective over $S$.

Finally, we prove that the morphism $p_i : V_i \to U_i$ glue together to a proper birational morphism $\pi : X' \to X$; this is because they are compatible on $U$, which is scheme-theoretically dense in $V_i$ for each $i$ thus also also scheme-theoretically dense in $V_i$ and $V_j$, thus $p_i$ and $p_j$ are compatible on $V_i \cap V_j$ as the target $X$ is separated over $S$.

To show $\pi$ is proper, firstly notice $\pi^{-1}(U_i) = V_i$; there are decompositions $V_i \to \pi^{-1}(U_i) \to U_i$, where $V_i \to U_i$ is proper, thus $V_i \to \pi^{-1}(U_i)$ is also proper and $V_i$ is schematically dense in $\pi^{-1}(U_i)$ because it contains $U_i$, so it is and isomorphism.

For the same reason $U \to \pi^{-1}(U)$ is an isomorphism. Finally $\pi$ is projective because it factors through some map $X' \to X \times_S \mathbb{P}_S^{n_i} = \mathbb{P}_X^2$ and it is proper.

If $X$ is reduced, then $X'$ is reduced by (5.4.4.65), and if $X$ is irreducible, then $X' = Z$ is the closure of $j(X)$ by (5.4.4.70), which is irreducible. □
6 Technical Lemmas

Lemma (5.4.6.1). Let $X$ be a scheme and $x$ a point, then there exists an open affine nbhd $U$ of $x$ that $\mathcal{O}_X(U) \to \mathcal{O}_{X,x}$ is injective, if any of the follows holds:

- $X$ is integral.
- $X$ is locally Noetherian.
- $X$ is reduced with f.m. irreducible components.

Proof: This problem is clearly local hence follows from the algebra case (4.1.1.34).

Lemma (5.4.6.2) [Spread Out Stalk Morphism]. Let $X, Y$ be schemes over $S$, $s \in S$ and $x, y$ be pts over $S$, then:

- Let $f, g : X \to Y$ be morphisms over $S$ that $f(x) = g(x) = y$ and $f^*_x = g^*_x$, then $f = g$ on a nbhd $U$ of $x$ if any of the following holds:
  - (a) $Y \leftarrow S$ is locally of f.t..
  - (b) $X$ is integral.
  - (c) $X$ is locally Noetherian.
  - (d) $X$ is reduced with f.m. irreducible components.

- Let $\varphi : \mathcal{O}_{Y,y} \to \mathcal{O}_{X,x}$ be a local ring map over $\mathcal{O}_{S,s}$, then there is a morphism $f$ from a nbhd $U$ of $x$ mapping to $Y$ that $f(x) = y$, and $f^*_x = \varphi$, if any of the following holds:
  - (a) $Y \leftarrow S$ is locally of f.p..
  - (b) $Y \leftarrow S$ is locally of f.t. and $X$ is integral.
  - (c) $Y \leftarrow S$ is locally of f.t. and $X$ is locally Noetherian.
  - (d) $Y \leftarrow S$ is local of f.t. and $X$ is reduced with f.m. irreducible components.

Proof: Cf. [[Sta]0BX6].

Prop. (5.4.6.3) [Base Change of Fields is Quotient Map]. For any scheme $X$ over a field $k$ and algebraic extensions $K/k$, $X_K \to X$ is a quotient map, as it is surjective (5.6.2.1), continuous and closed (5.4.4.39).

Lemma (5.4.6.4). Let $X$ be a qs scheme and $Z_i$ be a finite set of irreducible components of $X$. Let $\eta_i$ be the generic point of $Z_i$, then there are open affine subsets $\eta_i \in U_i$ that $U_1, \ldots, U_n$ are pairwise disjoint.

Proof: 

Lemma (5.4.6.5). Let $X$ be a qs scheme and $Z_i$ be a finite set of irreducible components of $X$. Let $\eta_i$ be the generic point of $Z_i$ and $x \in X$, then there is an affine open subset of $X$ containing $x$ and $\eta_i$.

Proof: Let $x \in Z_1, \ldots, Z_r$ but $x \notin Z_{r+1}, \ldots, Z_n$, then we can find an arbitrary affine open nbhd $W$ of $x$ that contains $\eta_1, \ldots, \eta_r$ but not $\eta_{r+1}, \ldots, \eta_n$. By (5.4.6.4), we may choose pairwise disjoint affine open nbhds $\eta_{r+1} \in U_{r+1}, \ldots, \eta_m \in U_n$. Now $U_i \cap W$ is quasi-compact and doesn’t contain $\eta_i$, so we can shrink $U_i$ s.t. $W \cap U_i = \emptyset$ by (4.1.7.24). Then $U = W \coprod (\bigcup U_i)$ satisfies the desired condition.
Main references are [Sta] and [Vak17].

5.5 Quasi-Coherent Sheaves on Schemes

1 (Quasi-)Coherent Sheaves

Lemma (5.5.1.1) [Associated Qco Sheaves on Affine Scheme]. On an affine scheme Spec $A$, there is a sheaf $\tilde{M}$, that is $M_f$ on Spec $A_f$. To check it is a sheaf, we only need to check to affine coverings, and this is by (4.4.2.2).

Prop. (5.5.1.2) [Qco Sheaves on Affine Schemes]. $M \mapsto \tilde{M}$ is an equivalence to the category of quasi-coherent sheaves over Spec $A$. In particular,

$$\text{Hom}_A(M, \Gamma(X, G)) \cong \text{Hom}_{\mathcal{O}_X}(\tilde{M}, G),$$

so $M \mapsto \tilde{M}$ commutes with colimits and is exact, and commutes with pullbacks.

When $A$ is Noetherian, this also induces an equivalence between finite $A$-modules and coherent sheaves over Spec $A$, because finiteness for modules is local (5.4.1.5).

Proof: For any $A$-module $M$, there is a sheaf of modules $\mathcal{F}_M$ on $X = \text{Spec } A$ by (5.2.2.26). This is left adjoint to $\Gamma$ and defines a functor from the category of $A$-modules to the category of $\mathcal{O}_{\text{Spec } A}$-modules.

By universal property of $\mathcal{F}_M$ (5.2.2.26), there is a natural map $\mathcal{F}_M \to \tilde{M}$ corresponding to the ring map $M \to \Gamma(\text{Spec } A, M) = M$. The induced maps on the stalk at a point $x$ is $M \otimes_A \mathcal{O}_{X,x} \to M_x$, which is isomorphism, so $\mathcal{F}_M \cong \tilde{M}$.

From the universal property of $\tilde{M} = \mathcal{F}_M$, $\text{Hom}(\tilde{M}, \tilde{N}) = \text{Hom}(M, N)$, thus $\sim$ is fully faithful, to show it is an equivalence, it suffices to show for any Qco sheaf $\mathcal{F}$ on Spec $A$, the natural map $\Gamma(X, \mathcal{F}) \to \mathcal{F}$ is an isomorphism. Cf. [Sta]01IA.

If $0 \to M_1 \to M \to M_2 \to 0$ is exact, then $0 \to \tilde{M}_1 \to \tilde{M} \to \tilde{M}_2 \to 0$ is exact, because localization is exact. □

Prop. (5.5.1.3) [properties of (Quasi-)Coherent Sheaves on Schemes].

- $\mathcal{QCoh}(X)$ and $\mathcal{Coh}(X)$ are weak Serre subcategories of $\text{Mod}_{\mathcal{O}_X}$, and $\mathcal{Coh}(X)$ is a Serre subcategory of $\mathcal{QCoh}(X)$.
- Colimits in $\text{Mod}(\mathcal{O}_X)$ preserve $\mathcal{QCoh}(X)$, because localization is exact.
- Tensor product of two (Q)co sheaf is (Q)co, and locally free if they are locally free. More explicitly, $\tilde{M} \otimes_A \tilde{N} \cong \tilde{M} \otimes_{\mathcal{O}_X} \tilde{N}$ as tensor product commutes with $\pi^*$.
- If $\mathcal{F}$ is Qco, then so does $T(\mathcal{F}), \text{Sym}(\mathcal{F})$ and $\wedge(\mathcal{F})$, by (5.2.3.12).
- Given $\mathcal{F}, \mathcal{G} \in \mathcal{QCoh}(\mathcal{F})$ that $\mathcal{F}$ is f.p., $\text{Hom}(\mathcal{F}, \mathcal{G}) \in \mathcal{QCoh}(X)$, by (5.2.3.2) and (5.5.1.2). More explicitly, affine locally $\text{Hom}_{\mathcal{O}_X}(\tilde{M}, \tilde{N}) = \text{Hom}_A(M, N)$.
- Pullback preserves $\mathcal{QCoh}(X)$ and $\mathcal{Coh}(X)$, by (5.2.2.29). More explicitly, if $\text{Spec } B \subset Y$ is mapped into $\text{Spec } A \subset X$, then $f^*(\mathcal{F})(\text{Spec } B) = \mathcal{F}(\text{Spec } A) \otimes_A B$, using the fact $\tilde{M} = \mathcal{F}_M = \pi^* M$. \

Cf. [Sta]01IA.
Prop. (5.5.1.4) [Qco Sheaves of F.T./F.P]. Let $X = \text{Spec} \ A$ and $\mathcal{F} = \widetilde{\mathcal{M}}$ a Qco sheaf on $X$, then $\mathcal{F}$ is of f.t./f.p. if $M$ is of f.t./f.p. over $A$.

Proof: These follows from the fact finiteness/f.p. are local properties for modules over a ring (4.1.4.4).

Def. (5.5.1.5) [Locally Projective Qco Sheaves]. Let $X$ be a scheme, then a locally projective Qco sheaf is a Qco sheaf $\mathcal{F}$ on $X$ that is affine locally a locally projective module sheaf.

Proof: The question is local so we let $Y$ be affine, and then $X$ is qcqs, so we cover it with affine opens $U_i$ and their intersections are $U_{ijk}$. Then we see by sheaf property

$$0 \to f_\ast \mathcal{F} \to \bigoplus_i f_\ast (\mathcal{F}|_{U_i}) \to \bigoplus_{ijk} f_\ast (\mathcal{F}|_{U_{ijk}})$$

The last two are Qco because two are maps between affine schemes, so the first is Qco.

Prop. (5.5.1.6) [Qcqs Pushforward]. If $f$ is qcqs, then the pushforward of of a Qco sheaf is Qco. (Used in ??).

Proof: The question is local so we let $Y$ be affine, and then $X$ is qcqs, so we cover it with affine opens $U_i$ and their intersections are $U_{ijk}$. Then we see by sheaf property

$$0 \to f_\ast \mathcal{F} \to \bigoplus_i f_\ast (\mathcal{F}|_{U_i}) \to \bigoplus_{ijk} f_\ast (\mathcal{F}|_{U_{ijk}})$$

The last two are Qco because two are maps between affine schemes, so the first is Qco.

Prop. (5.5.1.7) [Qco Sheaves on Qcqs Schemes]. For a qcqs scheme $X$ and $s \in \Gamma(X, \mathcal{O}_X)$, and a Qco module $\mathcal{F}$, $(\Gamma(X, \mathcal{F}))_s \cong \Gamma(X_s, \mathcal{F})$.

Proof: The canonical map $f : X \to \text{Spec} \Gamma(X, \mathcal{O}_X)$ is qcqs, so $f_\ast \mathcal{F}$ is Qco on Spec $\Gamma(X, \mathcal{O}_X)$ by (5.5.1.6). Then the result follows from the fact $f^{-1}(\text{Spec} \Gamma(X, \mathcal{O}_X)_s) = X_s$ and the definition of $f_\ast$.

Lemma (5.5.1.8) [Extending Qco Sheaves]. Let $i : U \to X$ be a quasi-compact open immersion of schemes, $\mathcal{F}$ a Qco $\mathcal{O}_X$-module and $\mathcal{G} \subset \mathcal{F}|_U$ a Qco $\mathcal{O}_U$-submodule, then there exists a Qco $\mathcal{O}_X$-submodule $\mathcal{G}' \subset \mathcal{F}$ that $\mathcal{G}'|_U = \mathcal{G}$.

Proof: Immersion is separated (5.4.4.86), so $i_\ast \mathcal{G}$ is a Qco $\mathcal{O}_X$-sheaf by (5.5.1.6), and it is a submodule of $i_\ast \mathcal{F}$, so the kernel $\mathcal{H} = \ker(\mathcal{F} \oplus i_\ast \mathcal{G} \to i_\ast \mathcal{F})$ is also Qco by (5.5.1.3), and $\mathcal{H} \subset \mathcal{F}$, $\mathcal{H}|_U = \mathcal{G}$.

Prop. (5.5.1.9) [Extending Qco Sheaves of F.T.]. Let $X$ be a qcqs scheme, and $U \subset X$ a qc open subset, $\mathcal{F}$ a Qco $\mathcal{O}_X$-module and $\mathcal{G} \subset \mathcal{F}|_U$ a Qco $\mathcal{O}_U$-submodule of f.t., then there exists a Qco $\mathcal{O}_X$-submodule $\mathcal{G}' \subset \mathcal{F}$ of finite type that $\mathcal{G}'|_U = \mathcal{G}$.

Proof: Let $n$ be the minimal number of affine open subsets $U_i$ that $X = U \cup \bigcup U_i$, by induction on $n$, it suffices to prove for $n = 1$. Thus we may assume $X = U \cup V$ where $U, V$ are affine opens. Now $U \cap V$ is qc because $X$ is qs. Then we can change $(X, U)$ to $(V, U \cap V)$, because we can glue the resulting sheaf. Then we reduce to the case $X$ is affine.

Let $X = \text{Spec} \ R$ and $\mathcal{F} = \widetilde{\mathcal{M}}$, then by (5.5.1.8), there exists a Qco sheaf $\widetilde{N}$ that $\widetilde{N}|_U = \mathcal{G}$. By hypothesis we can cover $U$ by f.m. open affine $D(f_i)$ that $\mathcal{N}_{f_i}$ is f.g., by element $x_{ij}/f_i^{\alpha_i}$. Let $\mathcal{N}'$ be the submodule of $\mathcal{N}$ generated by these elements $x_{ij}$, then $\widetilde{\mathcal{N}}'$ meets our requirement.
Cor. (5.5.1.10) [Qco Sheaf is a Direct Union of Qco Sheaves of F.T.]. Let $X$ be a qcqs scheme, then any Qco sheaf $\mathcal{F}$ on $X$ is a direct colimit of its Qco subsheaves of f.t..

Proof: It is a direct colimit because the sum of two Qco sheaves of f.t. is also Qco of f.t. Now for any affine open $U \subset X$ and $s \in \mathcal{O}_X(U)$, $s$ generates a Qco $\mathcal{O}_U$-submodule of f.t. of $\mathcal{F}|_U$, and by (5.5.1.9) this extends to a Qco $\mathcal{O}_X$-submodule of $\mathcal{F}$. Then we see that the direct colimit of Qco subsheaves of f.t. of $\mathcal{F}$ contains elements of $\mathcal{F}(U)$ for any affine open subset $U$, thus it is just $\mathcal{F}$. □

Def. (5.5.1.11) [Rank of Sheaves]. Let $X$ be a scheme and $\mathcal{F}$ a Qco sheaf on $X$, then the rank of $\mathcal{F}$ at $p \in X$ is $\text{rank}_p(\mathcal{F}) = \dim_k \mathcal{F}_p/\mathfrak{m}_p \mathcal{F}_p$.

Prop. (5.5.1.12) [Maximal Qco Submodule]. For $X$ a scheme and any $\mathcal{O}_X$-module $\mathcal{F}$, there is a Qco submodule of $\mathcal{F}$ maximal among all Qco submodules of $\mathcal{F}$. This is because a direct colimit of Qco sheaves is Qco (5.5.1.3).

Prop. (5.5.1.13) [Integral and Finite Modules]. Let $X$ be a qcqs scheme and $\mathcal{A}$ an integral Qco $\mathcal{O}_X$-submodule, then
- $\mathcal{A}$ is the directed colimits of its finite Qco $\mathcal{O}_X$-modules.
- $\mathcal{A}$ is a direct colimit of finite and finitely presented Qco $\mathcal{O}_X$-modules.

Proof: Cf. [Sta] 0817. □

Def. (5.5.1.14). ?

Associated Points

Def. (5.5.1.15) [Weakly Associated Points]. Let $X \in \text{Sch}$ and $\mathcal{F} \in \mathcal{QCoh}(X)$, then a weakly associated point of $\mathcal{F}$ is the set of points $x \in X$ that $\mathfrak{m}_x \subset \mathcal{O}_{X,x}$ is weakly associated to the module $\mathcal{F}_x$. The set of w.ass points are denoted by $\text{WeakAsso}(\mathcal{F})$. The weakly associated points of $X$ is the weakly associated points of $\mathcal{O}_X$.

Similarly we can stalkwise define the set of associated points of $X$.

Def. (5.5.1.16) [Embedded Points]. Let $X$ be a scheme and $\mathcal{F}$ a Qco sheaf on $X$, then an embedded point of $\mathcal{F}$ is an associated point that is a specialization of another associated point.

Prop. (5.5.1.17) [Properties of Associated Points]. Let $X$ be a scheme and $\mathcal{F}_i$ be Qco sheaves on $X$, then
1. $\text{Ass}(\mathcal{F}) \subset \text{WeakAsso}(\mathcal{F}) \subset \text{Supp}(\mathcal{F})$.
2. If $0 \to \mathcal{F}_1 \to \mathcal{F}_2 \to \mathcal{F}_3 \to 0$ is an exact sequence, then $\text{WeakAss}(\mathcal{F}_1) \subset \text{WeakAss}(\mathcal{F}_2)$, and $\text{WeakAss}(\mathcal{F}_2) \subset \text{WeakAsso}(\mathcal{F}_1) \cup \text{WeakAsso}(\mathcal{F}_3)$.
3. $\text{WeakAss}(\mathcal{F}) = \emptyset$ iff $\mathcal{F} = 0$. 
4. The generic points of $\text{Supp}(\mathcal{F})$ are in $\text{WeakAsso}(\mathcal{F})$. In particular, generic points of $X$ are in $\text{WeakAss}(X)$.

5. If $X$ is locally Noetherian, then $\text{Ass}(\mathcal{F}) = \text{WeakAsso}(\mathcal{F})$.

6. If $X$ is reduced, then $\text{WeakAsso}(X)$ is just the generic points of $X$. In particular, $X$ has no embedded points.

7. If $X$ is locally Noetherian, then an associated point is an embedded point iff it is not a generic point of $\text{Supp}(\mathcal{F})$.

8. If $X$ is locally Noetherian and $\mathcal{F}$ is coherent, then $\mathcal{F}$ has no embedded points iff it satisfies $(S_1)$.

9. If $X$ is locally Noetherian of dimension $\leq 1$, then $X$ is C.M. iff it has no embedded points.

Proof: By (4.2.5.21), these reduces to the affine case, so they follows from

- (4.2.5.13)(4.2.5.16).
- (4.2.5.14).
- (4.2.5.16).
- (4.2.5.16).
- (4.2.5.21).
- (4.2.5.24).
- (4.2.5.23).
- [Sta]031Q.
- [Sta]0BXG.

Prop. (5.5.1.18). Let $X$ be a scheme and $\mathcal{F} \in \mathcal{Q}\mathcal{Coh}(X)$. If $U$ is an open subset of $X$ that contains $\text{WeakAsso}(\mathcal{F})$, then $\Gamma(X, \mathcal{F}) \to \Gamma(U, \mathcal{F})$ is injective.

Proof: If $s \in \Gamma(X, \mathcal{F})$ be a section that restricts to 0 on $U$, let $\mathcal{F}'$ be the subsheaf generated by $s$, then $\text{WeakAss}(\mathcal{F}') \subset \text{WeakAsso}(\mathcal{F})$, but $\text{Supp}(\mathcal{F}') \subset X \setminus U$, thus $\text{WeakAss}(\mathcal{F}') = 0$, so $\mathcal{F}' = 0$ by (5.5.1.17).

Prop. (5.5.1.19) [Schematically Dense and Associated Points]. Let $X$ be a locally Noetherian scheme and $U \subset X$ an open subset, then the following are equivalent:

- $U$ is schematically dense in $X$.
- $U$ is dense in $X$ and contains all the embedded points of $X$.
- $U$ contains $\text{Ass}(X)$.

Proof: The problem is local, so we assume $X = \text{Spec} A$, then 2, 3 are clearly equivalent.

Let $U = \bigcup_i D(f_i)$, then by (5.4.4.64), $U$ is schematically dense in $A$ iff $A \to \prod A_{f_i}$ is injective. If $p = \text{Ann}(x)$ for some $x \in A$, then $x$ maps to some non-zero element of $A_{f_i}$, then $f_i \notin p$, so $p \subset D(f_i) \subset U$. Conversely, if $\text{Ass}(X) \subset U$, then every map $A \to A_p$ factors through $A \to A_{f_i}$ for some $i$, so injectivity of $A \to \prod_{p \in \text{Ass}(X)} A_p$ implies injectivity of $A \to \prod_{i} A_{f_i}$.

Prop. (5.5.1.20). Let $X$ be a scheme and $\varphi: \mathcal{F} \to \mathcal{G} \in \mathcal{Q}\mathcal{Coh}(X)$ that $\mathcal{F}_x \to \mathcal{G}_x$ is injective for any $x \in \text{WeakAss}(\mathcal{F})$, then $\varphi$ is injective.
Proof: The hypothesis says $\text{WeakAss}(\ker(\varphi)) = 0$, so $\ker(\varphi) = 0$ by (5.5.1.17).

Fitting Ideals

Def. (5.5.1.21) [Fitting Ideals]. Let $X \in \text{Sch}$ and $F \in \mathcal{Q}\text{Coh}^\text{ft}(X)$, the fitting ideal of $F$ is defined to be $\text{fit}$.

Locally Free Sheaves

Prop. (5.5.1.22) [Locally Free is Stalkwise]. $F \in \mathcal{Q}\text{Coh}^\text{pf}(X)$ is locally free iff its stalks are all free, by (4.3.1.7).

Def. (5.5.1.23). Let $X \in \text{Sch}$ and $\delta : X \to \mathbb{N}$ a locally constant function, then the category of locally free sheaves of rank $\delta$ is denoted by $\mathcal{C}oh^\text{free}_\delta(X)$. The category of locally free sheaves is denoted by $\mathcal{C}oh^\text{free}(X)$

Prop. (5.5.1.24) [Locally Free Sheaves]. Suppose $0 \to F' \to F \to F'' \to 0$ is an exact sequence of sheaves on a scheme $X$, then

- If $F', F''$ are both locally free, then so is $F$.
- If $F, F'$ are both locally free of finite rank, then so is $F''$.

Proof: Firstly of all in each case all sheaves are Qco by (5.5.1.3).

1: on an affine open $U = \text{Spec } A \subset X$, the exact sequence is induced by $0 \to A' \to \Gamma(U, F) \to A^J \to 0$, so it splits and $\Gamma(U, F) \cong A^{I+J}$ is free.

2: on an affine open $U = \text{Spec } A \subset X$, the exact sequence is induced by $0 \to \Gamma(U, F') \to A^m \to A^n \to 0$, where the map $A^m \to A^n$ is represented by a $n \times m$ matrix $M$. Then $U$ is covered by open subsets $U_i$ that some $n \times n$ minor of $M$ is invertible. Then after a change of coordinates on each subset, $F(U_i) \cong A^{m-n}$.

Prop. (5.5.1.25). For a exact sequence $0 \to F' \to F \to F'' \to 0$ in $\mathcal{Q}\text{Coh}^\text{free}(X)$, there is a filtration of $\text{Sym}^r F$:

$$0 = G^{r+1} \subset G^r \subset \ldots \subset G^0 = \text{Sym}^r F$$

that

$$G^p / G^{p+1} \cong \text{Sym}^p F' \otimes \text{Sym}^{r-p} F''.$$ 

Proof: On any affine open subset, choose a splitting of the exact sequence, then use coordinates.

Prop. (5.5.1.26). For a exact sequence $0 \to F' \to F \to F'' \to 0$ in $\mathcal{C}oh^\text{free}(X)$, there is a filtration of $\wedge^r F$:

$$0 = G^{r+1} \subset G^r \subset \ldots \subset G^0 = \wedge^r F$$

that

$$G^p / G^{p+1} \cong \wedge^p F' \otimes \wedge^{r-p} F''.$$ 

In particular,

$$\wedge^r F' \otimes \wedge^r F'' \cong \wedge^r F.$$ 

and when $F'' \cong L$ is a line bundle, there is an exact sequence

$$0 \to \wedge^r (F') \to \wedge^r (F) \to \wedge^{r-1} (F') \otimes L \to 0$$
Proof: On any affine open subset, choose a splitting of the exact sequence, then use coordinates.

Prop. (5.5.1.27) [Perfect Pairing Wedge Product Sheaf]. Let $\mathcal{F}$ be a locally free sheaf of rank $n$, then there is a perfect pairing $\wedge^n \mathcal{F} \otimes \wedge^{n-r} \mathcal{F} \to \wedge \mathcal{F}$ which is a perfect pairing, i.e. it induces an isomorphism $\wedge^n \mathcal{F} \cong (\wedge^{n-r} \mathcal{F})^\vee \otimes \wedge \mathcal{F}$.

Proof: The map is natural, and the isomorphism can be seen at the level of stalks, by (5.2.3.11).

Prop. (5.5.1.28). Let $0 \to \mathcal{F} \to \mathcal{G} \to \mathcal{H} \to 0$ is an exact sequence in $\mathcal{QCoh}(X)$ where $\mathcal{H}$ is a locally free sheaf, then for any $\mathcal{Qco}$ sheaf $\mathcal{E}$ of $X$, then for any $\mathcal{Qco}$ sheaf $\mathcal{E}$ on $X$, there is an exact sequence of sheaves

$$0 \to \mathcal{Hom}(\mathcal{H}, \mathcal{E}) \to \mathcal{Hom}(\mathcal{G}, \mathcal{E}) \to \mathcal{Hom}(\mathcal{F}, \mathcal{E}) \to 0.$$  

In particular, $0 \to \mathcal{H}^\vee \to \mathcal{G}^\vee \to \mathcal{F}^\vee \to 0$ is exact.

Proof: As $\mathcal{Hom}(-, \mathcal{E})$ is left exact, it suffices to show the last one is surjective. This is local, so we may assume $0 \to \mathcal{F} \to \mathcal{G} \to \mathcal{H} \to 0$ is $0 \to M \to N \to \mathbb{P}^n \to 0$, so this sequence splits, and the then $\mathcal{Hom}(\mathcal{G}, \mathcal{E}) \to \mathcal{Hom}(\mathcal{F}, \mathcal{E})$ is surjective, by (5.5.1.3).

Prop. (5.5.1.29) [Grothendieck]. Every object in $\mathcal{Coh}^{\text{free},r}(\mathbb{P}^1_k)$ is isomorphic to $\bigoplus_{i=1}^r \mathcal{O}(a_i)$ for a unique non-decreasing sequence of integers $a_1, \ldots, a_r$.

Proof: Use induction on $r$. The $r = 1$ case follows from (5.5.3.16). For a general $r$, let $\mathcal{E} \in \mathcal{Coh}^{\text{free},r}(\mathbb{P}^1_k)$, then $\mathcal{E}(m)$ is generated by global sections for $m$ large as $\mathcal{O}_{\mathbb{P}^1}$ is ample, and $H^0(\mathcal{E}(-m)) = H^1(\mathcal{E}^\vee(m)) = 0$ by Serre duality and (5.7.2.5), so there is a maximal $m$ s.t. there is a non-zero map $\mathcal{O}(m) \to \mathcal{E}$. The image of this map is also locally free and has degree $\geq m$ by (5.11.2.8), so it must have degree $m$ and $\mathcal{O}_X(m) \to \mathcal{E}$ is injective by (5.11.2.8). Now the cokernel $\mathcal{F}$ is also locally free, because otherwise let $\mathcal{F}_{\text{tor}}$ be the torsion part of $\mathcal{F}$ (5.11.2.16), and let $\mathcal{N}$ be the inverse image of $\mathcal{F}_{\text{tor}}$ in $\mathcal{E}$, then it is locally free thus invertible, and $\mathcal{O}(m) \to \mathcal{N}$, so $N = \mathcal{O}(m)$ by (5.11.2.8), and $\mathcal{F}_{\text{tor}} = 0$.

There is an exact sequence

$$0 \to \mathcal{O}(-1) \to \mathcal{E}(-m-1) \to \mathcal{F}(-m-1) \to 0$$

which induces $H^0(\mathcal{E}(-m-1)) = H^0(\mathcal{F}(-m-1)) = 0$ as $H^1(\mathbb{P}_k^1, \mathcal{O}(-1)) = 0$, so by induction hypothesis $\mathcal{F} = \bigoplus_{i=1}^r \mathcal{O}(a_i)$ and $a_i \leq m$. To show this sequence splits, notice $\text{Ext}^1(\mathcal{F}(-m-1), \mathcal{O}(-1)) = \bigoplus_{i=1}^r H^1(\mathcal{O}(m-a_i)) = 0$.

Prop. (5.5.1.30) [Splitting Principal]. Let $X$ be an integral scheme and $\mathcal{E} \in \mathcal{Coh}^{\text{free}}(X)$, then there exists a modification $X' \to X$ s.t. $f^* \mathcal{E}$ has a filtration by invertible sheaves.

Proof: Use induction on rank($\mathcal{E}$). If rank($\mathcal{E}$) $\leq 1$, this is trivial, otherwise let rank($\mathcal{E}$) = $r$, $P = \mathbb{P}(\mathcal{E})$, then $\pi: P \to X$ is proper and there is a canonical surjection $\pi^* \mathcal{E} \to \mathcal{O}_P(1)$, with kernel in $\mathcal{Coh}^{\text{free},r-1}(P)$. Let $U$ be an open subset of $X$ s.t. $E$ is trivial, then $\pi^{-1}(U) \cong \mathbb{P}_U^{r-1}$. Let $s: U \to \mathbb{P}_U^{r-1}$ be a section, and let $X'$ be the scheme-theoretic closure of $U$, which is integral. Then $X' \to X$ is proper and thus a modification. Now $f^* \mathcal{E}$ has an invertible quotient, and we are done by induction hypothesis.
5.5. QUASI-COHERENT SHEAVES ON SCHEMES

Coherent Sheaves

Prop.(5.5.1.31)[Coh(X)]. The category of coherent sheaves on a scheme \( X \) is denoted by \( \text{Coh}(X) \).

When \( \mathcal{O}_X \in \text{Coh}(X) \), \( \text{Coh}(X) = \mathcal{QCo}^\text{ft}(X) \) (5.2.2.28).

In particular when \( X \) is locally Noetherian, \( \text{Coh}(X) = \mathcal{QCo}^\text{ft}(X) \). And the notion of coherence are used usually only when \( X \) is locally Noetherian.

(Quasi-)coherence is an affine local property by (5.2.2.30). \( \mathcal{QCo}(X) \) is an Abelian category, by (5.2.2.28).

Lemma(5.5.1.32). If \( f \) is finite, then \( f_* \) maps coherent sheaves to coherent sheaves.

Proof: This is trivial. \( \square \)

Prop.(5.5.1.33)[Proper Pushforward]. If \( f \) is a proper morphism between locally Noetherian schemes, then \( f_* \) maps coherent sheaves to coherent sheaves.

Proof: Immediate from Grothendieck’s coherence theorem (5.7.4.11). \( \square \)

Prop.(5.5.1.34)[Artin-Rees]. Let \( X \) be a Noetherian scheme, \( \mathcal{F} \) a coherent \( \mathcal{O}_X \)-module, \( \mathcal{G} \) a Qco subsheaf of \( \mathcal{F} \), \( \mathcal{I} \subset \mathcal{O}_X \) a Qco sheaf of ideals, then there exists some \( c > 0 \) that for all \( n \geq c \)

\[ \mathcal{I}^{n-c}(\mathcal{I}^n \mathcal{F} \cap \mathcal{G}) = \mathcal{I}^n \mathcal{F} \cap \mathcal{G}. \]

Proof: Cover \( X \) by f.m. affine open subsets, then this follows from the affine case (4.2.2.13). \( \square \)

Cor.(5.5.1.35)[Vanish Analytically]. Let \( X \) be a Noetherian scheme, \( \mathcal{F} \) a coherent \( \mathcal{O}_X \)-module, for any element \( f \in \bigcap_n \mathfrak{m}_x^n \mathcal{F} \), \( f \) vanishes at a nbhd of \( x \).

Proof: This follows from the intersection theorem (4.2.2.14). \( \square \)

Prop.(5.5.1.36)[Deligne]. On a Noetherian scheme \( X \), let \( \mathcal{F} \) be a Qco sheaf, \( \mathcal{G} \) be a coherent sheaf and \( \mathcal{I} \) be a Qco sheaf of ideals corresponging to \( Z, U = X - Z \), then we have

\[ \lim_{\rightarrow} \text{Hom}_{\mathcal{O}_X}(\mathcal{I}^n \mathcal{G}, \mathcal{F}) \cong \text{Hom}_{\mathcal{O}_U}(\mathcal{G}_|U, \mathcal{F}_|U). \]

In particular,

\[ \lim_{\rightarrow} \text{Hom}_{\mathcal{O}_X}(\mathcal{I}^n, \mathcal{F}) \cong \Gamma(U, \mathcal{F}). \]

Proof: Cf.[Sta]01YB. \( \square \)

Prop.(5.5.1.37)[Kleinmann]. If \( X \) is a Noetherian integral separated locally factorial scheme, then every coherent sheaf on \( X \) is a quotient of a finite locally free sheaf.

Proof: Cf.[Hartshorne P238]. \( ? \)

Prop.(5.5.1.38)[Support of Modules]. For \( X \in \text{Sch} \) and \( \mathcal{F} \in \mathcal{QCo}^\text{ft}(X) \), the support (5.2.2.2) \( \text{Supp}(\mathcal{F}) \) is closed by (5.2.2.24).

For a flat morphism \( f \), \( \text{Supp}(f^*(\mathcal{F})) = f^{-1}(\text{Supp}\mathcal{F}) \), by (5.2.2.18).

Proof: because affine locally, for a set of generators \( x_i \) of \( M \), \( \text{Ann}(\mathcal{F}) = \bigcup \text{Ann}(x_i) \), and \( \text{Ann}(x_i) \) is closed. \( \square \)

Cor.(5.5.1.39). Any coherent sheaf on an integral scheme is locally free over a dense open subset.
Cor. (5.5.1.40) [Geometric Nakayama]. If $\mathcal{F} \in \mathcal{Qcoh}^f(X)$ and for some $p \in U \subset X$ and $a_1, \ldots, a_n \in \mathcal{F}(U)$ generate $\mathcal{F}_p \otimes k(p)$, then there is an affine nbhd $V \subset U$ that $a_1, \ldots, a_n$ generate $\mathcal{F}(V)$.

Cor. (5.5.1.41) [Upper-Semicontinuity of Ranks]. For a Qco sheaf $\mathcal{F}$ of f.t. over $X$, the rank function $p \mapsto \text{rank}_p(\mathcal{F})$ is an upper semicontinuous function on $X$.

**Proof:** By Nakayama, $\varphi(y)$ is equal to the minimal number of generators of the $\mathcal{O}_y$-module $\mathcal{F}_y$. But these generators extends to a nbhd of $y$, so $\varphi \leq n$ on this nbhd. \hfill $\square$

Def. (5.5.1.42) [Schematic Support]. Let $X$ be a scheme and $\mathcal{F}$ a Qco sheaf of f.t. over $X$, then the **annihilating ideal** is the ideal $\mathcal{I} \subset \mathcal{O}_X$ that is affine-locally defined by $\text{Ann}(\mathcal{F}(U)) \subset \mathcal{O}_X(U)$, and the **schematic support** $\text{Supp}(\mathcal{F})$ of $\mathcal{F}$ is the closed subscheme of $X$ corresponding to $\text{Ann}(\mathcal{F})$.

Prop. (5.5.1.43). Let $\mathcal{F}$ be a Qco sheaf of f.t. over a reduced scheme that the rank function $\text{rank}_p(\mathcal{F})$ is locally constant, then it is locally free.

**Proof:** Let $\text{rank}_p(\mathcal{F}) = n$, by (5.5.1.38), for any $x \in X$, there exists an affine nbhd $U = \text{Spec} \ A$ of $x$ and a surjection $f : \mathcal{O}_U^n \to \mathcal{F}_U$. Consider the kernel of $f$. If $(r_1, \ldots, r_n)$ is in the kernel and $r_1 \neq 0$, then $r_1 \notin p$ for some prime $p$ of $A$, as $A$ is reduced. Then $\text{rank}_{x_p}(\mathcal{F}) < n$, contradiction. \hfill $\square$

**Torsion-Free Sheaves**

Def. (5.5.1.44) [Torsion Sheaves]. Let $X$ be an integral scheme, then a **torsion sheaf** is a Qco sheaf that its stalk at the generic point of $X$ vanishes. Equivalently, for any affine open $U \subset X$, $\mathcal{F}(U)$ is a torsion $\mathcal{O}_X(U)$-module.

Prop. (5.5.1.45). Any

Prop. (5.5.1.46). A torsion $\mathcal{O}_X$-module of f.t. on an integral scheme vanish on a dense open subset.

Prop. (5.5.1.47). For $X$ integral, any $\mathcal{F} \in \mathcal{Qcoh}(X)$ factors as $0 \to \mathcal{F}_{\text{tor}} \to \mathcal{F} \to \mathcal{F}_{\text{tf}} \to 0$, where $\mathcal{F}$ is a torsion sheaf (5.5.1.44) and $\mathcal{F}_{\text{tf}}$ is Qco and torsion-free.

Cor. (5.5.1.48). The subpresheaf $U \to \{s \in \mathcal{F}(U) | s_\eta = 0\}$ is a sheaf, and it is also Qco as on an affine open $U \subset X$, it is just $\mathcal{F}(U)_{\text{tor}}$. So the quotient is clearly Qco and torsion-free.

**Devissage of Coherent Sheaves**

Lemma (5.5.1.49). Let $X$ be a Noetherian scheme and $\mathcal{F} \in \mathcal{Coh}(X)$, let $\mathcal{I}$ be a sheaf of ideals that correspond to $Z$, then $\text{Supp}(\mathcal{F}) \subset Z$ iff $\mathcal{I}^n\mathcal{F} = 0$ for some $n$. (This follows easily from Noetherian and (4.2.5.8)).

Lemma (5.5.1.50). Let $X$ be a Noetherian scheme and $\mathcal{F} \in \mathcal{Coh}(X)$ s.t. $\text{Supp}(\mathcal{F}) = Z_1 \cup Z_2$ where $Z_1, Z_2$ are closed, then there is an exact sequence of coherent sheaves $0 \to \mathcal{G}_1 \to \mathcal{F} \to \mathcal{G}_2 \to 0$ that $\text{Supp}(\mathcal{G}_i) \subset Z_i$.

**Proof:** Let $\mathcal{I}$ be the ideal defining the induced reduced structure of $Z_2$, we use the exact sequence $0 \to \mathcal{I}^n\mathcal{F} \to \mathcal{F} \to \text{Coker} \to 0$ and use (5.5.1.49) on $X \setminus Z_2$ to find $n$ large that $\text{Supp}(\mathcal{I}^n\mathcal{F}) \subset Z_1$, and notice Coker has support in $Z_2$. \hfill $\square$
Lemma (5.5.1.51). Let \( X \) be an integral scheme and \( Z \subset X \) an integral closed subscheme with generic point \( \xi \). If \( F \in \text{Coh}(X) \) satisfies \( F_\xi \) is annihilated by \( m_\xi \), then there exists some \( r \geq 0 \) and sheaf of ideals \( I \) on \( Z \) and an injection \( i_*(I^{\oplus r}) \hookrightarrow F \) that is an isomorphism at \( \xi \).

Proof: Cf.[Sta]01YE.

Prop. (5.5.1.52). Let \( X \) be a Noetherian scheme and \( F \in \text{Coh}(X) \), then there is a filtration of coherent sheaves that the quotients are pushforward of ideal sheaves on integral subschemes of \( X \). This is analogous to the filtration in the module case.

Proof: We consider the set of these counterexamples and their \( \text{Supp} \), then use Noetherian induction. The minimal one \( Z \) is irreducible, otherwise from (5.5.1.50) we find a filtration for it. Let the ideal of sheaf of the induced reduced structure of \( Z \) be \( I \), then \( I^nF = 0 \) for some \( n \) by (5.5.1.49), then we may assume \( IF = 0 \). Then we use (5.5.1.51) to finish the proof.

Cor. (5.5.1.53) [Basic Devissage]. Let \( X \) be a Noetherian scheme and \( P \) be a property of coherent sheaves on \( X \) s.t.

1) for an exact sequence of sheaves: \( 0 \to F_1 \to F \to F_2 \to 0 \) if \( F_i \) has \( P \), then \( F \) has \( P \).

2) for any integral closed subscheme \( i : Z \subset X \) and any \( \text{Qco} \) sheaf of ideals \( I \) on \( Z \), \( P \) holds for \( i_*I \).

then \( P \) holds for any coherent sheaf of \( X \).

Lemma (5.5.1.54). Cf.[Sta]01YH.

Prop. (5.5.1.55) [Devissage of Coherent Sheaves I]. Let \( X \) be a Noetherian scheme and \( P \) be a property of coherent sheaves on \( X \) s.t.

1) for an exact sequence \( 0 \to F_1 \to F \to F_2 \to 0 \in \text{Coh}(X) \), if two of them have \( P \), then the third also has \( P \).

2) For every integral closed subscheme \( Z \) of \( X \) with generic point \( \xi \), there is a \( G \in \text{Coh}(X) \) that

(a) \( \text{Supp} G = Z \).
(b) \( G_\xi \cong \mathcal{O}_X/m_\xi \).
(c) \( P \) holds for \( G \).

Then \( P \) holds for every coherent sheaf on \( X \).

Proof: Suppose otherwise, let \( Z \) be the minimal counterexample of item 2 of (5.5.1.55). Then it is easily seen that \( P \) holds for any \( F \) with support strictly contained in \( Z \). Then take \( G \) as in item 2, and let \( 0 \to i_*(I^{\oplus r}) \to G \to \text{Coker} \to 0 \), then \( \text{Supp}(\text{Coker}) \) is strictly contained in \( Z \), and \( r = 1 \) by hypothesis, so \( i_*I \). Then for any other sheaf of ideals \( I' \) on \( Z \), \( I' \) is supported on a smaller subscheme, then it has \( P \), otherwise there are two exact sequences

\[
0 \to i_*I \to i_* (I + I') \to Q \to 0,
\]

\[
0 \to i_*I' \to i_* (I + I') \to Q \to 0,
\]

where \( I, Q \) are supported on smaller subschemes, so \( P \) also holds for \( I' \).

Prop. (5.5.1.56) [Devissage of Coherent Sheaves II]. Let \( X \) be a Noetherian scheme and \( P \) be a property of coherent sheaves on \( X \) s.t.
(1) for an exact sequence of sheaves: \(0 \rightarrow \mathcal{F}_1 \rightarrow \mathcal{F} \rightarrow \mathcal{F}_2 \rightarrow 0\), if \(\mathcal{F}_i\) has \(P\), then \(\mathcal{F}\) has \(P\).

(2) If \(\mathcal{F}^{\text{tr}}\) has \(P\), then \(\mathcal{F}\) has \(P\).

(3) For every integral closed subscheme \(Z\) of \(X\) with generic point \(\xi\), there is a \(\mathcal{G} \in \text{Coh}(X)\) that

(a) \(\text{Supp}\, \mathcal{G} = Z\).

(b) \(\mathcal{G}_{\xi}\) is annihilated by \(m_{\xi}\).

(c) For every sheaf of ideals \(\mathcal{I}\) on \(X\) that \(\mathcal{I}_{\xi} = \mathcal{O}_{X,\xi}\), there is a Quco subsheaf \(\mathcal{G}' \subset \mathcal{I}\mathcal{G}\) that \(\mathcal{G}'_{\xi} = \mathcal{G}_{\xi}\) and \(P\) holds for \(\mathcal{G}'\).

Then \(P\) holds for every coherent sheaf on \(X\).

Proof: Cf.\([\text{Sta}]01YM\).

\[\square\]

2 Projective Spaces

Prop.(5.5.2.1). For any graded ideal \(I \subset S\), \(V_+(I) = \emptyset\) iff \(S_+ \subset \sqrt{I}\).

Proof: \[\square\]

Def.(5.5.2.2)[Projective Schemes]. For a graded ring \(S\), we have a scheme \(\text{Proj}(S)\) that consists of homogenous primes of \(S\) minus \(S_+\) and the affine cover is \(D(f) = \{p|f \not\in p\}\), and \(\mathcal{O}(D(f)) = \text{Spec}\, S(f)\), where \(S(T)\) is the degree zero part of \(T^{-1}S\). It has \(\mathcal{O}_p = S(p)\).

Proof: Cf.\([\text{Sta}]01M5\)?

\[\square\]

Cor.(5.5.2.3). For any graded ring \(S\), \(\text{Proj}(S)\) is a separated scheme.

Proof: Check that for standard affine opens \(D_+(f)\) and \(D_+(g)\), \(D_+(f) \cap D_+(g) = D_+(fg)\) is affine open, and \(S(f) \otimes \mathbb{Z}\, S(g) \rightarrow S(fg)\) is surjective, which are both clear. \[\square\]

Prop.(5.5.2.4)[Representing Functor of Projective Schemes]. Let \(S\) be a graded ring generated by \(S_1\) over \(S_0\), then \(\text{Proj}(S)\) represents the functor that maps a scheme \(Y\) to the set of pairs \((\mathcal{L}, \psi)\), where \(\mathcal{L}\) is an invertible sheaf on \(Y\), and \(\psi: S \rightarrow \Gamma_+(Y, \mathcal{L})\) is a graded ring homomorphism that \(\mathcal{L}\) is generated by the global sections \(\psi(S_1)\), up to strict equivalences.

Proof: Cf.\([\text{Sta}]01NA\). \[\square\]

Prop.(5.5.2.5)[Associated Quco Sheaves]. Let \(M\) be a graded \(S\)-module, then

- there is a unique Quco sheaf \(\widetilde{M} \in \text{Qcoh}(\text{Proj}(S))\) s.t. \(\Gamma(D_+(f), \widetilde{M}) = M_f\) and the restrictions are compatible with base changes..

- For a point \(x \in \text{Proj}(S)\) corresponding to a homogenous prime not containing \(S_+\), \(\widetilde{M}_x = M_\psi\).

- \(M \mapsto \widetilde{M}\) is an exact functor from the category of graded \(S\)-modules to \(\text{Qcoh}(\text{Proj}(S))\).

- There is a canonical ring map \(S_0 \rightarrow \Gamma(\text{Proj}(S), \mathcal{O}_{\text{Proj}(S)})\) and canonical \(S_0\)-module map \(M_0 \rightarrow \Gamma(\text{Proj}(S), \widetilde{M})\).

Proof: ?

4: This follows from the fact short exact sequences can be checked on stalks, and item2. \[\square\]

Cor.(5.5.2.6). There is a canonical morphism of schemes \(\text{Proj}(S) \rightarrow \text{Spec}\, S_0\).
Prop. (5.5.2.7). If $X \subset \mathbb{P}_k^n$ is a closed subvariety disjoint from a $d$-dimensional subspace $L \subset \mathbb{P}_k^n$, then the projection $\pi : X \to \mathbb{P}^{n-d-1}$ with center $L$ induces a finite map $X \to \pi(X)$.

Proof: Cf.[Shafarovich 1, P63].

Cor. (5.5.2.8). If $F_0, \ldots, F_s$ are forms of degree $m > 0$ on $\mathbb{P}_k^n$ having no common zero on a closed subvariety $X \subset \mathbb{P}^n$, then $\varphi(x) = [F_0(x), \ldots, F_s(x)]$ defines a finite map $\varphi : X \to \varphi(X)$.

Proof: Let $v_m : \mathbb{P}^n \to \mathbb{P}^N$ be the Veronese embedding of degree $m$, then $X \to v_m(X)$ is an isomorphism, and $\varphi$ is a composition of $v_m$ and a projection $\mathbb{P}_k^N \to \mathbb{P}_k^n$, thus it is a finite map, by (5.5.2.7).

Prop. (5.5.2.9) [Tensor and Proj]. For two graded ring with the same $S_0 = A$, Proj($S \times_A T$) $\cong X \times_A Y$, where $(S \times_A T)_n = S_n \times_A T_n$.

Proof:

Def. (5.5.2.10) [Relative Proj]. The relative Proj $S$ over locally Noetherian $Y$ of a Qco graded $\mathcal{O}_Y$-algebra $S$ f.g. over $S_0$ by coherent $S_1$ is the glueing of locally Proj $S$. Proj $S \to Y$ is locally projective thus proper. It is equipped with invertible sheaf $\mathcal{O}(1)$ by glueing.

Prop. (5.5.2.11) [Closed Subscheme of Projective Scheme]. The closed scheme of $X = \mathbb{P}_A^n$ corresponds to the saturated homogenous ideal $I_Y$, (i.e. for any $s$, if there is an $n$ that for any $i, x_i^n s \in I_Y$, then $s \in I_Y$).

So projective scheme over Spec $S_0$ corresponds to Proj $S$, where $S$ are f.g. over $S_0$ by $S_1$ saturated in the sense above.

Proof: A closed immersion is proper, thus the kernel $I_Y$ of the structural map is a Qco (5.5.1.3), so it must be an ideal on every affine open, because Qco is affine local. Then we should use (5.5.3.6), $\Gamma_s(I_Y)$ will suffice. Cf.[Hartshorne Ex2.5.10].

Prop. (5.5.2.12). The global section of a projective space Proj $S \to$ Spec $S_0$ is just $S_0$, this is by (5.5.3.6).

Prop. (5.5.2.13). A quasi-projective scheme $X$ over a field $k$ of dimension $r$ can be covered by $r + 1$ open affine subsets. This is because there are $r$ hyperplane that intersect $X$ non-empty. This can happen by choosing a hyperplane non-intersecting the generic point of $X$, otherwise we choose many hyperplane, then their intersection is empty.

Sheaves on Proj

Def. (5.5.2.14) [Serre Twisting Sheaves]. Let $S$ be a graded ring and $X = \text{Proj}(S)$, there are Qco Serre twisting sheaves $\mathcal{O}_X(n) = \mathcal{S}(n)$. For $\mathcal{F} \in \mathcal{QCoH}(\text{Proj}(S))$, the Serre twisting sheaf of $\mathcal{F}$ is the sheaf $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{O}_X(n)$.

Prop. (5.5.2.15). Let $S$ be a graded ring and $X = \text{Proj}(S)$,

1. there are canonical maps

$$\mathcal{O}_X(m) \otimes_{\mathcal{O}_X} \mathcal{O}_X(n) \to \mathcal{O}_X(m + n),$$

inducing a map of graded rings $S \to \Gamma_s(X, \mathcal{O}_X) = \oplus_{n \geq 0} \Gamma(X, \mathcal{O}_X(n))$. 
2. For any $\mathcal{F} \in \text{Sh} (\mathcal{O}_X)$, there are canonical maps

$$\mathcal{O}_X (n) \otimes \mathcal{O}_X \mathcal{F} \to \mathcal{F} (n).$$

inducing a map of graded module structure of $\Gamma_*(X, \mathcal{O}_X)$ on $\Gamma_*(X, \mathcal{F}) = \oplus_{n \geq 0} \Gamma_*(X, \mathcal{F} (n))$.

3. There is a canonical map $\Gamma_*(X, \mathcal{F}) \to \mathcal{F}$ that is identity on global sections.

4. For any graded $S$-module $M$, let $M (n) = M \otimes_S S (n)$, there are maps $\tilde{M} (n) \to \tilde{M} (n)$. (Use property of Qco sheaves).

5. For graded rings $M, N$ over $S$, there are canonical maps $\tilde{M} \otimes \mathcal{O}_X \tilde{N} \to \tilde{M} \otimes_S \tilde{N}$.

Proof:

Prop. (5.5.2.16). Let $S$ be a graded ring s.t. $S$ is generated by $S_1$ over $S_0$, then

1. $(M \otimes_S \tilde{N}) (f) \cong M (f) \otimes_{S (f)} \tilde{N} (f)$ for $f \in S_1$.

2. There canonical maps in item 1, 4, 5 of (5.5.2.15) are isomorphisms.

3. For a graded ring map $S \to T$, we have the corresponding Proj map $f : U \to T$ that $f^* (\tilde{M}) \cong (M \otimes_S T) |_U$ and $f^* (\tilde{N}) |_U \cong \tilde{N} |_U$. That’s to say, $f^* (\tilde{M} (n)) = f^* (\tilde{M} (n))$ and $f^* (\tilde{M} (n)) = f^* (\tilde{M} (n))$. □

Proof: 1:

2: By 1 and check locally that tensoring $f^!$ is an isomorphism on $D_+ (f)$. □

Cor. (5.5.2.17). $\mathcal{O}_X (n) \otimes \mathcal{O}_X (m) \cong \mathcal{O}_X (n + m)$ for any scheme $X$ projective over $Y$.

Prop. (5.5.2.18) [Twisting of Proj]. With notation as in (5.5.2.10), Let $S' = S \ast \mathcal{L} ; S'_d = S_d \otimes \mathcal{L}^d$, then $\varphi : \text{Proj} S' \to \text{Proj} S$ is an isomorphism that induces

$$\mathcal{O}' (1) \cong \varphi^* \mathcal{O} (1) \otimes \pi'^* \mathcal{L}.$$

Prop. (5.5.2.19). If $Y$ is Noetherian and admits an ample invertible sheaf, then by definition, we have $S_1 \otimes \mathcal{L}^n$ is base point free for some $n$, thus we have a morphism $\text{Proj} (S \ast \mathcal{L}^n) \to \mathbb{P}_Y^n$, so $P = \text{Proj} S$ is $H$-quasi-projective with $\mathcal{O} (1) = \mathcal{O}_P (1) \otimes \pi^* \mathcal{L}^n$.

Relative Projective Spaces

Def. (5.5.2.20) [Relative Projective Spaces].

Def. (5.5.2.21) [Relative Projective Bundles]. Let $S$ be a scheme, $\pi : V \to S$ is called an Qco vector bundle if it is affine, and $\pi_* \mathcal{O}_V$ endowed with the structure of a graded $\mathcal{O}_S$-algebra structure $\pi_* \mathcal{O}_V = \oplus \mathcal{E}_n$, where $\mathcal{E}_0 = \mathcal{O}_S$, and Sym$^n \mathcal{E}_1 \to \mathcal{E}_n$ is an isomorphism for any $n$. The category of Qco vector bundles on $S$ is denoted by $\text{Vect}^{\text{Qcoh}} (S)$.

A morphism of affine bundles is a map $E' \to E$ over $S$ that the associated map $f_* : \pi_* \mathcal{O}_V \to \pi'_* \mathcal{O}_{V'}$ is compatible with grading.

For $\mathcal{E} \in \text{Qcoh} (X)$, we can define the associated vector bundle $V (\mathcal{E})$ as $\text{Spec}_S \text{Sym} (\mathcal{E}) (5.2.3.10)(5.2.7.12)$. In this way, the category of Qco vector bundles over $S$ is anti-equivalent to the category of Qco $\mathcal{O}_S$-algebras.

For $\mathcal{E} \in \text{Qcoh} (X)$, we can define the associated projective bundle $P (\mathcal{E})$ as $\text{Proj}_S \text{Sym} (\mathcal{E}) (5.2.3.10)(5.2.7.12)$. It is equipped with a Serre twisting sheaf $\mathcal{O} (1)$, which is the glue of locally the Serre sheaf in projective space. There is a surjective morphism $\pi^* (\mathcal{E}) \to \mathcal{O} (1)$ (local check).
Prop. (5.5.2.22). Let \( g : Y \to X \) by a scheme over \( X \), a morphism \( Y \to \mathbb{P}(\mathcal{E}) \) over \( X \) is equivalent to an invertible sheaf \( \mathcal{L} \) on \( Y \) and a surjective map \( g^* \mathcal{E} \to \mathcal{L} \).

In particular, giving a morphism \( X \to \mathbb{P}(\mathcal{E}) \) over \( X \) is equivalent to an invertible sheaf with \( n \) generators.

Proof: If there is a morphism, it will pullback \( \pi^* \mathcal{E} \to \mathcal{O}(1) \) into \( g^* \mathcal{E} \to L \). For the converse, construct locally and glue, we have the natural morphisms \( A[x_1/x_1, \ldots, x_n/x_1] \to \mathcal{O}_{X,s_i} : x_j/x_1 \to s_j/s_i \) in a homogenous sense. It is natural hence glue together. For the module, maps \( x_i \to s_i \). □

Cor. (5.5.2.23). All automorphisms of \( \mathbb{P}^n_k \) is linear.

Proof: The Picard group of \( \mathbb{P}^n_k \) is \( \mathbb{Z} \) and is generated by \( \mathcal{O}(1) \), so the automorphism will map \( \mathcal{O}(1) \) to \( \mathcal{O}(\pm 1) \) and \( \mathcal{O}(-1) \) has no global section. And the globals section is \( n \)-dimensional and determines the morphism by the prop. □

Def. (5.5.2.24)[Projective Space]. Let \( A \) be a ring, the projective space \( \mathbb{P}^n_A \) is defined to be \( \mathbb{P}^n_A = \text{Proj}(A[T_0, \ldots, T_n]) \) with \( \deg(T_i) = 1 \). It represents the functor that maps a scheme \( T \) to the equivalence classes of pairs \( (\mathcal{L}, (s_0, \ldots, s_n)) \), where \( \mathcal{L} \) is an invertible sheaf on \( T \), and \( s_0, \ldots, s_n \in \Gamma(T, \mathcal{L}) \) that generate \( \mathcal{L} \) by (5.5.2.22). For any scheme \( S \), \( \mathbb{P}^n \times Z S \) is called the projective space over \( S \).

Prop. (5.5.2.25). Let \( R \) be a ring and \( X = \mathbb{P}^n_R, F \in \mathcal{QCoh}(X) \), then the canonical map \( \Gamma_s(X, F) \to F \) is an isomorphism.

Proof: Cf.[Sta]03GM. This is a corollary. □

Prop. (5.5.2.26)[Closed Subschemes of \( \mathbb{P}^n_R \)]. Let \( Z \) be a closed subscheme of \( \mathbb{P}^n_R \), then it is of the form

\[ Z = \text{Proj}(R[X_0, \ldots, X_n]/I) \subset \text{Proj}(R[X_0, \ldots, X_n]) \]

where \( I = \oplus I_n \) and \( I_n = \ker(R[X_0, \ldots, X_n]_d \to \Gamma(Z, \mathcal{O}_Z)) \).

Proof: Cf.[Sta]03GI. □

Prop. (5.5.2.27)[Segre Embedding]. Let \( S \) be a scheme, there is a natural closed immersion

\[ \mathbb{P}^n_S \times_S \mathbb{P}^n_S \to \mathbb{P}^{mn+m+n}_S \]

called the Segre embedding.

Proof: It suffices to prove for \( S = Z \), and in this case, it suffices to write down an invertible sheaf on \( \mathbb{P}^n_S \times_S \mathbb{P}^n_S \) with \( (n+1)(n+1) \) global sections that generate it. Then we take the invertible sheaf \( \mathcal{L} = \pi_1^* \mathcal{O}_{\mathbb{P}^m}(1) \oplus \pi_2^* \mathcal{O}_{\mathbb{P}^n}(1) \) and the sections \( X_i Y_j \), where \( (X_0, \ldots, X_m) \) generate \( \mathcal{O}_{\mathbb{P}^m}(1) \) and \( (Y_0, \ldots, Y_n) \) generate \( \mathcal{O}_{\mathbb{P}^n}(1) \).

It is a closed immersion by[Sta]01WD. □

Prop. (5.5.2.28)[Venerose Embedding].
3 Invertible Sheaves

General invertible sheaves on a ringed site is treated in 5.

Prop. (5.5.3.1) [Faithfully Flat Descent]. To show a quasi-coherent sheaf is a line bundle, it suffices to show fpqc-locally, by (4.4.2.1).

Def. (5.5.3.2) [Basepoint-Free Line Bundles]. Let \( \mathcal{L} \) be a line bundle over a scheme \( X \) over a field \( k \), then it is called basepoint free if the intersections \( \{ \text{div}(s) \mid s \in H^0(V) \} \) is empty.

Prop. (5.5.3.3). If \( X \) is qcqs over a field \( k \) and \( K \triangleleft k \) is a field extension, then \( \mathcal{L} \) is basepoint free over \( X_K \).

Proof: By flat base change (5.7.5.1), \( H^0(X_K, \mathcal{L}_K) = H^0(X, \mathcal{L}) \otimes_k K \).

Prop. (5.5.3.4) [Relative Triviality]. Let \( f : X \to Y \) be a finite morphism of schemes and \( \mathcal{L} \in \text{Pic}(X) \), then for any \( y \in Y \), there exists a nbhd \( U \) of \( y \in Y \) s.t. \( \mathcal{L}|_{f^{-1}(U)} \) is trivial.

Proof: Cf. [Sta]0BUT.

Prop. (5.5.3.5) [Global Sections]. Let \( \mathcal{L} \) be an invertible sheaf over qcqs scheme \( X \), for \( F \in \mathcal{QCoh}(X) \), let the global section functor \( \Gamma_* (F) = \oplus \Gamma(X, F \otimes \mathcal{L}^n) \), then

\[ \Gamma_* (F)_{(f)} \cong F(X_f) \]

where \( s \in \Gamma(X, \mathcal{L}) \). In particular that if there is a section \( f \) of \( F \) on \( X_s \), then for some \( n \), \( f \otimes s^n \) is a global section of \( F \otimes \mathcal{L}^n \).

Proof: This is nearly the same as the proof that \( (\text{Spec } A)_f = \text{Spec } A_f \), Cf. [Sta]0PW.

Cor. (5.5.3.6). When \( X = \text{Proj } S \) projective over \( \text{Spec } S_0 \) and \( F \in \mathcal{QCoh}(X) \), \( \Gamma_*(F) \cong F \), where \( \Gamma_*(F) = \oplus_{n \in \mathbb{Z}} \Gamma(X, F(n)) \), which is a graded \( S \)-module. In particular, \( \Gamma_* \) for projective space \( P^n_A \) equals \( A[x_1, \ldots, x_n] \).

Def. (5.5.3.7) [Regular Sections].

Prop. (5.5.3.8) [Complete Series]. Let \( H^0(X, \mathcal{L}) \) be the sections that corresponds to injective maps \( \mathcal{L}^{-1} \to \mathcal{O}_X \), then there is a canonical isomorphism

\[ H^0(X, \mathcal{L})_{\text{reg}}/H^*(X, \mathcal{O}_X^n) \cong |\mathcal{L}|. \]

Notice when \( X \) is not integral, \( H^0(X, \mathcal{L})_{\text{reg}} \) may not equal \( H^0(X, \mathcal{L}) \).

Proof: Cf. [Kle05]P22.

Prop. (5.5.3.9) [Meromorphic Sections]. Let \( X \) be a locally Noetherian scheme having no embedded points, then every invertible sheaf \( \mathcal{L} \in \text{Pic}(X) \) has a meromorphic section. In particular, this applies for \( X \) integral, by (5.5.1.17).

Proof: Cf. [Sta]0EMI.
Picard Groups

Remark (5.5.3.10) [Picard Groups]. The Picard group \( \text{Pic}(X) \) of a local ringed space \((X, \mathcal{O}_X)\) is defined in (5.2.5.7), and it is isomorphic to \( H^1(X, \mathcal{O}_X) \) by (5.3.1.17).

Prop. (5.5.3.11) [Class Group]. If \( X = \text{Spec} \mathcal{O} \) where \( \mathcal{O} \) is a Dedekind domain, then by (4.2.7.8), the isomorphism class of invertible sheaves on \( X \) is equivalent to the isomorphism class of fractional ideals modulo principle ideals. Thus \( \text{Pic}(\mathcal{O}) \) equals the class group of \( \mathcal{O}(4.2.7.9) \). In particular, if \( R \) is a UFD, then \( \text{Pic}(\text{Spec} R) = 0 \).

Def. (5.5.3.12) [Invertible Sheaf Associated to Cartier Divisors]. For a Cartier divisor on a scheme \( X \), we can define \( \mathcal{O}(D) \) the line bundle associated to \( D \) as the sub \( \mathcal{O}_X \)-module of \( K \) locally generated by \((f_i^{-1})\), where \( D = (f_i) \) locally. Equivalently, it is the line bundle \( \mathcal{I}_D^{-1} \).

Def. (5.5.3.13) [Linear Series]. Let \( \mathcal{L} \in \text{Pic}(X) \), then denote \(|\mathcal{L}|\) the complete linear series of effective Cartier divisors \( D \) s.t. \( \mathcal{L}(D) \cong \mathcal{L} \).

Def. (5.5.3.14) [Weil divisor of an invertible Sheaf]. For \( X \) a locally Noetherian integral scheme and \( \mathcal{L} \) an invertible sheaf in \( \mathcal{K} \), if \( s \in \Gamma(X, \mathcal{K} \otimes \mathcal{L}) \) is a meromorphic section of \( \mathcal{L} \) (which exists by (5.5.3.9)), for any prime Weil divisor \( Z \) with generic pt \( \eta \), define \( \text{ord}_Z(s) = \text{ord}_{\mathcal{O}_{Z,\eta}}(s/s_\eta) \) (4.1.2.10), for any \( s_\eta \) a generator of \( \mathcal{L}_\eta \) over \( \mathcal{O}_{X,\eta} \). This is independent of \( s_\eta \) chosen.

The prime Weil divisors that \( \text{ord}_Z(s) \neq 0 \) is locally finite, the same as in (6.1.2.18). And any two different sections \( s_i \) defines Weil divisors up to a difference of \( \text{div}(f)(6.1.2.18) \). So we can define the Weil divisor class associated to \( \mathcal{L} \) as \( \sum \text{ord}_Z(s)[Z] \) for any meromorphic section \( s \) of \( \mathcal{L} \).

It is easy to verify that this induces a homomorphism from \( \text{Pic}(X) \) to \( \text{Cl}(X) \).

Prop. (5.5.3.15) [Cl-Pic]. For a normal integral locally Noetherian scheme, the above map \( \text{Pic}(X) \to \text{Cl}(X)(5.5.3.14) \) is an injection. It is an isomorphism iff all local rings of \( X \) are UFD.

Explicitly, the inverse image of a prime Weil divisor \( D \) is the sheaf \( \mathcal{O}_X(D) = \text{Hom}(\mathcal{I}_D, \mathcal{O}_X) = \mathcal{I}_D^{-1} \), and there is an exact sequence of sheaves on \( X \):

\[ 0 \to \mathcal{O}_X(-D) = \mathcal{I}_D \to \mathcal{O}_X \to i_*\mathcal{O}_D \to 0 \]

In particular, this applies to non-singular prevarieties over a field \( k \), by (5.4.2.8).

Proof: If it is not injective, then some meromorphic section on \( \mathcal{L} \) has no associated Weil divisors, then it suffices to show \( \mathcal{L} \) is trivialized by \( s \). Consider on an affine subscheme Spec \( A \), then \( \text{ord}_{A_p}(s) = 0 \) for each minimal prime \( p \) of \( A \), but \( A_p \) is DVR by (4.3.5.20), so \( s \in A_p^* \) for each minimal prime \( p \), so \( s \in A_*^* \) (4.3.5.11). This shows \( s \) trivialize \( \mathcal{L} \).

To show it is surjective, it suffices to show any Weil divisor \( D \) is in the image: notice \( D \) is an effective Cartier divisor by (5.8.1.4), and by definition (5.8.1.5) the vanishing of the canonical section \( 1_D \in \mathcal{O}_X(D) \) is exactly \( D \).

Prop. (5.5.3.16) [Examples of Picard Groups].

- If \( X \) is a locally Noetherian normal integral separated scheme, then so are \( X \times \text{Spec} \mathbb{Z}[T] \) and \( \mathbb{P}^n_X \), and \( \text{Cl}(X \times \text{Spec} \mathbb{Z}[T]) = \text{Cl}(X) \) and \( \text{Cl}(\mathbb{P}^n_X) = \mathbb{Z} \oplus \text{Cl}(X) \).

- For a UFD \( R \), \( \text{Pic}(\mathbb{A}^n_R) = 0 \).

- For a UFD \( R \), \( \text{Pic}(\mathbb{P}^n_R) \cong \text{Cl}(\mathbb{P}^n_R) \cong \mathbb{Z} \), and it is generated by \( \mathcal{O}_{\mathbb{P}^n_R}(1) \).
• For a UFD $R$, $\text{Pic}(\mathbb{P}^1_R \times \mathbb{P}^1_R) \cong \text{Cl}(\mathbb{P}^1_R \times \mathbb{P}^1_R) \cong \mathbb{Z} \oplus \mathbb{Z}$.

• If $k$ is a field and $Y \subset \mathbb{P}^n_k$ is a hypersurface of degree $d$, then $\text{Pic}(\mathbb{P}^n_k \setminus Y) \cong \text{Cl}(\mathbb{P}^n_k \setminus Y) \cong \mathbb{Z}/d\mathbb{Z}$.

Proof: By $(5.5.3.15)$ and $(6.1.5.7)(6.1.7.10)(6.1.5.8)(6.1.5.9)$. □

Prop. (5.5.3.17). Let $X$ be a complete prevariety over a field $k$ of characteristic $p > 0$, then for any $n$ prime to $p$ and any purely inseparable field extension $k'/k$, the natural map

$$\text{Pic}(X)[n] \to \text{Pic}(X_{k'})[n]$$

is an isomorphism.

Proof: Cf. [Sta]0CD5. □

4 Ample Invertible Sheaves

Prop. (5.5.4.1). Let $X \in \text{Sch}$ and $\mathcal{L} \in \text{Pic}(X)$. Then for any affine open $U \subset X$ and a section $s$ of $\mathcal{L}$, $X_s \cap U$ is affine.

Proof: It suffices to show: If $R$ is a ring, $N$ is an invertible $R$-module and $s \in N$, then $U = \{p|s \notin pN\}$ is an affine open subset of $\text{Spec} R$. For this, let $R' = \lim_{\rightarrow} - \otimes N^{\otimes m}$, then in fact $U = \text{Spec} R'$. Because locally, $R'$ is just $R_s$ via an isomorphism $N_f \cong R_f$. □

Def. (5.5.4.2) [Ample Invertible Sheaves]. On a quasi-compact scheme $X$, an ample invertible sheaf is a line bundle $\mathcal{L} \in \text{Pic}(X)$ s.t. there is some $n \in \mathbb{Z}_+$ and sections $s_i \in \Gamma(X, \mathcal{L}^n)$ that $X_{s_i}$ is an affine cover of $X$. In particular, an ample invertible sheaf is globally generated.

For a qc morphism $f: X \to Y$, an invertible sheaf on $X$ is called $f$-ample iff it is ample restricted to every open subscheme $f^{-1}(V)$, where $V$ is an affine open in $Y$. In particular, an invertible sheaf $\mathcal{L}$ on a quasi-compact scheme $X$ is ample iff it is $f$-ample where $f: X \to \text{Spec} Z$.

Prop. (5.5.4.3). An invertible sheaf $\mathcal{L}$ is $(f)$-ample iff $\mathcal{L}^m$ is $(f)$-ample.

Prop. (5.5.4.4) [Ample Implies Separatedness]. When there is a $f$-ample invertible sheaf for $f: X \to Y$ qc, then $f$ is separated. In particular, if there is an ample line bundle over a qc scheme $X$, then $X$ is separated.

Proof: [Sta]09MP. □

Prop. (5.5.4.5) [Characterizing Ampleness]. Let $X$ be a qc scheme and $\mathcal{L}$ be an invertible sheaf on $X$, $S = \Gamma_*(X, \mathcal{L})$, then the following are equivalent:

1. $\mathcal{L}$ is ample.

2. The open subsets $X_s$, where $s \in \Gamma_*(X, \mathcal{L})$ homogeneous, cover $X$, and the associated morphism $X \to \text{Proj} S$ is an open immersion.

3. The open subsets $X_s$ where $s \in \Gamma_*(X, \mathcal{L})$ homogeneous, form a topological basis for $X$.

4. The open subsets $X_s$ that is affine and where $s \in \Gamma_*(X, \mathcal{L})$ homogeneous, form a topological basis for $X$.

5. For any Qco sheaf $\mathcal{F}$ on $X$, the sum of images of the canonical maps $\Gamma(X, \mathcal{F} \otimes \mathcal{L}^n) \otimes \mathcal{L}^{-n} \to \mathcal{F}$ is surjective.
6. $X$ is quasi-separated, and for any Qco sheaf $\mathcal{F}$ on $X$ of f.t., $\mathcal{F} \otimes \mathcal{L}^\otimes n$ is generated by global sections for $n$ sufficiently large.

7. $X$ is quasi-separated, and for any Qco sheaf $\mathcal{F}$ on $X$ of f.t., there exists an integer $n$ that $\mathcal{F}$ is a quotient of a direct sum of f.m. copies of $\mathcal{L}^\otimes -n$.

Proof: Cf.[Sta]01Q3. □

**Cor.(5.5.4.6).** The pullback of an ample invertible sheaf along a qc immersion is an ample invertible sheaf.

**Cor.(5.5.4.7).** Let $S$ be a quasi-separated scheme and $X, Y$ be schemes over $S$. If $\mathcal{L}$ is an ample invertible sheaf over $X$ and $\mathcal{N}$ an ample invertible sheaf over $Y$, then $\mathcal{M} = \text{pr}_1^* \mathcal{L} \otimes \mathcal{O}_{X \times_S Y} \text{pr}_2^* \mathcal{N}$ is ample over $X \times_S Y$.

Proof: Because $X \times_S Y \to X \times Y$ is a qc immersion, by(5.5.4.6), it suffices to show for $S = \text{Spec } Z$. Then if $X_i$ is an affine nbhd of $x$ and $Y_i$ is an affine nbhd of $y$, then $(X \times Y)_{\pi_i}^* s \otimes s^\mathcal{L}_i$ is an affine nbhd of $x \times y$. □

**Cor.(5.5.4.8) [Tensor Product of Ample Invertible Sheaves is Ample].** If $M$ an invertible sheaf generated by global sections and $\mathcal{L}$ is an ample invertible sheaf, then $\mathcal{L} \otimes M$ is ample. In particular if $\mathcal{L}, \mathcal{M}$ are ample invertible sheaves, then $\mathcal{L} \otimes \mathcal{M}$ is ample.

Proof: For any $x \in X$ and $U$ a nbhd of $x$, choose $s \in \Gamma(X, \mathcal{L}^n)$ that $x \in X_s \subset U$, and choose $t \in \Gamma(X, \mathcal{M})$ that $t_x \neq 0$, then $x \in X_{s \otimes t^\mathcal{M}} \subset U$, thus $X_r$ form a basis for $X$ where $r \in \Gamma(X, (\mathcal{L} \otimes \mathcal{M})^n)$, so $\mathcal{L} \otimes \mathcal{M}$ is ample. □

**Cor.(5.5.4.9).** If $\mathcal{L}$ is ample and $\mathcal{M}$ is an invertible sheaf, then $\mathcal{M} \otimes \mathcal{L}^\otimes n$ is ample for $n$ sufficiently large.

Proof: This is because $\mathcal{L} \otimes \mathcal{M}^n$ is generated by global sections for $n$ sufficiently large, thus $\mathcal{L} \otimes \mathcal{M}^{n+1}$ is ample, by(5.5.4.8). □

**Prop.(5.5.4.10) [Gluing Ample Invertible Sheaves].** Let $X$ be a qc scheme s.t. there is an affine open covering of the form $X_{s_i}$ where $s_i$ are sections of $\mathcal{L}_i$ and $\mathcal{L}_i$ are globally generated line bundles in $\text{Pic}(X)$, then $X$ has an ample line bundle.

Proof: Let $X_{s_i}$ be an affine open covering of $X$ where $s_i$ are sections of globally generated invertible sheaves $\mathcal{L}_i, i = 1, \ldots, r$. As $\mathcal{L}_i$ are globally generated, let $X = \bigcup_j X_{i,j}$ for $j = 0, 1, \ldots, m_i$ where $t_{i0} = s_i$. Then for the line bundle $\otimes_i \mathcal{L}_i$, the sections $t_{1,j_1} \otimes \ldots \otimes t_{r,j_r}$ where at least one of $j_i$ equals 0, covers $X$, and they are all affine by(5.5.4.1). So $\otimes_i \mathcal{L}_i$ is ample. □

**Prop.(5.5.4.11).** $f : X \to Y$, let $\mathcal{L}$ be $f$-ample on $X$ and $\mathcal{M}$ ample on $Y$, then $\mathcal{L} \otimes f^* \mathcal{M}^n$ is ample for $n$ large.

Proof: Cf.[Sta]0892? □

**Cor.(5.5.4.12).** If $f : X \to Y$ is quasi-affine, then the pullback of an ample invertible sheaf is ample, by(5.4.4.19) and(5.5.4.3).

**Prop.(5.5.4.13) [Pullback of Ampleness].** If $f : Y \to X$ is finite and surjective morphism between schemes proper over a Noetherian affine scheme, then for any invertible sheaf $\mathcal{L}$ on $X$, $\mathcal{L}$ is ample iff $f^* \mathcal{L}$ is ample.
Proof: Cf.[Sta]0B5V.

One direction follows from (5.5.4.12). For the other we use Serre criterion (5.7.2.8) and devise-
sage (5.5.1.56). We only verify 3: By (5.4.4.42), there exists such coherent sheaf $f_*\mathcal{F}$ for any integral
subscheme, and for any Qco sheaf of ideals $I$, $I f_*\mathcal{F} = f_*(f^{-1}I \mathcal{F})$ because $f$ is affine, thus

$$H^p(X, I f_*\mathcal{F}) = H^p(X, f_*(f^{-1}I \mathcal{F} \otimes \mathcal{L}^n)) = H^p(Y, f^{-1}I \mathcal{F} \otimes \mathcal{L}^n)$$

by projection formula, and $f$ is affine. This vanish for $n$ large. □

Cor. (5.5.4.14) [Ampleness and Irreducible Components]. Let $X$ be a scheme proper over a
Noetherian affine scheme, then an invertible sheaf $\mathcal{L}$ on $X$ is ample iff it is ample on the induced
reduced structure of irreducible components of $X$.

Proof: This is (5.5.4.13) applied to the case $\coprod X_i \rightarrow X$. □

Prop. (5.5.4.15) [Ampleness Restricted to Reduced Case]. If $i: Z \rightarrow X$ is a closed immersion of
schemes that induce homeomorphism on the underlying topology, then $\mathcal{L}$ is ample iff $i^*\mathcal{L}$ is ample.

In particular, this applies to $X_{\text{red}} \rightarrow X$.

Proof: Cf.[Sta]09MW. □

Prop. (5.5.4.16). Let $f: X \rightarrow Y$ be a proper morphism of schemes and $\mathcal{L}$ an invertible sheaf on $X$.
If $y \in Y$ satisfies $\mathcal{L}_y$ is ample on $X_y$, then there is a nbhd $U$ of $y \in Y$ that $\mathcal{L}|_{f^{-1}(U)}$ is $f$-ample.

Proof: Cf.[Sta]0D2S. □

Prop. (5.5.4.17) [Finite Map and Ample]. Let $\mathcal{L}$ be a basepoint-free line bundle on a proper
scheme $X$, then the associated map $X \rightarrow \text{Proj}(\mathcal{O}_X, \mathcal{L})$ is finite iff $\mathcal{L}$ is ample.

Proof: Cf.[Positivity in Algebraic Geometry, P28]. □

Prop. (5.5.4.18). Let $X$ be a scheme. Let $\mathcal{L}$ be an ample invertible $\mathcal{O}_X$-module. Let $n_0$ be an integer.
If $H^p(X, \mathcal{L}^{-n}) = 0$ for $n \geq n_0$ and $p > 0$, then $X$ is affine.

Proof: Cf.[Sta]0EBD. □

Prop. (5.5.4.19) [Descent of Ample Line Bundles]. Let $K/k$ be a field extension, $X$ a scheme
over $k$ s.t. there exists an ample line bundle on $X_K$, then $X$ also has an ample line bundle.

Proof: Cf.[Sta]0BDC. □

Very Ample Invertible Sheaves

Def. (5.5.4.20) [Very Ampleness]. Let $f: X \rightarrow S$ be a morphism, a $f$-very ample invertible sheaf
on $X$ is the pullback of $\mathcal{O}(1)$ along some immersion $X \rightarrow \text{Proj}(\mathcal{E})$ for some Qco module $\mathcal{E}$ over $Y$,
Cf.(5.5.2.14). It is called H-very ample iff $\mathcal{E}$ is trivial. Notice when $X$ is proper, this immersion
must be closed by (5.4.5.3).

When $S$ is affine and $f: X \rightarrow S$ is of f.t., $f$-very ample is equivalent to H-very ample.

Proof: Cf.[Sta]02NP. □
Prop.(5.5.4.21) [Tensor Product of Very Ample Line Bundles]. Let \( f : X \to \text{Spec } A \) be a morphism. If \( L \) is H-very ample and \( M \) is generated by global sections, then \( L \otimes M \) is H-very ample. In particular, the tensor product of two H-very ample invertible sheaves is H-very ample.

Proof: The hypothesis means \( L = \varphi^*O(1) \), where \( \varphi : X \to P^n_k \) is an immersion, and \( M = \psi^*O(1) \), where \( \psi : X \to P^m_k \) is a morphism. Then the product \( T : X \to P^n_k \times P^m_k \) is also an immersion, by base change trick (5.4.4.2), as \( P^n_k \times P^m_k \to P^n_k \) is separated. Then \( S \circ T : X \to P^{mn+m+n} \), where \( S : P^n_k \times P^m_k \to P^{mn+m+n} \) is the Segre embedding, is also an immersion, and \((ST)^*O(1) \cong L \otimes M \), thus it is H-very ample.

Prop.(5.5.4.22) [Ample and H-Very Ample]. If \( f : X \to S \) is locally of f.t. and \( L \) is an ample invertible sheaf on \( X \), then \( L^{\otimes m} \) is H-very ample for \( m \) sufficiently large.

Proof: Choose an affine open cover \( \{V_i\} \) of \( S \). By (5.5.4.5), there are f.m. affine opens \( X_{s_i} \) that cover \( X \) refining a inverse image of \( \{V_i\} \). Now \( O_X(X_{s_i}) \) is f.g. over \( O_S(V_i) \), so we can find f.m. \( f_{ij} \in O_X(X_{s_i}) \) that generates it over \( O_S(V_i) \). By (5.5.3.5), we can write each \( f_{ij} = s_{ij}/s_{ij}^{e_{ij}} \) for some \( a_{ij} \) homogenous. We can multiply by a factor to make all the \( s_{ij}^{e_{ij}} \) the same degree \( N \), and \( f_{ij} = s_{ij}s_i^{N/\text{deg}(s_i)-e_{ij}} \), then all the elements \( s_i, s_{ij} \) generates the invertible sheaf \( L \), thus inducing a map \( j : X \to P^m_k \). This map is an immersion, because \( j^{-1}(D(T_i)) = X_{s_i} \) and the function \( T_{ij}/T_i \) on \( D(T_i) \) pulls back to \( s_{ij}/s_{ij} \). Thus \( j \) is locally a closed immersion, thus an immersion.

Now \( L^{\otimes d_1} \) is H-very ample for some \( d_1 \), in particular it is separated, and by (5.5.4.5) there is some \( d_2 \) that \( L^{\otimes d} \) is generated by global sections for all \( d \geq d_2 \), then by (5.5.4.21), \( L^{\otimes d} \) is H-very ample for \( d \geq d_1 + d_2 \).

Prop.(5.5.4.23) [f-very Ample Implies f-Ample]. If \( f : X \to S \) is qc, then \( f \)-very ample implies \( f \)-ample.

Proof: Cf.[Sta]01VN. □

Cor.(5.5.4.24) [Serre]. If \( f : X \to S \) is of f.t. and \( S \) is affine, \( L \) is an invertible sheaf on \( X \), then the following are equivalent:

- \( L \) is ample .
- \( L \) is \( f \)-ample.
- \( L^{\otimes n} \) is \( (H-)f \)-very ample for some (all large)\( n \).

Proof: This follows from (5.5.4.20)(5.5.4.22) and (5.5.4.23). □

Cor.(5.5.4.25). If \( f : X \to S \) is of f.t. and \( S \) is quasi-compact, \( L \) is an invertible sheaf on \( X \), then the following are equivalent:

- \( L \) is \( f \)-ample.
- \( L^{\otimes n} \) is \( (H-)f \)-very ample for some (all large)\( n \).

Proof: Cf.[Sta]01VU. □

5 Sheaf of Differentials

Prop.(5.5.5.1) [Differentials on Schemes]. Consider a morphism of schemes \( X \to Y \), we define the sheaf of differentials \( \Omega_{X/Y} \) together with an \( S \)-derivative \( O_X \to \Omega_{X/S} \) as for ringed sites (5.2.4.7).
Then it is a Qco sheaf by \((5.2.4.5)\). In fact, if \(U = \text{Spec } A\) is mapped into \(\text{Spec } B \subset S\), then \(\Omega_{X/S}(U) \cong \Omega_{A/B}\).

In particular, the stalk of \(\Omega_{X/S}\) at a point \(x \in X\) is \(\Omega_{\mathcal{O}_{X,x}/\mathcal{O}_{S,f(x)}}\).

Thus when \(X \to Y\) is locally of f.t.(or locally of f.p.), then \(\Omega_{X/S}\) is an \(\mathcal{O}_X\)-module of f.t.(or of f.p.).

**Prop.(5.5.5.2) [Base change and Differentials].** Let \(\xymatrix{ X' \ar[r]^-f & X \ar[d]^g \cr S' \ar[r]_g & S }\) be a commutative diagram of schemes, then there is a canonical map

\[ f^* \Omega_{X/S} \to \Omega_{X'/S'} \]

which is an isomorphism if the diagram is a fiber product square.

**Proof:** Such a diagram gives a diagram \((f^{-1}g^{-1}\Omega_S \to f^{-1}\Omega_X) \to ((g')^{-1}(\mathcal{O}_{S'}) \to \mathcal{O}_{X'})\) of sheaves of rings on \(X'_{zar}\), thus the conclusion follows from \((5.2.4.5)\) and \((5.2.7.17)\).

**Prop.(5.5.5.3).** Let \(X, Y\) be schemes over another scheme \(S\), then

\[ \pi_1^* \Omega_{X/S} \oplus \pi_2^* \Omega_{Y/S} \cong \Omega_{X \times_S Y/S}, \]

where the maps are given by \((5.5.5.2)\).

**Proof:** It suffices to check on affine subschemes, so we may assume \(X, Y, S\) are affine, thus the map is given by

\[ \Omega_{A/S} \oplus_S B \oplus_{A \otimes_S B} \Omega_{B/S} \otimes_S A \to \Omega_{A \otimes_S B/S} \]

which is an isomorphism by \((4.4.3.6)\).

**Prop.(5.5.5.4).** Let \(X, Y\) be schemes over another scheme \(S\), then \(\Omega_{X \times_S Y/S} \cong \pi_1^* \Omega_{X/S} \oplus \pi_2^* \Omega_{Y/S}\).

**Prop.(5.5.5.5) [Jacobi-Zariski Sequence].** Let \(f : X \to Y\) and \(g : Y \to Z\), then there is an exact sequence of sheaves on \(X\):

\[ f^* \Omega_{Y/Z} \to \Omega_{X/Z} \to \Omega_{X/Y} \to 0. \]

Where the maps come from \((5.5.5.2)\).

**Proof:** Immediate from \((4.4.3.8)\).

**Prop.(5.5.5.6).** The stalk of the differential sheaf \(\Omega_{X/k}\) at a rational point \(x\) of a scheme over a field \(k\) is just the Zariski cotangent space \(m_x/m_x^2\) \((5.6.4.22)\).

**Proof:** Using the Jacobi exact sequence \((4.4.3.8)\) on an affine nbhd \(\text{Spec } A\) of \(x\) for \(A\) and \(m_x\). Then we verified that there is a right inverse of \(A/m^2 \to k(x) = x\), then it follows that \(m_x/m_x^2 \cong \Omega_{A/k} \otimes_A k(x) = \Omega_{A_{m_x}/k}\) which is the stalk of \(\Omega_{X/k}\) by \((5.5.5.1)\).

**Prop.(5.5.5.7) [Euler Exact Sequence].** If \(X = \mathbb{P}^n_A = \text{Proj}(A[x_0, \ldots, x_n])\) over \(Y = \text{Spec } A\), then there is an exact sequence

\[ 0 \to \Omega_{X/A} \to (\mathcal{O}_X(-1))^{n+1} \to \mathcal{O}_X \to 0. \]

\(\Omega_{X/A}\) is locally free by \((5.10.1.16)\), so by taking dual and exterior powers,

\[ 0 \to \mathcal{O}_X \to \mathcal{O}_X(1)^{n+1} \to T_X \to 0, \quad K_X \cong \mathcal{O}_X(-n-1). \]
5.5. QUASI-COHERENT SHEAVES ON SCHEMES 605

Proof: Let \( S = A[x_0, \ldots, x_n] \), \( E = S(-1)^{\oplus n+1} \) with a basis \( e_0, \ldots, e_n \), then there is a map of \( S \)-graded modules \( E \to S \) with kernel \( M \). \( E \to S \) is surjective in all dimension \( \geq 1 \), so we have an exact sequence

\[
0 \to \tilde{M} \to \tilde{E} \to \mathcal{O}_X \to 0.
\]

Notice \( E_{(x_i)} \to S_{(x_i)} \) is given by \( e_j \mapsto x_j/x_i \), so \( \tilde{M}|_{D(x_i)} \) is a free sheaf generated by sections \( 1/x_i e_j - (x_j/x_i^2)e_i, j \neq i \). So we can define \( \varphi_i : \Omega_{X/A}|_{D(x_i)} \to \tilde{M}|_{D(x_i)} : d(x_j/x_i) \mapsto 1/x_i e_j - (x_j/x_i^2)e_i, j \neq i \) mapping isomorphically onto the kernel. It suffices to show this map glue to a map \( \Omega_{X/A} \to \tilde{E} \): On \( D(x_i,x_j) \), \( x_k/x_i = (x_k/x_j) \cdot (x_j/x_i) \), so

\[
d(\frac{x_k}{x_i}) - \frac{x_k}{x_j}d(\frac{x_j}{x_i}) = \frac{x_j}{x_i}d(\frac{x_k}{x_j}).
\]

Applying \( \varphi_i \) to the LHS and \( \varphi_j \) to the RHS gives the same element \( 1/x_i e_k - (x_k/x_i x_j)e_j \), which shows compatibility. \( \square \)

Conormal Sheaves

Def.(5.5.5.8) [Conormal Sheaf of an Immersion]. Let \( i : Z \to X \) be a closed immersion with corresponding sheaf of ideals \( \mathcal{I} \). Consider the Qco sheaf \( \mathcal{I}/\mathcal{I}^2 \), which is annihilated by \( \mathcal{I} \), thus corresponds to a sheaf on \( Z \) by (5.2.6.18), called the conormal sheaf \( \mathcal{C}_{Z/X} \) of \( Z \).

More generally, if \( i \) is any immersion, we can define the conormal sheaf as the conormal sheaf of the closed immersion \( i : Z \to X \setminus \partial Z \). And also the normal sheaf \( \mathcal{N}_{Z/X} \) is defined to be \( \mathcal{N}_{Z/X} = \text{Hom}_{\mathcal{O}_X}(\mathcal{I}/\mathcal{I}^2, \mathcal{O}_Z) \).

Prop.(5.5.5.9) [Pullback of Conormal Sheaf]. Let \( \begin{array}{c} Z' \to X' \to Z \to X \end{array} \) be a fiber product square where \( i, i' \) are immersions, then the canonical map

\[
f^\ast \mathcal{C}_{Z'/X} \to \mathcal{C}_{Z/X}
\]

is surjective, and if \( g \) is flat, it is an isomorphism.

Proof: Change \( X' \to X \setminus \partial Z' \) and \( X \to X \setminus (g^{-1} \partial Z' \cup \partial Z) \), we may assume \( i \) is a closed immersion. Then we may localize to the case \( X' \) and \( X \) is affine. Then we notice if \( R' \to R \) is a ring map and \( I' \subset R' \) is an ideal, with \( I = I'R \), then \( (I'/I')^2 \otimes_{R'} R \to I/I^2 \) is surjective, and if \( R/R' \) is flat, then \( I \cong I' \otimes_{R'} R \), and the map is an isomorphism. \( \square \)

Prop.(5.5.5.10). Let \( Z \to Y \to X \) be immersions of schemes, then there is a canonical exact sequence

\[
i^\ast \mathcal{C}_{Y/X} \to \mathcal{C}_{Z/X} \to \mathcal{C}_{Z/Y} \to 0
\]

Proof: By changing \( Y \to Y \setminus \partial Z \) and \( X \to X \setminus (\partial(Y \setminus Z)) \), we can assume the immersions are closed immersion. Now by restricting to affine subsets, it suffices to show that for surjective ring maps \( C \to B \to A \), if \( I = \ker(B \to A), J = \ker(C \to A), K = \ker(C \to B) \), then there is an exact sequence

\[
K/K^2 \otimes_B A \to J/J^2 \to I/I^2 \to 0.
\]

But this follows from the observation \( K = \ker(J \to I) \). \( \square \)
Prop. (5.5.5.11) [Conormal Sheaf of the Diagonal]. Let \( f : X \to S \) be a morphism, then there is a canonical isomorphism between \( \Omega_{X/S} \) and the conormal sheaf of the diagonal \( \Delta : X \to X \otimes_S X \).

**Proof:** Cf. [Sta]08S2. \( \square \)

Cor. (5.5.5.12). If \( f : X \to S \) is a monomorphism, e.g. an immersion, then \( \Omega_{X/S} = 0 \).

Prop. (5.5.5.13). If \( f : Z \to X \) is an immersion of schemes over \( S \), then there is an exact sequence of sheaves on \( Z \):
\[
\mathcal{C}_{Z/X} \to i^*\Omega_{X/S} \to \Omega_{Z/S} \to 0.
\]

**Proof:** Replace \( X \) be \( X \setminus \partial Z \), we can assume \( f \) is a closed immersion. This follows immediate from (5.2.4.6). \( \square \)

Prop. (5.5.5.14). If \( i : Z \to X \) is an immersion over \( S \) that locally has a left inverse, then the canonical sequence
\[
0 \to \mathcal{C}_{Z/X} \to i^*\Omega_{X/S} \to \Omega_{Z/S} \to 0.
\]
is locally split exact. In particular, if \( s : S \to X \) is a section of the structure morphism \( X \to S \), then the map \( \mathcal{C}_{S/X} \to s^*\Omega_{X/S} \) is an isomorphism.

**Proof:** Cf. [Sta]0474. \( \square \)

Prop. (5.5.5.15). Let \( \begin{array}{ccc}
Z & \xrightarrow{i} & X \\
\downarrow j & & \downarrow \\
Y & \end{array} \) be a commutative diagram where \( i, j \) are immersions, then there is a canonical exact sequence
\[
\mathcal{C}_{Z/Y} \to \mathcal{C}_{Z/X} \to i^*\Omega_{X/Y} \to 0,
\]
where the first arrows comes from (5.5.5.9) and the second map comes from (5.5.13).

**Proof:** By replacing \( Y \) by \( Y \setminus \partial Z \) and \( X \) by \( X \setminus (\partial i(Z) \cup \partial j(Z)) \), then we may assume \( i, j \) are closed immersion. Then we check locally, the exactness follows from (8.2.1.5). \( \square \)
5.6 More Properties of Schemes

Main references are [Sta].

Notations (5.6.0.1). • Use notations defined in Properties of Schemes.

1 Finitely Presentedness

Def. (5.6.1.1) [Locally of Finite Presentation]. A morphism between schemes \( f : Y \to X \) is called of locally finite presentation iff for any point \( x \in X \), there is an open affine mapped into an open affine that the ring map is of finite presentation. It is called of finite presentation iff moreover it is qcqs.

Locally of finite presentation is local on the source and target and it is stable under composition and base change but it doesn’t satisfies the base change trick by (5.4.1.6)(5.4.1.5) and (4.3.7.9).

Prop. (5.6.1.2). Open immersion is locally of finite presentation.

Prop. (5.6.1.3). When the target is locally Noetherian, (locally)finite type and (locally)finite presentation is equivalent.

Prop. (5.6.1.4). For \( f : X \to Y \) over \( S \), if \( X/S \) is locally of f.p. and \( Y/S \) is locally of f.t., then \( f \) is locally of f.p.. If moreover \( X \) is of f.t. and \( Y \) is qs, then \( f \) is of f.t..

Proof: The first follows from (4.3.7.11), the second needs to check qcqs. Qc follows from (5.4.4.27).

□

Prop. (5.6.1.5) [Chevalley]. A qc morphism locally of f.p. maps locally constructible subset to locally constructible subset.

Proof: We prove \( f(E) \cap U_i \) is constructible for every \( U_i \) affine open in \( X \). The inverse image of \( U_i \) is qc, hence a locally constructible set is constructible (3.8.3.10). So we reduce to the affine case (4.1.7.3).

□

Cor. (5.6.1.6). As in the proposition, if \( Y \) is qc, and the image is dense in \( Y \), then it contains an open dense subset of \( Y \), by (3.8.3.17).

2 Flatness

Def. (5.6.2.1) [Flatness for Schemes]. Flat modules and flat morphisms over schemes are defined in the same way as that of ringed spaces (5.2.2.15).

Prop. (5.6.2.2). Flatness is stalkwise by (5.2.2.17), it is stable under base change and compositions.

Thus for \( F \in \Coh(X) \) is flat over \( X \) iff it is locally free, by (4.4.1.10)

For any affine open subsets \( \text{Spec} A \subset X \), \( \Gamma(\text{Spec} A, F) \) is flat over \( A \), because flatness is also stalkwise for modules (4.1.4.2). Similarly, a morphism of schemes \( f : X \to Y \) is flat iff for any affine opens \( \text{Spec} B \subset X, \text{Spec} A \subset Y \) that \( f(\text{Spec} B) \subset \text{Spec} A \) is flat over \( A \).

Prop. (5.6.2.3). For a flat morphism of ringed space, \( f^* \) is exact.

Proof: Because it is \( f^{-1} \) followed by tensoring with \( \mathcal{O}_X \), check on stalks.

□
Prop. (5.6.2.4) [Faithfully Flat Descent for Flat Modules]. Let \( f : X \to Y \) be a morphism of schemes over \( S \) and \( G \in \mathcal{QCoh}(Y) \), then \( G \) is flat over \( S \) iff \( f^*G \) is flat over \( S \). In particular, \( Y \) is flat over \( S \) iff \( X \) is flat over \( S \).

**Proof:** This follows from (4.4.1.6).

Prop. (5.6.2.5). For a Qco sheaf \( F \) on a scheme \( X \), the following are equivalent, by (4.3.1.7).

1. \( F \) is finite projective.
2. \( F \) is f.p. and flat.
3. \( F \) is f.p. and all its localizations at (maximal)primes are free.
4. \( F \) is finite locally free.
5. \( F \) is finite and locally free.
6. \( F \) is finite and all its localizations at primes are free and the function \( p \to \dim_{k(p)} F \otimes_R k(p) \) is a locally constant function on \( \text{Spec} \, R \).

Cor. (5.6.2.6). Let \( f : X \to Y \) be a finite morphism of locally Noetherian schemes and \( Y \) is reduced, the following are equivalent:

- \( f \) is flat.
- \( f_*\mathcal{O}_X \) is locally free.
- \( \dim_{k(x)}(\pi_*\mathcal{O}_X)_x \otimes k(x) \) is a locally constant function for \( x \in Y \).

**Proof:** 3 follows from (5.5.1.43).

Prop. (5.6.2.7) [Going-Down]. Generalizations lift along a flat morphism.

**Proof:** We can find an affine nbhd, then choose a nbhd of the inverse image, then a generalization in an affine open is a true generalization, so it reduce to the affine case. The rest follows from going-down (4.4.1.19).

Cor. (5.6.2.8) [Flat Map and Irreducible Components]. A flat morphism maps generic points to generic points.

Prop. (5.6.2.9) [Flat Map and Associated Points]. Let \( f : X \to S \) be a morphism of schemes that \( S \) is locally Noetherian, and \( F \) a Qco sheaf on \( X \). If \( F \) is flat over \( S \), then \( f \) maps \( \text{WeakAss}(F) \) to \( \text{Ass}(S) \). In particular, if \( X \) is flat over \( S \), then \( f \) maps \( \text{WeakAss}(X) \) to \( \text{Ass}(S) \).

**Proof:** Let \( x \in X, f(x) = s \) that \( s \in \text{Ass}(S) \), then we get a map \( (\mathcal{O}_{S,s}, \mathfrak{m}_s) \to (\mathcal{O}_{X,x}, \mathfrak{m}_x) \). If \( \mathfrak{m}_s \) is not associated point, then by prime avoidance (4.1.1.4), there is some \( m \in \mathfrak{m}_s \) that is not a non-zero divisor, by (4.2.5.17), so \( f^2(m) \) is also a non-zero divisor on \( F_x \), so \( \mathfrak{m}_x \) is not a weakly associated point of \( F \).

Prop. (5.6.2.10) [Flat Map is Open]. A flat morphism locally of f.p. is (universally)open, hence it is qc.

And a qc f.f. morphism of schemes is a quotient map.

**Proof:** It suffices to consider the affine case. Then the assertion follows from (4.4.1.32).

For the second, by (5.6.2.7), a subset whose inverse image is closed is stable under specialization (surjectiveness used), then it is closed by (5.4.4.9).
Prop.(5.6.2.11) [Cartier Divisor and Flat Base Change].
- The flat base change of Cartier divisor is also a Cartier divisor.
- The flat base change of a regular embedding is also a regular embedding.
- The flat base change commutes with blow up, by universal property.

Prop.(5.6.2.12) [Flat Pullback of Closed Subschemes]. Let \( Z \subset X \) be a closed subscheme corresponding to a Qco sheaf of ideals \( I \), and \( f : X' \to X \) be a flat morphism, then the pullback \( Z' \subset X' \) is a closed subscheme that corresponds to the ideal sheaf \( f^*I \).

Proof: This is because \( f^* \) is exact.

Prop.(5.6.2.13) [Pullback of Flat Closed Subschemes]. Let \( X \) be a scheme over \( S \), \( S' \to S \) be a morphism of schemes, and \( Z \subset X \) be a closed subscheme corresponding to a Qco sheaf of ideals \( I \) flat over \( S \), then the pullback \( Z' \subset X' \) is a closed subscheme that corresponds to the ideal sheaf \( f^*I \).

Prop.(5.6.2.14) [Flat Loci is Open]. For a morphism \( f : X \to S \) locally of f.p., and \( F \in \mathcal{Q}\text{coh}^{bf}(X) \), then the set of points of \( X \) that \( F \) is flat over \( S \) is open. In particular, if \( f \) is a closed map, then the set of points of \( Y \) that \( F \) is flat is open.

Proof: Cf.[Sta]00RC. The last assertion follows from the first one.

Prop.(5.6.2.15) [Generic Flatness]. For a morphism \( f : X \to S \) of f.t., if \( S \) is reduced and \( F \) is a Qco f.t. \( \mathcal{O}_X \)-module, then there exists an open dense subset \( U \) of \( S \) that \( X_U \to U \) is flat, of f.p., and \( F|_{X_U} \) is flat over \( U \) and of f.p. over \( \mathcal{O}_U \).

Proof: As flat and f.p. is local on the base, it suffices to show for \( S \) affine. Then this almost immediately reduces to the affine case??y choosing an affine cover of \( X \), except that we need \( X_U \) to be qs over \( U \). To achieve this, it suffices to do it second time and let \( X = \bigcup_{i \leq n} \text{Spec } B_i = \bigcup X_i, \) and \( X_i \cap X_j = D(I_{ij}), M_{ij} = B_i/I_{ij}, \) then choose \( f \) large enough that over \( S_f, \) all \( M_{ij} \) are f.p. over \( B_i, \) then by (4.2.5.9), \( X_{i,f} \cap X_{j,f} \) is qc, thus \( X_f \) is f.p. over \( S_f \).

Prop.(5.6.2.16) [Fibral Criterion of flatness]. Let \( S \in \text{Sch} \) and \( f : X \to Y \in \text{Sch}/S, F \in \mathcal{Q}\text{coh}^{bf}(X) \). Let \( x \in X, y = f(x) \) and \( x \) maps to \( s \in S \). Suppose \( X,Y \) are both locally Noetherian or \( X \) is locally of f.p. over \( S \) and \( Y \) is locally of f.t. over \( S \), then the following are equivalent:
- \( F \) is flat over \( S \) at \( x \) and \( F_s \) is flat over \( Y_s \) at \( x \).
- \( Y \) is flat over \( S \) at \( y \) and \( F \) is flat over \( Y \) at \( x \).

Proof: Cf.[Sta]039B, 039C.

Prop.(5.6.2.17) [Hilbert Polynomial Constant in Flat Family]. For \( X/T \) projective, where \( T \) is an integral Noetherian scheme and \( X \subset \mathbb{P}_T^n \). Then for each point \( T, X_t \) is a closed subscheme of \( \mathbb{P}_k(t)^n \), so we can consider its Hilbert Polynomial \( P_t \). Then \( X/T \) is flat iff \( P_t \) is independent of \( T \).

Needs huge improvement.

Proof: \( P_t(m) = \dim_k H^0(X_t, \mathcal{O}_{X_t}(m)) \) for \( m \) large by (5.7.3.10). And we may let \( X = \mathbb{P}_T^n \) and prove for any coherent sheaf \( F \). Moreover, we may let \( T \) be a affine local Noetherian, because flatness is local and we only need to compare Hilbert polynomial with the generic point. Now we prove a stronger assertion: The following are equivalent:
• \( \mathcal{F} \) is flat over \( T \).
• \( H^0(X, \mathcal{F}(m)) \) is a free \( A \)-module of finite rank, for \( m \) large.
• The Hilbert polynomial \( P_t \) of \( \mathcal{F}_t \) on \( X_t = \mathbb{P}^n_{k(t)} \) is independent of \( t \).

1 \( \rightarrow \) 2: Use the canonical cover and Čech cohomology, then we notice when \( m \) is large, \( H^0(X, \mathcal{F}(m)) \) is a kernel of the Čech resolution, so it is flat. And it is also finite by (5.7.4.12). Then it is free because it is flat by (4.4.1.10).

2 \( \rightarrow \) 1: Let \( M = \oplus_{m \geq m_0} H^0(X, \mathcal{F}(m)) \), then \( \widetilde{M} = \mathcal{F}(5.5.3.6) \), notice that the truncation doesn’t affect.

2 \( \rightarrow \) 3: It suffice to prove that for any \( t \in T \), when \( m \) is large,
\[
H^0(X_t, \mathcal{F}_t(m)) \cong H^0(X, \mathcal{F}(m)) \otimes_A k(t).
\]

For this, we may use (5.7.5.1) to pass to the localization and assume \( t \) is the closed pt of \( T \). Then \( A \rightarrow k(t) \) is surjective and we may let \( A^q \rightarrow A \rightarrow k \rightarrow 0 \), then by (5.7.4.8), we have \( H^0(X_t, \mathcal{F}_t(m)) \) is the cokernel of \( H^0(X, \mathcal{F}(m))^q \rightarrow H^0(X, \mathcal{F}(m)) \), but this cokernel is \( H^0(X, \mathcal{F}(m)) \otimes_k k \) because tensoring is right-adjoint, so we are done.

3 \( \rightarrow \) 2: We have the rank of \( H^0(X, \mathcal{F}(m)) \) at the generic and closed point of \( T \) are the same (still use \( H^0(X_t, \mathcal{F}_t(m)) \cong H^0(X, \mathcal{F}(m)) \otimes_A k(t) \)). Now (4.4.8.1) gives \( H^0(X, \mathcal{F}(m)) \) is free. It is f.g. automatically.

\[\square\]

Cor. (5.6.2.18). For a flat morphism to a connected scheme \( T \), the dimension, degree, and arithmetic genus of the fibers are independent of \( t \).

\[\text{Proof:}\] By (5.7.3.6) and (5.7.3.12). \[\square\]

Def. (5.6.2.19). For a surjective map of varieties \( f : X \rightarrow T \) over an alg.closed field \( k \), its fiberes over closed points with induced reduced structure \( X_t \) is called a \textbf{algebraic family of varieties parametrized by} \( T \) if

1. \( f^{-1}(t) \) is irreducible of dimension \( \dim X - \dim T \) for every closed point \( t \).

2. If \( \zeta \) is the generic point of \( f^{-1}(t) \), then \( F^q m_t \) generates the maximal ideal \( m_\zeta \subset \mathcal{O}_{\zeta, X} \).

Prop. (5.6.2.20). If \( X_t \) is an algebraic family of normal varieties over an alg.closed field \( k \) parametrized by a nonsingular curve \( T \), then it is a flat family of schemes.

\[\text{Proof:}\] By (5.11.1.20), \( X \rightarrow T \) is flat. So what we need to do is to prove \( X_t \) is reduced so \( X_t = X_{(t)} \). Let \( A = \mathcal{O}_{x, X} \), let \( u_t \) be a uniformizer of \( \mathcal{O}_{t, T} \), then \( A/tA \) is the local ring of \( x \) on \( X_t \). By hypothesis \( X_t \) is irreducible so \( tA \) has a unique minimal prime \( p \) in \( A \), and \( t \) generate the maximal ideal of \( A_p \) by hypothesis. The local ring of \( X_{(t)} \) is \( A/p \), so \( A/p \) is normal by hypothesis. Then the result follows from (4.3.5.13). \[\square\]

Cor. (5.6.2.21) [Igusa]. Let \( X_{(t)} \) be an algebraic family of normal varieties in \( \mathbb{P}^n_k \) for \( k \) alg.closed parametrized a variety \( T \), then the Hilbert polynomials of \( X_{(t)} \) are independent of \( t \).

\[\text{Proof:}\] Why is \( X/T \) projective? Cf. [Hartshorne P265]. \[\square\]
Degenerating Techniques

Finite Locally Free Morphism

Def.(5.6.2.22)[Finite Locally Free]. A morphism $f : X \to Y$ is called finite locally free of rank $d$ if it is affine, and $f_*\mathcal{O}_X$ is a finite locally free $\mathcal{O}_Y$-module of rank $d$.

Cor.(5.6.2.23). If $f$ is finite locally free of rank $n$, then for any locally free sheaf $E$ of rank $k$ on $X$, $f_*E$ is locally free of rank $nk$.

Prop.(5.6.2.24). $f$ is finite locally free iff it is finite, flat and of f.p.. In particular, when $Y$ is locally Noetherian, this is equivalent to $f$ is finite flat.

Proof: Both notions are local on the target, so we reduce to the ring case, which is (4.3.1.7). □

Cor.(5.6.2.25). Finite locally freeness is stable under composition and base change, and it is local on the target.

Prop.(5.6.2.26)[Trace and Norm]. Let $f : Y \to X$ be a finite locally free map of constant rank, then there are trace and norm maps $\text{tr} : f_*\mathcal{O}_Y \to \mathcal{O}_X, \text{Nm} : f_*\mathcal{O}_Y \to \mathcal{O}_X$ compatible with arbitrary base change.

Proof: The proof is the same as that of (4.3.1.11). □

Prop.(5.6.2.27). Let $f : Y \to X$ be a finite locally free map of constant rank, and $b \in \Gamma(Y, \mathcal{O}_Y)$, then $f(Z(b)) = Z(\text{Nm}(b))$.

Proof: We can assume $X$ is affine, then we need to show that for a prime $p$ with inverse images $p_i$, $b \in \cup p_i$ iff $\text{Nm}(b) \in p$. We localize at $p$, then $\text{Nm}(b) \in p$ iff $\text{Nm}(b)$ is non-invertible iff multiplication by $b$ is non-invertible iff $b$ is non-invertible iff $b \notin \cup p_i$, because $p_i$ are all the maximal ideals of $B_p$. □

3 Dimensions

Main references are [Mat80] and [Vak17]Chap11.

Prop.(5.6.3.1)[Locally Algebraic Scheme is Catenary]. If $X$ is a locally algebraic scheme over a field $k$ purely of dimension $n$, and $Y$ an irreducible subscheme of $X$, then $\dim Y + \text{codim}(Y, X) = \dim X$.

Proof: Choose an affine open of the generic point of $Y$, then we are reduced to the affine case (4.2.4.3)(4.2.4.7). □

Prop.(5.6.3.2). For any scheme, $\dim \mathcal{O}_x = \text{codim}(\overline{\{x\}}, X)$.

Prop.(5.6.3.3). For an integral scheme algebraic over a field $k$,

$$\dim X = \dim \mathcal{O}_{p,X} = \dim U = \text{tr.deg } K(X)/k$$

for any closed point $p$ and any open subscheme $U$.

Proof: Use closed point are dense (5.4.1.26) and $k$ is universal catenary to prove it is true for some $U$ and all the closed point in it, so other $U$’s because $X$ is irreducible. The last equation follows from (4.2.4.23). □
Prop. (5.6.3.4) [Finite Surjection Preserves Dimension]. Let $X \to Y$ be a surjective finite morphism of algebraic integral schemes over a field $k$, then $\dim X = \dim Y$.

Proof: The hypothesis implies that for any affine open $\text{Spec} \, A \subset Y$, the inverse image is $\text{Spec} \, B$ that $A \to B$ is an injective integral ring extension, so we can use (5.6.3.3) and (4.2.4.14). □

Prop. (5.6.3.5). Let $X$ be a locally Noetherian scheme, if $U \subset X$ is an open subscheme that $U \to X$ is affine, then every irreducible complements of $X - U$ has codimension ≤ 1. And if $U$ is dense, then equality must hold.

Proof: Cf. [Sta]0BCU. □

Prop. (5.6.3.6) [Local Dimensions]. Let $X$ be a locally algebraic scheme over a field $k$ and $x \in X$, then the local dimension $\dim_x(X)$ equals the maximal dimension of irreducible components of $X$ passing through $x$, by (4.2.4.27).

Prop. (5.6.3.7). If $f : X \to Y \in \text{Sch}^{\text{loc}, \text{ft}} / S$, $x \in X$ and $s = f(x)$, then

$$\dim_x(X_s) = \dim O_{X,s,x} + \text{tr.deg}_{k(s)} k(x).$$

Proof: This reduces to the case $Y = \text{Spec} \, k(s)$, and it follows from (4.2.4.28). □

Prop. (5.6.3.8) [Semicontinuity of Dimension]. Let $f : X \to S$ be a morphism of schemes locally of f.t., then the function $x \mapsto \dim_x(X_{f(x)})$ is upper-semicontinuous on $X$.

Moreover, if $f$ is of f.p., then the open subsets $\{x \mid \dim_x(X_{f(x)}) \leq n\}$ is retrocompact.

Proof: This follows directly from (4.2.4.32). □

Prop. (5.6.3.9) [Local Dimension and Base Change]. Let

$$
\begin{array}{ccc}
X' & \xrightarrow{g'} & X \\
\downarrow f' & & \downarrow f \\
S' & \xrightarrow{g} & S
\end{array}
$$

be a fiber product diagram of schemes, and $f$ is locally of f.t.. Suppose $x' \in X'$, $x = g'(x')$, $s = g(s')$. Then

- $\dim_x(X_s) = \dim_{x'}(X_{s'})$.
- $\dim O_{F,x'} = \dim O_{X',x'} - \dim O_{X,x} = \text{tr.deg}_{k(s)}(k(x)) - \text{tr.deg}_{k(s')}(k(x'))$.

where $F$ is the fiber of the morphism $X'_s \to X_s$ over $x$. In particular, $\dim O_{X',x'} \geq \dim O_{X,x}$ and $\text{tr.deg}_{k(s})(k(x')) \leq \text{tr.deg}_{k(s)}(k(x))$.

- Given $s', s$, $x$ that $f(x) = g(s')$, there exists an $x' \in X'$ that $\dim O_{X',x'} = \dim O_{X,x}$ and $\text{tr.deg}_{k(s')}(k(x')) = \text{tr.deg}_{k(s)}(k(x))$.

Proof: It can be reduced to the case that $S = \text{Spec} \, k(s)$, $S' = \text{Spec} \, k(s')$ and $X, X'$ affine. Then 1 follows from (4.2.4.31), and 2, 3 follows from (4.2.4.26). □

Cor. (5.6.3.10) [Dimension and Field Extension]. Let $K/k$ be a field extension, $X$ a locally algebraic scheme over $k$ purely of dimension $n$, then $X_K$ is a scheme purely of dimension $n$. 


Remark (5.6.3.11). This proposition shows in particular local dimension behaves better than the dimension of the stalk.

Def. (5.6.3.12) [Relative Dimensions]. A morphism of schemes which locally of f.t. is called of relative dimension \( n \) iff all fibers \( X_s \) are equidimensional of dimension \( n \).

Prop. (5.6.3.13). Being a morphism of relative dimension \( n \) is stable under field extension, by (5.6.3.10).

Dimension and Flatness

Prop. (5.6.3.14) [Faithfully Flat Morphism]. If \( f : Y \to X \) is a faithfully flat morphism, then \( \dim Y \geq \dim X \).

Proof: This is easy from (5.6.2.7).

Prop. (5.6.3.15) [Integral Flat Morphisms]. If \( f : X' \to X \) is an integral flat morphism of schemes, and \( X \) is pure of dimension \( n \), then so does \( X' \). The converse holds if \( f \) is faithfully flat.

Proof: By (5.6.2.8) and (5.4.4.35), \( f \) maps an irreducible component of \( X' \) onto an irreducible component of \( X \). Then by (3.8.3.26), the proposition reduces to the affine case (4.2.4.15). If \( f \) is faithfully flat, then every irreducible component of \( X \) is in the image.

Cor. (5.6.3.16) [Dimension and Field Extension]. If \( K/k \) is an algebraic extension, \( X \) a scheme over \( k \) purely of dimension \( n \), then \( X_K \) is a scheme purely of dimension \( n \). Compare with (5.6.3.10).

Prop. (5.6.3.17) [Dimension Extension and Flatness]. Let \( f : X \to Y, g : Y \to S \) be locally of f.t., \( x \in X, y = f(x), s = g(y) \), then

\[
\dim_x(X_s) \leq \dim_x(X_y) + \dim_y(Y_s).
\]

Moreover, equality holds if \( \mathcal{O}_{X,x}/\mathcal{O}_{Y,y} \) is flat.

In particular, if \( S = \text{Spec} k \) and \( X, Y \) are irreducible and \( X \) is flat over \( Y \), then \( \dim X_y = \dim X - \dim Y \) for any \( y \in Y \).

Proof: By (5.6.3.7) and the fact transcendental degree is additive, this reduces to

\[
\dim \mathcal{O}_{X,x} \leq \dim \mathcal{O}_{X,y} + \dim \mathcal{O}_{Y,y}.
\]

We can assume \( X, Y \) is affine and \( S = \text{Spec} k(s) \), so the rest follows from (4.2.4.13).

Cor. (5.6.3.18). If \( f : X \to Y, g : Y \to Z \) are of relative dimension \( m \) and \( n \) (5.6.3.12), and \( f \) is flat, then \( g \circ f \) is of relative dimension \( m + n \).

Cor. (5.6.3.19) [Generic Dimension Equation]. If \( f : X \to Y \) is a dominant morphism of irreducible algebraic schemes over \( K \) that \( X \) is reduced, then there is a dense open subset \( U \) of \( Y \) that for any \( y \in Y \),

\[
\dim(Y_y) = \dim X - \dim Y.
\]

Proof: This is a combination of the above proposition and generic flatness (5.6.2.15).
Prop. (5.6.3.20) [Relative Dimension and Base Change]. By (5.6.3.9), the base change of a morphism of locally algebraic schemes over a field \( k \) of relative dimension \( n \) is still of relative dimension \( n \). In particular, for a variety over \( K \) a field, the dimension is invariant under base change of fields.

Cor. (5.6.3.21). Let \( Y, Z \) be irreducible locally algebraic schemes over \( k \), then \( Y \times_k Z \) is pure of dimensional \( \dim(Y) + \dim(Z) \).

Proof: Combine (5.6.3.20) and (5.6.3.17).

Prop. (5.6.3.22). For a morphism \( f : X \to Y \) between locally Noetherian schemes which is flat and locally of f.t and of relative dimension \( n \), then if \( y = f(x) \), we have \( \dim_x(X_y) = \dim_x(X) - \dim_y(Y) \).

Proof: Shrinking the nbhd, we may assume \( \dim_x(X) = \dim X \) and \( \dim_y(Y) = \dim Y \) and \( X, Y \) are affine. Now \( f \) is locally of f.p. and flat, so it is open (5.6.2.10). So we may assume \( f \) is surjective. Then \( \dim \mathcal{O}_{X,a} = \dim \mathcal{O}_{Y,b} + \dim \mathcal{O}_{X,b,a} = \mathcal{O}_{Y,b} + n \) by (4.2.4.13), then taking supremum??, the result follows.

Cor. (5.6.3.23). For a morphism of schemes that is flat and of f.t., if \( Y \) is irreducible, then \( X \) is equidimensional of dimension \( \dim Y + n \) iff \( X_y \) is equidimensional of dimension \( n \) for every \( y \in Y \).

Proof: The proof highly relies on (5.6.3.3).

If \( X \) is equidimensional of dimension \( \dim Y + n \), for \( Z \subset X_y \) an irreducible component, choose a closed pt \( x \) of \( Z \) not contained in any other irreducible component, then
\[
\dim_x Z = \dim_x X - \dim_y Y = \dim X - \dim \{x\} - \dim Y + \dim \{y\}.
\]
The two closures are of the same dimension because by (4.2.6.10), their quotient field extension is finite, and use (4.4.2.14).

Conversely, for an irreducible component of \( X \), choose a closed pt \( x \) of \( Z \) not contained in any other irreducible component, then the image is also closed, by (5.4.1.27), so the result is immediate.

Prop. (5.6.3.24). If \( f : X \to Y \) is a proper flat morphism of schemes of f.p., then the dimension of fibers of \( f \) is a locally constant function.

Proof: Cf. [Sta]04DJ.

4 Smoothness

Def. (5.6.4.1) [Smooth Morphisms]. A \textbf{smooth morphism} \( f : X \to Y \) between schemes is a morphism that there is an open affine cover \( \{U_i\} \) of \( S \) and an open affine cover \( V_{ij} \) of \( f^{-1}(\{U_i\}) \) that the ring map is smooth (4.4.5.12). In particular, it is locally of f.p.. A \textbf{standard smooth morphism} is the Spec map of a standard smooth ring map.

Smoothness is local on the source and target (4.4.5.13). Smoothness is stable under base change and composition (4.4.5.13).

Prop. (5.6.4.2). For a smooth morphism \( X \to S \), the morphism of differential \( \Omega_{X/S} \) is locally free and \( \dim_x \Omega_{X/S} = \dim_x(X_f(x)) \) (local dimension (3.8.3.25)).

Proof: We can assume that \( X \to S \) is standard smooth, so by the proof in (4.4.5.12), \( \Omega_{X/S} \) is free of dimension \( n - c \), and also standard smooth is relative global complete intersection (4.4.5.11), so \( U_f(x) \) is equidimensional of dimension \( n - c \), thus the result.
Cor. (5.6.4.3) [Differential Criterion of Smoothness]. If $X \to S$ is a flat of relative dimension $n$, then $X$ is smooth over $S$ iff it is locally of f.p. and $\Omega_{X/S}$ is locally free of dimension $n$, by (4.4.5.23).

Prop. (5.6.4.4) [Smooth Morphism is Open]. Smooth morphism is syntomic hence flat. Smooth morphism is locally of f.p. Hence smooth morphism is universally open (5.6.2.10).

Smooth morphism is locally standard smooth (4.4.5.12).

Prop. (5.6.4.5) [Fiberwise and Stalkwise]. For a morphism $X \to S$ locally of f.p., the following are equivalent:

- It is smooth at a point $x \in X$ over $s \in S$.
- $O_{X,x}/O_{X,f(x)}$ is flat and $X_{f(x)}/k(f(x))$ is smooth at $x$, by (4.4.5.20).
- $O_{X,x}/O_{S,f(x)}$ is flat and $\Omega_{X/S,x}$ can be generated by $\dim_x(X_{f(x)})$ elements, by (5.6.4.2) and (4.4.5.23).
- $O_{X,x}/O_{S,f(x)}$ is flat and $\Omega_{X/S,x}$ can be generated by $\dim_x(X_{f(x)})$ elements, by Nakayama, because $\Omega_{X/S,x}$ is of f.p. by (4.4.3.9).

In particular, a smooth morphism can be seen as a family of smooth schemes.

Proof:

Cor. (5.6.4.6) [Smoothness over DVR]. Let $R$ be a DVR with fraction field $K$ and residue field $k$, then an integral $R$-scheme $X$ of f.t. is smooth over $R$ iff $X_K \neq \emptyset$ and both $X_K/K$ and $X_k/k$ are smooth.

Proof: Notice that it is flat iff $X_K \neq \emptyset$.

Prop. (5.6.4.7). If $X \to Y$ is a smooth map of schemes over $S$, then by (5.5.5.5)(4.4.5.5), there is an exact sequence of sheaves:

$$0 \to f^*\Omega_{Y/S} \xrightarrow{df^*} \Omega_{X/S} \to \Omega_{X/Y} \to 0$$

Prop. (5.6.4.8). If $Z \to X \to S$, $Z/S$ is smooth and $Z \to X$ is an immersion, then there is an exact sequence of sheaves (5.5.5.13)(4.4.5.6):

$$0 \to C_{Z/X} \to i^*\Omega_{X/S} \to \Omega_{Z/S} \to 0$$

Prop. (5.6.4.9). If $X \to Y \to S$, and $X \to Y$ are faithfully flat and locally of f.p., $X/S$ is smooth, then $Y/S$ is smooth.

Proof: Cf. [Sta] 05B5.

Prop. (5.6.4.10). If $f : X \to S$ is faithfully flat and locally of f.p., then the set of points of $S$ s.t. $f$ is smooth is table under base change.

Proof:

Prop. (5.6.4.11). By (5.6.4.5)(5.6.4.2), A morphism is smooth of relative dimension $n$ is equivalent to fppf+fibers equidimensional of dimension $n$ and $\Omega_{X/S}$ is locally free of dimension $n$.

Prop. (5.6.4.12) [Jacobian Criterion for Projective Schemes]. Let $X$ be a closed subscheme of $\mathbb{P}_R^n$ defined by $r$ polynomials $F_1(X_0, \ldots, X_n), \ldots, F_r(X_1, \ldots, X_n)$, then for $x \in X$, $X$ is smooth at $x$ iff the Jacobian has rank $\geq n - \dim_x X$ at $x$ iff the Jacobian has rank $= n - \dim_x X$ at $x$. 
Proof: Assume that $x$ is in the standard open $X_0 \neq 0$, then we can use Euler’s identity $\sum X_i \partial F_i = \dim(F) F$ to eliminate the first row, then divide by $X_0^{\dim F}$ to get the Jacobian on the affine open $\text{Spec} R[x_0, \ldots, x_n]$, so we finish by $(4.4.5.24)$. □

Prop.(5.6.4.13) [Generic Smoothness on the Source]. Let $\pi : X \to Y$ be a dominant map of integral schemes of f.t. that $K(Y) \to K(X)$ is separable, then there is a non-empty open subscheme $U \subset X$ that $\pi|_U$ is smooth of relative dimension $\dim X - \dim Y$.

Proof: This reduces to the affine case, and follows from $(4.4.5.29)$ and $(5.6.3.17)$. □

Prop.(5.6.4.14) [Generic Smoothness on the Target]. Let $\pi : X \to Y$ be a morphism of $k$-varieties where $\text{char } k = 0$, and $X$ is smooth over $k$, then there is a dense open subset $U \subset Y$ that $\pi^{-1}(U) \to U$ is smooth.


Smooth over Fields

Prop.(5.6.4.15) [Differential Criterion of Smoothness]. Let $X$ be a scheme algebraic over a field $k$.

- If $X$ is equidimensional of dimension $n$, then $X$ is smooth over $k$ iff $\Omega_{X/k}$ is locally free of dimension $n$.
- If $\Omega_{X/k}$ is locally free, and $k$ is of char 0 or $k$ is perfect and $X$ is reduced, then $X$ is smooth over $k$.

Proof: 1: This follows from $(5.6.4.3)$.

2: If $k$ is of characteristic 0, then this follows from $(4.4.5.28)$.

perfect case: [Sta]04QP. ? □

Prop.(5.6.4.16) [Smooth over Field and Geo.Regular]. For a scheme locally algebraic over a field $k$, $X$ is geometrically regular iff it is smooth over $k$. In particular, if $k$ is perfect, then smoothness is equivalent to regularity, by $(5.4.3.18)$.

Proof: The question is local around $x$, so may assume $X$ is affine. Then this follows from $(4.4.5.27)$. □

Cor.(5.6.4.17) [Hartshorne Definition]. By $(5.6.4.5)$ and $(5.6.4.16)$, a morphism between schemes algebraic over a field $k$ is smooth of relative dimension $n$ iff $f$ is flat and every fiber of $f$ is geometrically regular of dimension $n$.

Cor.(5.6.4.18). A smooth scheme over a field $k$ is regular hence normal.

Prop.(5.6.4.19) [Smoothness and Separable Closed Points]. Let $X$ be smooth over a field $k$, then the set of closed points of $X$ with finite separable residue field $k(x)/k$ is dense in $X$.

Proof: It suffices to show there exists one such points. By $(5.6.6.7)$, we can assume $X \xrightarrow{\pi} \mathbb{A}_k^d \to k$, where $\pi$ is étale. Thus $X$ is open in $\mathbb{A}_k^d$ by $(5.6.6.3)$. Then we can choose a closed point of $\pi(X)$ s.t. the residue field is finite separable, as $k^{\text{sep}}$ is infinite. Then choose an inverse image, then the residue if finite étaleover $k$, by $(5.6.6.8)$. This point is clearly closed. □
Prop. (5.6.4.20) [Smoothness at Rational Points]. Let $X$ be a locally algebraic scheme over a field $k$. Let $x \in X$ that $k(x)/k$ is finite separable, then $X$ is smooth at $x$ iff it is $x$ is a regular point, by (4.4.5.26).

Prop. (5.6.4.21) [Geo. Reduced Scheme Generic Smooth]. Let $X$ be a locally algebraic scheme over a field $k$ that is geometrically reduced, then it contains an open dense subset that is smooth over $k$.

Proof: The problem is local, so we may assume $X$ is affine, consider its irreducible components, all their intersections can be removed, because they are nowhere dense, so we may assume $X$ is irreducible. So $X$ is integral, let $\eta$ be the generic pt, then $k(\eta)/k$ is separable, by (5.4.3.2). Then choose an affine subscheme $\text{Spec} A \subset X$, then $A$ is smooth at (0) over $k$, by (4.4.5.29), then by definition, it is smooth on some dense open subscheme of $X$. \qed

Tangent Spaces

Def. (5.6.4.22) [Relative Tangent Spaces]. Let $X$ be a scheme over $S$ and $x \in X$, define $T^*_x/S_x = \Omega_{X/S, x} \otimes_{O_{X, x}} k(x)$, and $T_{x/S} = \text{Hom}_{k(x)}(T^*_x/S_x, k(x)) = \text{Hom}_{O_{X, x}}(\Omega_{X/S, x}, k(x))$, called the relative tangent space of $X$ over $S$ at $x$.

When $x \in X$ mapping to $s \in S$, $T_{x/S} = \text{Hom}_{k(x)}(m_x/m_x^2, k(x))$, where $m_x$ is the maximal ideal of the stalk of $x \in X_s$.

Then it can be verified that for a $k$-scheme and a rational point $x \in X$, $T_{x/S}$ is in bijection with $\text{Mor}_k(\text{Spec} k[\varepsilon], X)$ that maps the closed point to $x$.

Prop. (5.6.4.23) [Tangent Map]. Let $f : X \to Y$ be a morphism of schemes over $S$, $x \in X$, $f(x) = y$. Assume $k(x) = k(y)$, then $f$ defines a natural linear map

$$df : T_{X/S_x} \to T_{Y/S_y} : \text{Hom}_{O_{X, x}}((\Omega_{X/S})_x, k(x)) \to \text{Hom}_{O_{Y, y}}((f^*\Omega_{Y/S})_y, k(x))(5.5.5.5) = \text{Hom}_{O_{X, x}}(\Omega_{Y/S_y} \otimes_{O_{Y, y}} O_{X, x}, k(y)) = \text{Hom}_{O_{Y, y}}(\Omega_{Y/S_y}, k(y))$$

Cor. (5.6.4.24). Via similar argument, if $k(x) = k(s) = k(y)$, there is an isomorphism

$$T_{X/S_x} \oplus T_{Y/S_y} \cong T_{X \times_S Y(x, y)}.$$

Prop. (5.6.4.25). Let $X$ be a scheme over a field $k$ and $x \in X$ with residue field $k(x)$, then the tangent space is canonical isomorphic to $\text{Mor}(k(x)[\varepsilon], X)$ that maps the closed point to $x$. And the vector bundle structure is given by the cogroup structure on $\text{Spec} k[\varepsilon] : \mu : k[\varepsilon] \otimes k[\varepsilon] \to k[\varepsilon]$.

Prop. (5.6.4.26) [Krull’s Principal Tangent Theorem]. Let $Z \subset X$ be a closed subscheme with ideal of definition $I$, $x \in Z$, then $T_{Z, x}$ is the subspace of $T_{X, x}$ cut out by $(I \mod m_x^2)$. In particular, $T_{Y \cap Z, p} = T_{Y, p} \cap T_{Z, p} \subset T_{X, p}$.

Prop. (5.6.4.27) [Tangent Criterion of Smoothness]. By (5.6.4.16)(5.6.4.20) and the definition of regular local ring, if $X$ is a locally algebraic scheme over a field $k$, then $X$ is smooth at a point $x$ with residue field $k(x)/k$ separable iff $\text{dim}_k(T_{X, x}) \leq (\leq)$ the dimension of $O_{X, x}$.
Bertini’s Theorem

Prop.(5.6.4.28)[Bertini]. Let $k$ be a field. For any quasi-projective scheme $X \subset \mathbb{P}^n_k$ smooth away from f.m. points, there is an open dense subset $U$ of the dual projective space $\mathbb{P}^n_k^\vee$ s.t. for any closed point $[H] \subset U$, $H$ doesn’t contain any component of $X$, and the scheme $H \cap X$ is smooth over $k$.

Moreover, if $X$ is a variety and $\dim X \geq 2$, the smooth cut is even a smooth variety by (5.8.6.25) and (5.4.2.9).

Proof: Let $\mathbb{P}^n = \text{Proj } k[x_0, \ldots, x_n], (\mathbb{P}^n)^\vee = \text{Proj } k[a_0, \ldots, a_n]$. Let $\overline{X}$ be cut out by equations $f_1, \ldots, f_r$, we define a projective scheme $Z \subset \mathbb{P}^n \times (\mathbb{P}^n)^\vee$ be cut by the equations

- $f_r$,
- $f_{r+1} = \sum a_i x_i$,
- determinants of $(r + 1) \times (r + 1)$-minors of $(\frac{\partial f_i}{\partial x_j})(r + 1) \times n$.

Now for any $(x, [H]) \in Z$, $x \in X, x \in H$ that $[H]$ is closed in $(\mathbb{P}^n)^\vee$, the last equation means $X \cap H$ is non-smooth at $p$ or contains the irreducible component passing $p$, by Jacobian criterion (5.6.4.12). Now consider the projection $Z \rightarrow X$, for each closed point $p \in X$ that $\dim_p X = d$, the codimension of the fiber of $Z$ over $x$ is of dimension $r - 1 = n - \dim_x X - 1$ (To see this, one way is use regularity and tangent space, another way is to use the fact $(x_i)$ is orthogonal to $(\frac{\partial f_i}{\partial x_j})$ for all $i$ by Euler identity, so the $r+1$ restrictions of $(a_i)$ are linearly independent), then by (5.6.3.17), $\dim Z = \dim \pi_1^{-1}(Z) \leq n - 1$.

Thus the image of $Z$ in $\mathbb{P}^n_k^\vee$ is also a closed subscheme of dimension $\leq n - 1$.

If $X$ has f.m. singular points, we also need to cut out the surfaces $N_{k(x)/k}(\sum x_i^k a_i)$, where $(x'_i)$ are the f.m. closed singular points of $x$. They are also of dimension $n - 1$. $\square$

Cor.(5.6.4.29)[Bertini’s Theorem for Surfaces]. Similarly, for any $d \geq 0$, a generic dimension $d$ surface intersect $X$ at a smooth subscheme, by using Veronese embedding.

Cor.(5.6.4.30). When $X \subset \mathbb{P}^n_k$ is a projective $k$-variety where $k$ has characteristic 0, the scheme $Z$ in $\mathbb{P}^n_k^\vee$ is called the dual variety of $X$. When $X$ is irreducible and smooth, it is of dimension $n - 1$.

Proof: $\square$

Prop.(5.6.4.31). The dual variety of the dual variety is $X$ itself.

Proof: Cf.[Joe Harris, Algebraic Geometry, 15.24]. $\square$

Prop.(5.6.4.32)[Kleinman-Bertini]. Let $X$ be a $k$-variety that is homogenous space for a $k$-variety $G$ over a field $k$, suppose $\alpha : Y \rightarrow X, \beta : Z \rightarrow X$ are morphisms of varieties, then

- There is a non-zero open subset $V \subset G$ that for any closed point $\sigma \in V$, $\dim \sigma(Y) \times_X Z = \dim Y + \dim Z - \dim X$.
- If $Y, Z$ are smooth over $k$ of characteristic 0, then there is a non-empty open subset $V \subset G$ that $(G \times_k Y) \times_X Z \rightarrow G$ is smooth. In particular, for any closed point $\sigma \in V$, $\sigma(Y) \times_X Z$ is smooth over $k(\sigma)$ of dimension $\dim Y + \dim Z - \dim X$.

Proof: Let $\Gamma = (G \times_k Y) \times_X Z$, then there is a map $\Gamma \rightarrow Y \times_k Z$. $Y \times_k Z$ has dimension $\dim Y + \dim Z$ by (5.6.3.21), and there is a base change diagram

\[
\begin{array}{ccc}
(G \times_k Y) \times_X Z & \longrightarrow & Y \times_k Z \\
\downarrow & & \downarrow \\
G \times_k X & \longrightarrow & X \times_k X
\end{array}
\]
and $G \times X \to X \times X$ is flat as it is equivariant under $G \times G$-action, by (5.6.2.15), thus $\Gamma \to Y \times_k Z$ is flat of relative dimension $\dim G - \dim X$, thus it has dimension $\dim Y + \dim Z + \dim G - \dim X$.

1: This follows from (5.6.3.19) applied to the map $G \times_k Y \times_k Z \to G$.

2: As $G \times X \to X \times X$ is flat, and its fiber are isomorphic to $G_x$, which is the fiber of the map $\alpha_x : G \to X$, and this map is smooth by (5.6.4.14), thus $G \times X \to X \times X$ is smooth, and then the assertion follows from (5.6.4.14).

\[ \square \]

Cor. (5.6.4.33). Let $Z$ be a smooth $k$-variety where $\text{char} k = 0$. Let $V$ be a f.d. basepoint-free line series on $Z$, then the section of a general element of $V$ is smooth.

Proof: Apply Kleinman-Bertini to $\varphi_V : Z \to \mathbb{P}V^\vee$, $Y = V(\sum a_i x_i) \in PV \times PV^\vee \to PV^\vee$, $X = PV^\vee$. \[ \square \]

5 Unramified

More advanced materials to learn at [Sta]Chap40.

Def. (5.6.5.1) [Unramified Morphism]. A morphism is called (G-)unramified iff there is an open affine cover $U_i$ and an open affine cover of $f^{-1}(U_i)$ that the induced ring map is (G-)unramified (4.4.6.4). Equivalently, $\Omega_{X/S} = 0$ and it is locally of f.t.(f.p.).

(G-)unramifiedness is local on the source and target (5.4.1.5) (5.4.1.6). (G-)unramifiedness is stable under base change and composition (4.4.6.4). Moreover, unramifiedness satisfies the base change trick.

Prop. (5.6.5.2). An unramified map is locally quasi-finite.

Proof: Cf. [Sta]02V5. \[ \square \]

Prop. (5.6.5.3) [Fiberwise]. A morphism is (G-)unramified iff it is locally of f.t.(f.p.) and all the fibers $X_s$ are disjoint unions of spectra of finite separable extensions of $k(p)$.

Proof: By (4.4.6.7), Notice $pS_q = qS_q$ is equivalent to every $q$ is minimal in $X_p$, which is equivalent to $X_p$ is discrete. \[ \square \]

Cor. (5.6.5.4) [Unramified over Fields]. A scheme over a field $k$ is unramified iff it is a disjoint union of spectra of finite separable extensions of $k$, because locally of f.p. is trivially satisfied.

Prop. (5.6.5.5) [Diagonal is Open]. A morphism $X \to S$ is (G-)unramified iff it is of f.t.(f.p.) and the diagonal is a clopen immersion of $X$, thus all of $X$.

Proof: If it is unramified, then the diagonal is an open immersion by (4.4.6.10). Conversely, $\Omega_{X/S}$ is just the conormal sheaf of the diagonal map, so it is zero. \[ \square \]

Cor. (5.6.5.6) [Sections of Unramified Morphism]. Any section of an unramified morphism is an open immersion. In particular, a section of a separable unramified morphism is a clopen immersion.

Proof: This follows from the proposition and the fact $S \to X$ is a base change of $\Delta_{X/S}$. \[ \square \]

Cor. (5.6.5.7). Let $X, Y$ be schemes over $S$, if $f, g$ are two maps from $X$ to $Y$, then if $Y/S$ is unramified and $f, g$ are equal on a pt $x$ of $X$ (both on image and residue field), then there is a nbhd of $x$ that $f, g$ are equal.
Proof: This follows as $\Delta_{Y/S}$ is open immersion, so the set that $f, g$ are equal is open in $X$. □

Prop. (5.6.5.8) [Fiberwise]. For a morphism $f : X \to S$ locally of f.t.(f.p.), let $x \in X, s = f(x)$, then the following are equivalent:

- It is $(G)$-unramified at $x$.
- The fiber $X_s$ is unramified over $k(s)$ at $x$, by (5.6.5.3).
- $\Omega_{X_s,x} = 0$.
- $\Omega_{X_s/x} \otimes_{O_{X,x}} k(x) = 0$ by (4.4.6.6).
- $m_x O_{X,x} = m_s$ and $k(x)/k(f(x))$ is separable.

Proof: $1 \to 2 \to 3 \to 4$ is clear. $4 \to 1$: Nakayama implies $\Omega_{X_s,x} = 0$, thus $\Omega_{X/S}$ vanishes on a nbhd of $x$ as it is Qco of f.t.

$4 \iff 5$ follows from (4.4.6.7). □

Cor. (5.6.5.9) [Generic Unramifiedness]. Let $f : X \to Y$ be a finite separable dominant morphism of integral schemes, then there exists an open dense nbhd $U$ of $Y$ s.t. $f : f^{-1}(U) \to U$ is unramified.

Prop. (5.6.5.10). If $X \to Y \to S$ is unramified, then $X/Y$ is also unramified. And if $X/S$ is $G$-unramified and $Y/S$ is of f.t., then $X/Y$ is $G$-unramified.

Proof: By (5.6.1.4) and (5.5.5.5). □

Prop. (5.6.5.11) [Unramified Points Base Change]. If $f$ is of f.t.(f.p.), then the set of points of $S$ that $f$ is unramified is stable under base change.

Proof: □

Prop. (5.6.5.12) [Tangent Criterion of unramifiedness]. Let $f : X \to Y$ be a morphism of schemes locally of f.t. over $S, x \in X, y = f(x)$, then the following are equivalent:

- $df : T_{X/S,x} \to T_{Y/S,y}$ is an injection (5.6.4.23).
- $f$ is unramified at $x$.

Proof: It follows from (5.6.4.23) that $df$ is an isomorphism iff $(f^*\Omega_{Y/S})_x \otimes_{O_{X,x}} k(x) \to \Omega_{X/S,x} \otimes_{O_{X,x}} k(x)$ is surjective, which by Jacobi-Zariski (5.5.5.5) is equivalent to $\Omega_{X/Y,x} \otimes_{O_{X,x}} k(x) = 0$, and this is equivalent to $f$ is unramified at $x$ by (5.6.5.8). □

Prop. (5.6.5.13) [Unramified U.i. Morphisms]. For a morphism $f$ of schemes, the following are equivalent:

- $f$ is unramified and a monomorphism.
- $f$ is unramified and universal injective.
- $f$ is locally of f.t., formally unramified and universal injective.
- $f$ is locally of f.t. and a monomorphism.
- $f$ is locally of f.t. and $X_y$ is either empty or $X_y \to y$ is an isomorphism for all $y \in Y$.

Proof: Cf. [Sta], 05VH. □

Prop. (5.6.5.14) [Unramified and Smoothness]. Let $f : X \to Y$ be a morphism of schemes over $S$ s.t. $X/S$ is smooth (of relative dimension $n$) and $Y/S$ is unramified, then $f$ is also smooth (of relative dimension $n$).

Proof: This follows from differential criterion (5.6.4.3) and (5.6.1.4). Notice to show it is flat, use the fact $\Delta_{Y/S}$ and $X \times Y \to Y$ are both flat (5.6.5.5). □
Noetherian Case

Prop. (5.6.5.15). Let $S$ be a Noetherian scheme, $X \to S$ a qc unramified morphism and $Y \to S$ a morphism with $Y$ Noetherian, then $\text{Mor}_S(Y, X)$ is a finite set.

Proof: Cf. [Sta], 0AKI.

Prop. (5.6.5.16) [Unramified Morphisms and DVR]. Let $R_v$ be a DVR with fraction field $K$ and $\varphi : X \to X'$ be a morphisms of schemes of f.t. over $R_v$. Let $Q \in X'(K)$ and $P \in X(K)$ with $\varphi(P) = Q$. Let $w|v$ be a valuation of $K(P)$ extending $v$. If $P$ extends to an $R_w$-valued point $\mathcal{P}$ of $X$, then using the fact $R_w \cap K = R_v$, we see $Q$ also extends to a $R_v$-valued point of $X'$.

Denote the image of the maximal ideal of $R_w$ under $P$ by $P(w)$, then if $\varphi$ is unramified at $P(w)$, then $K(P)/K$ is unramified in $w$.

Proof: Since the unramified point is open, $\varphi$ is also unramified at $P$, thus $K(P)/K$ is separable (5.6.5.8). For the rest, Cf. [Diophantine Geometry, P598].

6 Étale

More advanced materials to learn at [Sta] Chap 40.

Def. (5.6.6.1) [Étale Morphisms]. An étale morphism $f : X \to Y$ of schemes is a morphism s.t there is an open affine cover $\{U_i\}$ of $S$ and an open affine cover $V_{ij}$ of $f^{-1}(\{U_i\})$ that the ring map is étale. A standard étale morphism is the Spec map of a standard étale ring map.

étale is local on the source and target (4.4.7.5). Étale is stable under base change and composition (4.4.7.5).

Prop. (5.6.6.2) [Properties of Étale Morphisms].

- Étale at a point $x$ is equivalent to smooth and unramified at a $x$ (4.4.7.4).
- Étale at a point $x$ is equivalent to flat and $G$-unramified at that point, by (4.4.7.11). So étale over field is equivalent to $G$-unramified, because over a field it is obviously flat.
- Étale at a point $x$ is equivalent to locally standard étale at that point (4.4.7.17).
- A morphism is étale iff it is smooth of relative dimension 0, by definition (5.6.4.11).
- Étale is equivalent to flat, locally of f.p. and formally unramified, by (4.4.7.11).

Cor. (5.6.6.3). Étale map is smooth, hence syntomic, flat.

Étale map is universally open because it is flat and locally of f.p. (5.6.2.10).

Prop. (5.6.6.4). If $X, Y$ are étale over $S$, then any map $X \to Y$ is étale, by (4.4.7.13).

Prop. (5.6.6.5) [Fiberwise]. A morphism of schemes is étale iff it is flat, locally of f.p., and every fiber $X_s$ is a disjoint union of spectra of finite separable field extensions of $k(s)$.

Proof: Follows from (5.6.6.2) (5.6.5.3) and (4.4.7.10).

Cor. (5.6.6.6) [Étale Over Fields]. A scheme is étale over a field $k$ iff it is a disjoint union of spectra of finite separable field extensions. In particular, étaleover fields is equivalent to unramified over fields.
Prop. (5.6.6.7) [Smoothness and Étale]. If \( f : X \to Y \) is smooth at \( x \), then there exist a nbhd \( U \) of \( x \in X \) and nbhd \( V \) of \( f(x) \in Y \) that it factors through \( U \xrightarrow{\pi} \mathbb{A}^d \to V \), where \( \pi \) is étale.

Proof: Any standard smooth morphism can be factorized as an étale map over a polynomial algebra, as easily seen. \( \square \)

Prop. (5.6.6.8) [Stalkwise and Fiberwise]. For a morphism locally of f.p., by (5.6.5.8) and (5.6.4.5), the following are equivalent:

- It is étale at a point \( x \).
- \( \mathcal{O}_{X,x}/\mathcal{O}_{S,f(x)} \) if flat and \( X_{f(x)}/k(x) \) is smooth at \( x \).
- \( \mathcal{O}_{X,x}/\mathcal{O}_{S,f(x)} \) if flat and \( X_{f(x)}/k(x) \) is unramified at \( x \).
- \( \mathcal{O}_{X,x}/\mathcal{O}_{S,f(x)} \) is flat and \( \Omega_{X_{f(x)},x} = 0 \).
- \( \mathcal{O}_{X,x}/\mathcal{O}_{S,f(x)} \) is flat and \( \Omega_{X_{f(x)},x} \otimes_{\mathcal{O}_{X,x}} k(x) = 0 \).
- \( \mathcal{O}_{X,x}/\mathcal{O}_{S,f(x)} \) is flat and \( \mathfrak{m}_{f(x)}/\mathcal{O}_{X,x} = \mathfrak{m}_x \) and \( k(x)/k(s) \) separable.

In particular, an étale morphism can be seen as a family of smooth schemes.

Prop. (5.6.6.9) [Étale Schemes over Field]. Let \( k \) be a field and \( k^s \) its separable closure. Let \( \Gamma = \text{Gal}(k^s/k) \), then the functor \( X \mapsto X(k^s) \) is an equivalence between étale schemes over \( k \) to the category of discrete \( \Gamma \)-sets.

Proof: Cf. [Sta]03QR. \( \square \)

Prop. (5.6.6.10). If \( X \to Y \to S \), and \( X \to Y \) are faithfully flat and locally of f.p., \( X \to S \) is étale, then \( Y \to S \) is also étale.

Proof: Cf. [Sta]05B5. \( \square \)

Cor. (5.6.6.11). If \( f : X \to S \) is faithfully flat and locally of f.p., then the set of points of \( S \) s.t. \( f \) is étale is stable under base change.

Proof: This follows from (5.6.5.11) and (5.6.4.10). \( \square \)

Def. (5.6.6.12) [Étale Neighborhood]. For a point \( s : \text{Spec } k \to X \), an étale nbhd of \( s \) in \( X \) is defined to be an étale map \( U \to X \) that \( s \) factors through \( U \).

Prop. (5.6.6.13). For a morphism \( f : Y \to X \) of schemes étale over field \( k \), then \( f \) is surjective iff \( Y(k_s) \to X(k_s) \) is surjective.

Proof: If \( Y \to X \) is surjective, then? \( \square \)

Étale Connected Components

Def. (5.6.6.14) [Étale Connected Components]. Let \( X \) be a scheme over a field \( k \), let \( \pi_0(X) = \text{Spec}(\pi(X)) \), where \( \pi(X) \) is the largest étale subalgebra of \( \Gamma(X)(4.4.7.23) \).

Prop. (5.6.6.15). Let \( X \) be an algebraic scheme over a field \( k \), then

- for any field extension \( k'/k \), \( \pi_0(X_{k'}) = \pi_0(X)_{k'} \).
- Let \( Y \) be a schemes over a field \( k \), then \( \pi_0(X \times Y) = \pi_0(X) \times \pi_0(Y) \).
Proof:  1: Cf.[Mil17b]P15.
2: There is a map $\pi(X) \times_k \pi(Y) \to \pi(X \times Y)$. Because $\pi$ commutes with base change, we can base change to separable closure. In this case, it suffices to show if $X, Y$ is connected then $X \times Y$ is connected, but this follows from (5.4.3.12).

Prop. (5.6.6.16). Let $X$ be an algebraic scheme over a field $k$, then
- The mapping $\varphi : X \to \pi_0(X)$ induces a 1 to 1 correspondence of points of $\pi_0(X)$ and connected components of $X$.
- For all $x \in \pi_0(X)$, the fiber $\varphi^{-1}(x)$ is geo.connected over $k(x)$.

Proof: $\pi_0(X)$ is discrete, so the inverse image of each point is a sum of connected components of $X$. But this must be connected, because $\pi_0(X_{k(x)}) = \pi_0(X)_{k(x)} = k(x)$. Also, this implies for the alg.closure $\overline{k}$ of $k(x)$, $\pi_0(X_{\overline{k}}) = \pi_0(X_{k(x)})_{\overline{k}} = \overline{k}$, thus $X_{\overline{k}(x)}$ is geo.connected.

Noetherian Case

7 Zariski’s Main Theorem

References are [Sta]Chap36.38.

Prop. (5.6.7.1) [Zariski’s Main Theorem]. For a morphism $X \to S$ that is quasi-finite and separated, if $S$ is qcqs, Then there is a factorization $X \to T \to S$ that $X \to T$ is a qc open immersion and $T \to S$ is finite.

Proof: Cf.[Sta]05K0.

8 Complete Intersection

Should be refreshed with intrinsic definition of locally complete intersection, Cf.[Sta].

Def. (5.6.8.1) [Regular Embedding]. A regular embedding of codimension $r$ is a locally closed embedding $X \to Y$ that for $p \in X$, the ideal of $X$ in the local ring $\mathcal{O}_{Y,p}$ is generated by a regular sequence of length $r$.

Def. (5.6.8.2) [Complete Intersection]. A complete intersection of codimension $r$ in $Y$ is a closed subscheme $X$ that is the intersection of $r$ effective Cartier divisors $D_i$ that at each point $p \in X$, the equations defining $D_i$ form a regular sequence.

Def. (5.6.8.3) [Locally Complete Intersection]. A closed subscheme $Y$ of a nonsingular variety $X$ over a field $k$ is called locally complete intersection iff $Y$ is locally generated by $r = \text{codim}(Y,X)$ elements. By (4.3.4.17) $Y$ is C.M.. In particular, by (5.10.1.16), a regular variety is always a locally complete intersection.

Def. (5.6.8.4) [Syntomic Morphisms]. A standard syntomic morphism is the Spec map of a global complete intersection ring map (4.4.4.11). A syntomic morphism is a morphism that is locally a standard syntomic morphism.

Prop. (5.6.8.5). Syntomic is local on the source and target, stable under base change and composition, by (4.4.4.12).

Prop. (5.6.8.6). Syntomic is equivalent to flat, locally of f.p.+fibers being local complete intersections.
Proof: This follows from (4.4.4.18).

Cor. (5.6.8.7). Syntomic morphisms are universally open.

Prop. (5.6.8.8). An open immersion is syntomic, because localizations are global complete intersections (4.4.4.12).

Prop. (5.6.8.9). If \( f : X \to S \) is a syntomic map, then the function \( x \mapsto \dim_x(X_{f(x)}) \) is locally constant on \( X \). If it is standard syntomic, then it is constant.

Proof: It suffices to prove for syntomic maps, Cf. [Sta] 02K0.

Prop. (5.6.8.10). A local complete intersection has its ideal sheaf \( \mathcal{I} \), then \( \mathcal{I}/\mathcal{I}^2 \) locally free by (4.3.4.16).

Prop. (5.6.8.11). If \( Y \) is a complete intersection in \( \mathbb{P}_k^n \) of hypersurfaces of degree \( d_1, \ldots, d_r \), then \( \omega_Y = \mathcal{O}_Y(\sum_d_i - n - 1) \).

Proof: Use the exact sequence \( 0 \to \mathcal{O}_Z(n - d) \to \mathcal{O}_Z \to i_* \mathcal{O}_Y \to 0 \) and (5.10.1.17).

Prop. (5.6.8.12). For a complete intersection of dimension \( q \), \( H^i(Y, \mathcal{O}_Y(n)) = 0 \) for \( 0 < i < q \). And the natural map \( \Gamma(P, \mathcal{O}_P(n)) \to H^0(Y, \mathcal{O}_Y(n)) \) is a surjection for every \( n \). In particular, \( Y \) is connected, and the arithmetic genus \( p_a(Y) = \dim H^q(Y, \mathcal{O}_Y) \).

Proof: We use induction, the case \( Y = P \) follows from (5.7.2.1), let \( Y = Z \cap H \), where \( H \) has degree \( d \), then

\[
0 \to \mathcal{O}_Z(n - d) \to \mathcal{O}_Z \to i_* \mathcal{O}_Y \to 0
\]

thus use long exact sequence. The rest is easy.
5.7 Cohomology of Schemes

Main references are [Sta]Chap29.

Notations (5.7.0.1).
- Use notations defined in Cohomology on Ringed Sites.

1 Zariski Cohomology

Qco Sheaves

Lemma (5.7.1.1) [Zariski-Poincare]. A Qco sheaf on an affine scheme $X$ is Čech-acyclic.

Proof: Because the principal affine covers are cofinal in the ordering of covers, we only need to consider principal affine covers. Let $R \to A = \prod R_{f_i}$, then it is f.f., so we can use (4.4.2.2), just notice the higher term is $\prod_{i_0, \ldots, i_n} R_{f_{i_0} \cdots f_{i_n}}$. □

Prop (5.7.1.2) [Čech Cohomology on Separated Schemes]. If $X$ is separated and $F \in \mathcal{QCoh}(X)$, $H^p(X, F) = \check{H}^p(X, F) = H^p_{\text{alt}}\left(\{U_i \to X\}, F\right)$ for any open affine covering $\{U_i \to X\}$.

Proof: Use (5.3.2.16) and (5.3.2.6), the family of affine open subsets of $X$ satisfies the requirement because $X$ is separated and (5.7.1.1), thus the result. It can be calculated by alternating complexes by (5.3.2.7). □

Cor (5.7.1.3) [Affine Cohomological Vanishing]. If $X$ is affine and $F \in \mathcal{QCoh}(X)$, $H^i(X, F) = 0$ for $i > 0$.

For a qcqs scheme $X$, choose a finite affine cover $U_1, \ldots, U_t$ of $X$, then for any $F \in \mathcal{QCoh}(X)$, $H^n(X, F) = 0$ for $n \geq d$, where

\[ d = \max_{I \subseteq \{1, \ldots, t\}} (|I| + t(U_I)) \]

and $t(Y)$ is the minimal cardinality of an affine open cover of $Y$.

Proof: The last assertion follows form Čech to sheaf2 (5.3.2.13) and (5.7.1.2), as $U_I$ is separated for any $I \neq \emptyset$. □

Prop (5.7.1.4) [\mathcal{QCoh}(X) vs. \text{Mod}(O_X)]. If $X$ is a Noetherian scheme, then injective objects in $\mathcal{QCoh}(X)$ are all flabby (5.3.4.8), thus nearly calculating all cohomologies are legitimate in the category $\mathcal{QCoh}(X)$.

However, in general, this is not true, as there are examples of injective $A$-module $I$ s.t. $\check{I}$ is not flasque on Spec $A$, by [Sta]0274.

Proof: We use the Deligne formula (5.5.1.36) and the definition of injective, by considering the sheaf of ideals of the corresponding induced reduced structure. □

Prop (5.7.1.5) [Filtered Colimits]. If $X$ is qcqs, then sheaf cohomology on $X$ commutes with filtered colimits.

Proof: This follows from (5.1.4.9) the same way (6.4.1.8) follows from (5.1.4.20). □

Prop (5.7.1.6) [Ext For Coherent Sheaves]. On a locally Noetherian scheme, for $F \in \mathcal{QCoh}(X)$ and $G \in \mathcal{Coh}(X)$, $\mathcal{Ext}^i(F, G) \in \mathcal{QCoh}(X)$, and affine locally are given by $\mathcal{Ext}^i(F(U), G(U))$.

Moreover $G \in \mathcal{Coh}(X)$, then $\mathcal{Ext}^i(F, G) \in \mathcal{Coh}(X)$.
Proof: This follows from (5.8.5.13) and (5.8.5.10). □

Prop. (5.7.1.7). When \( X \) is locally Noetherian and \( \mathcal{F} \in \mathfrak{Coh}(X) \),
\[
\mathcal{E}xt^i(\mathcal{F}, \mathcal{G})_x \cong \text{Ext}^i_{\mathcal{O}_x}(\mathcal{F}_x, \mathcal{G}_x).
\]

Proof: Taking stalk is exact. □

Cor. (5.7.1.8). If \( X \) is locally Noetherian, suppose that every coherent sheaf is a quotient of a locally free sheaf, we can define the **homological dimension** \( \text{hd}(\mathcal{F}) \) of a coherent sheaf \( \mathcal{F} \) as the minimal length of a flat resolution of \( \mathcal{F} \). Then \( \text{hd}(\mathcal{F}) \leq n \iff \mathcal{E}xt^i(\mathcal{F}, \mathcal{G}) = 0 \) for every \( \mathcal{G} \) and every \( i > n \).

And \( \text{hd}(\mathcal{F}) = \sup \text{pd}_{\mathcal{O}_X}(\mathcal{F}_x) \), by (5.7.1.7).

Prop. (5.7.1.9) [Künneth Formula]. If \( X, Y \) are qcqs over a field \( k \) and \( \mathcal{F}, \mathcal{G} \) be \( \text{Qco} \ \mathcal{O}_X, \mathcal{O}_Y \)-modules, then there is a canonical isomorphism:
\[
H^n(X \times_{\text{Spec } k} Y, \text{pr}_1^* \mathcal{F} \otimes_{\mathcal{O}_X \otimes_{\text{Spec } k} Y} \text{pr}_2^* \mathcal{G}) \cong \oplus_{p+q=n} H^p(X, \mathcal{F}) \otimes_k H^q(Y, \mathcal{G}).
\]

Proof: Cf.[Sta]0BEF. □

Prop. (5.7.1.10). On a locally Noetherian scheme \( X \), any \( \text{Qco} \) sheaf \( \mathcal{F} \) admits a resolution of \( \text{Qco} \) sheaves that are flabby.

Proof: Because \( \text{QCoh}(X) \) is Serre subcategory, □

Lemma (5.7.1.11) [Gabber]. Let \( X \) be a scheme, then there exists a cardinal \( \kappa \) that every \( \text{Qco} \) sheaf is a colimit of its \( \kappa \)-generated \( \text{Qco} \) subsheaves.

Proof: Cf.[Sta]077N. □

Prop. (5.7.1.12) [\text{Qco Cohomology Comparison}]. For \( X \in \text{Sch}, \mathcal{F} \in \mathfrak{Coh}(X), \tau \in \{\text{fppf, étale, smooth, syntomic, Zariski}\} \), there are canonical isomorphisms
\[
H^p(X, \mathcal{F}) \cong H^p(\text{Sch}_\tau / X, \mathcal{F}) \cong H^p(X_{\text{Zar}}, \mathcal{F}) \cong H^p(X_{\text{ét}}, \mathcal{F}).
\]

Proof: Let \( \mathcal{C} = \text{Sch}_\tau / X \) or \( X_{\text{ét}}, X_{\text{Zar}} \). We use(5.3.2.16) with \( \mathfrak{G} \) the set of affine schemes and \( \text{Cov} \) the subset of \( \text{Cov}(\mathcal{C}) \) consisting of morphisms between affine schemes. Then Čech vanishing is clear in the affine case by(4.4.2.2). Thus(5.3.2.16) says \( H^p(\mathcal{C}, \mathcal{F}_\mathcal{C}) = 0 \) for \( p > 0 \).

Next, if \( U \subset X \) is an affine open s.t. \( U \to X \) is separated. Let \( \mathcal{U} \) be an affine open covering of \( U \), then all \( U_{i_0, \ldots, i_p} \) are affine, thus
\[
H^p(\mathcal{C}, \mathcal{F}_\mathcal{C}) = \check{H}(\mathcal{U}, \mathcal{F}_\mathcal{C}) = H^p(U, \mathcal{F}|_U)
\]
by(5.3.2.15).

Finally, for \( X \), take an injective resolution \( \mathcal{F} \to \mathcal{I}^* \), and an injective resolution \( \mathcal{F}_\mathcal{C} \to \mathcal{J}^* \). Then the latter restricts to a chain complex \( \mathcal{F} \to \mathcal{J}^*|_X \), which is exact because it is exact on any affine open \( U \subset X \) as \( H^p(\mathcal{C}, \mathcal{F}_\mathcal{C}) = 0 \) for \( p > 0 \). Thus by(3.4.3.5), there is a map \( \mathcal{J}^*|_X \to \mathcal{I}^* \), inducing a map \( H^p(\mathcal{C}, \mathcal{F}_\mathcal{C}) = H^p(X, \mathcal{J}^*) \to H^p(X, \mathcal{I}^*) \cong H^p(X, \mathcal{F}) \).

To show these map are isomorphisms, take an affine open covering \( U \) of \( X \), then there are Čech-to-derived spectral sequences
\[
^\tau E_2^{pq} = \check{H}^p(U, \mathcal{H}^q(\mathcal{F}^a)) \Rightarrow H^{p+q}(\mathcal{C}, \mathcal{F}_\mathcal{C}), \quad E_2^{pq} = \check{H}^p(U, \mathcal{H}^q(\mathcal{F}^a)) \Rightarrow H^{p+q}(\mathcal{C}, \mathcal{F}).
\]
The map \( \mathcal{J}^*|_X \to \mathcal{I}^* \) induces a map \( \check{C}^*(U, \mathcal{J}) \to \check{C}^*(U, \mathcal{I}) \) which induces a map of the spectral sequences. But as each affine open of \( X \) is separated over \( X \), the \( E^2 \)-page is an isomorphism by what we have proved. Thus \( \check{H}^q(\mathcal{F}^a) \to H^{p+q}(\mathcal{C}, \mathcal{F}) \) is an isomorphism. □
Proposition (5.7.1.13). For $X \in \text{Sch}$, $\tau \in \{\text{fpqc, étale, smooth, syntomic, Zariski}\}$,

$$H^1_r(X, \mathbb{G}_m) \cong \text{Pic}(X)(5.5.3.10).$$

Proof: As these $X_\tau$ are all locally ringed sites, by (5.3.1.17), $H^1_r(X, \mathbb{G}_m) \cong \text{Pic}(X_\tau)$. Thus it suffices to prove that

$$\text{Pic}(X_{\text{Zar}}) \to \text{Pic}(X_{\text{ét}}) \to \ldots \to \text{Pic}(X_{\text{fpqc}})$$

are isomorphisms. Then this is because any invertible sheaf is quasi-coherent by (5.2.5.8), so Pic$(X_\tau)$ are in fact the group of invertible objects in $\Omega\text{coh}(X_\tau)$. But $\Omega\text{coh}(X_\tau)$ are all equivalent categories, by fpqc descent for Qco sheaves (5.1.5.12).

2 Proper Schemes

Proposition (5.7.2.1) [Cohomology of Projective Space]. Let $X = \mathbb{P}^r_A$ we have:

(1)

$$H^q(X, \mathcal{O}_X(d)) = \begin{cases} (A[T_0, \ldots, T_r])_d & q = 0 \\ 0 & q \neq 0, r \\ \left(\frac{1}{T_0 \cdots T_r} A[\frac{1}{T_0}, \ldots, \frac{1}{T_r}]\right)_d & q = r \end{cases}$$

(2) The cup product defines a perfect pairing

$$H^0(X, \mathcal{O}_X(n)) \times H^r(X, \mathcal{O}_X(-n - r - 1)) \to H^r(X, \mathcal{O}_X(-r - 1)) \cong A.$$

Proof: $X$ is separated, we use Čech cohomology. Let $\mathcal{F} = \bigoplus_{d \in \mathbb{Z}} \mathcal{O}_X(d)$, then $\mathcal{F}$ is a Qco graded ring. Let $U_{i_0 \ldots i_k}$ be the affine open subset $U(x_{i_0}) \cap \ldots U(x_{i_k})$ of $X$, then $\mathcal{F}(U_{i_0 \ldots i_k}) = A[T_0, \ldots, T_r, T_{i_0}^{-1}, \ldots, T_{i_k}^{-1}]$ as graded rings, and the cohomology $H^\bullet(\mathcal{F})$ is calculated by the Čech complex (5.3.2.1)

$$\check{C}^\bullet = \prod_i A[T_0, \ldots, T_r, T_i^{-1}] \to \prod_{i,j} A[T_0, \ldots, T_r, T_i^{-1}, T_j^{-1}] \to \ldots \to A[T_0, \ldots, T_r, T_1^{-1}, \ldots, T_r^{-1}].$$

This complex has a natural $\mathbb{Z}^r$-grading, and the differential is natural inclusion thus preserves the grading, i.e.

$$\check{C}^\bullet = \bigoplus_{v \in \mathbb{Z}^r} \check{C}^\bullet(v)$$

where if we set $NEG(v) = \{i \in \{0, \ldots, r\} | v_i < 0\}$, then

$$\check{C}^\bullet(v) = \prod_{NEG(v) \subset \{i\}} A T_0^{v_0} \ldots T_r^{v_r} \to \prod_{NEG(v) \subset \{i,j\}} A T_0^{v_0} \ldots T_r^{v_r} \to \ldots \to A T_0^{v_0} \ldots T_r^{v_r}$$

is the subcomplex of $\check{C}^\bullet$. So it suffices to calculate the cohomology of $\check{C}^\bullet(v)$ for each $v$.

If $NEG(v) = \{0, 1, \ldots, n\}$, then there is only one term, so

$$H^\bullet(\check{C}^\bullet(v)) = \begin{cases} A T_0^{v_0} \ldots T_r^{v_r} & q = r \\ 0 & \text{otherwise} \end{cases}$$

The sum of all such $v$ clearly contribute to $\frac{1}{T_0 \cdots T_r} A[\frac{1}{T_0}, \ldots, \frac{1}{T_r}]$ in degree $r$.

If $NEG(v) = 0$, then the complex is isomorphic to the Čech complex calculating cohomology of Spec $A$ using the trivial cover $\{V_i \to \text{Spec} A\}, V_i \cong \text{Spec} A$ times $T_0^{v_0} \ldots T_r^{v_r}$. As Spec is separated,
it is just to the sheaf cohomology of Spec \( A \), which is \( A \) is degree 0 and 0 otherwise by (5.7.1.1). The sum of all such \( v \) clearly contribute to \( A[T_0, \ldots, T_r] \) in degree 0.

Finally, for other \( v \), choose a \( j \in \{0, 1, \ldots, n\} \setminus \mathrm{NEG}(v) \), then the maps

\[
h : \check{C}^{p+1}(v) \to \check{C}^p(v) : h(s)_{i_0 \ldots i_p} = s_{j i_0 i_p}
\]

(where we are using the alternating Čech complex) induces a homotopy between 0 and id, so \( \check{C}^{p+1}(v) \) have trivial cohomologies.

The pairing given by cup product makes \( T_0^{v_0} \ldots T_r^{v_r} \) dual to \( T_0^{-1-v_0} \ldots T_r^{-1-v_r} \), thus it is a perfect pairing.

\[\square\]

**Cor. (5.7.2.2)**. when \( n > 0 \), \( H^r(X, \mathcal{O}_X(n - r - 1)) = 0 \). Notice this an instance of the Kodaira vanishing theorem when \( k \) has characteristic 0 (11.8.8.3).

**Prop. (5.7.2.3)**. Let \( X = \mathbb{P}^n_k \) and \( 0 \leq p, q \leq n \), then \( H^q(X, \mathcal{O}_X^p) = 0 \) for \( p \neq q \) and when \( p = q \), \( H^q(X, \mathcal{O}_X^p) = k \).

**Proof**: By (5.5.1.26) and (5.5.5.7), there is an exact sequence \( 0 \to \Omega^q \to \wedge^q \mathcal{O}(-1) \to \Omega^{q-1} \to 0 \), and the middle has vanishing \( q \)-th cohomology by (5.7.2.1), thus we can induct and (5.7.2.1) gives the result.

**Prop. (5.7.2.4) [Cohomology of Complete Intersections]**. Let \( X \) be a closed subscheme of \( \mathbb{P}^n_k \) defined by a single homogenous equation \( f(x_0, x_1, x_2) \) of degree \( d \), then show that \( \dim H^0(X, \mathcal{O}_X) = 1 \), and if \( n \geq 2 \), \( \dim H^1(X, \mathcal{O}_X) = (d - 1)(d - 2)/2 \).

**Proof**: By (5.5.3.15), there is an exact sequence of sheaves on \( \mathbb{P}^n_k \):

\[
0 \to \mathcal{O}_{\mathbb{P}^n_k}(-d) \cong \mathcal{O}_{\mathbb{P}^n_k}(-X) \to \mathcal{O}_{\mathbb{P}^n_k} \to i_* \mathcal{O}_X \to 0
\]

which induces a long exact sequence (5.7.4.2):

\[
\begin{align*}
H^0(\mathbb{P}^n_k, \mathcal{O}_{\mathbb{P}^n_k}(-d)) & \to H^0(\mathbb{P}^n_k, \mathcal{O}_{\mathbb{P}^n_k}) \to H^0(X, \mathcal{O}_X) \to H^1(\mathbb{P}^n_k, \mathcal{O}_{\mathbb{P}^n_k}(-d)) \\
& \to H^1(\mathbb{P}^n_k, \mathcal{O}_{\mathbb{P}^n_k}) \to H^1(X, \mathcal{O}_X) \to H^2(\mathbb{P}^n_k, \mathcal{O}_{\mathbb{P}^n_k}(-d)) \to H^2(\mathbb{P}^n_k, \mathcal{O}_{\mathbb{P}^n_k})
\end{align*}
\]

By (5.7.2.1), this reads:

\[
0 \to k \to H^0(X, \mathcal{O}_X) \to 0 \to 0 \to H^1(X, \mathcal{O}_X) \to H^2(\mathbb{P}^n_k, \mathcal{O}_{\mathbb{P}^n_k}(-d)) \to 0,
\]

and if \( n = 2 \), \( \dim H^2(\mathbb{P}^2_k, \mathcal{O}_{\mathbb{P}^2_k}(-d)) = (d - 1)(d - 2)/2 \).

\[?\] It is faster using Hilbert Polynomial.

\[\square\]

**Lemma (5.7.2.5) [Cohomology of Projective Space]**. Let \( R \) be a Noetherian ring and \( n \geq 0 \), then for any coherent sheaf \( \mathcal{F} \) on \( \mathbb{P}^n_R \),

- \( H^i(\mathbb{P}^n_R, \mathcal{F}(n)) = 0 \) for \( i > 0 \) and \( n \) large enough.
- For any \( i \), \( H^i(\mathbb{P}^n_R, \mathcal{F}) \) is a finite \( R \)-module.
- For any \( k \in \mathbb{Z} \), \( \bigoplus_{d \geq k} H^0(\mathbb{P}^n_R, \mathcal{F}(d)) \) is a finite \( R[T_0, \ldots, T_n] \)-module.
5.7. COHOMOLOGY OF SCHEMES 629

1: The assertions are true for $\mathcal{O}_X(n)$ by (5.7.2.1), and for general $\mathcal{F}$, we use descending induction on $i$. This is true for $i > n$ by Čech cohomology (5.7.1.2). For general $i > 0$, choose a surjection $\bigoplus \mathcal{O}_X(n_i) \to \mathcal{F}$ with coherent kernel $\mathcal{R}(5.5.4.5)$, then there is an exact sequence

$$H^i(X, \oplus \mathcal{O}_X(n_i + n)) \to H^i(X, \mathcal{F}(n)) \to H^{i+1}(X, \mathcal{R}(n)),$$

and the left term vanish for $n$ large (5.7.2.1), and the right term vanish by induction hypothesis.

2: Notation as above, we use descending induction on $i$. This is true for $i > n$ by Čech cohomology (5.7.1.2). For general $i > 0$, $H^i(X, \oplus \mathcal{O}_X(n_i))$ is finite by (5.7.2.1), and $H^{i+1}(X, \mathcal{R})$ is finite by induction hypothesis, thus $H^i(X, \mathcal{F}(n))$ is also finite.

3: Notation as above, for $n$ large, $H^i(X, \oplus \mathcal{O}_X(n_i + n)) \to H^i(X, \mathcal{F}(n))$ is surjective. Thus $M_k = \bigoplus_{d \geq k} H^0(\mathbb{P}_k^n, \mathcal{F}(d))$ is a quotient of $N_k = \bigoplus_{d \geq k} H^0(\mathbb{P}_k^n, \mathcal{O}_X(d))$ for $k$ large. Notice for $k$ small enough, $N_k \cong \oplus_{i} R[T_0, \ldots, T_n][i]$ is a finite graded $R[T_0, \ldots, T_n]$-module, thus $N_k$ is finite for any $k$ as $R[T_0, \ldots, T_n]$ is Noetherian. Then $M_k$ is finite for $k$ large, and each $H^0(\mathbb{P}_k^n, \mathcal{F}(d))$ is itself finite by item 2, thus $M_k$ is a finite $R[T_0, \ldots, T_n]$-module for any $k$.

**Prop. (5.7.2.6)** [Cohomology of Proper Schemes]. Let $X$ be a proper scheme over a Noetherian ring $A$, $\mathcal{L}$ an ample invertible sheaf on $X$ and $\mathcal{F} \in \text{Coh}(X)$, then

- $H^i(X, \mathcal{F} \otimes \mathcal{L}^\otimes d) = 0$ for $i > 0$ and $d$ large enough.
- The graded ring $A = \bigoplus_{n \geq 0} H^0(X, \mathcal{L}^\otimes n)$ is a f.g. $R$-algebra.
- For any $k \in \mathbb{Z}$, $\bigoplus_{d \geq k} H^0(X, \mathcal{F} \otimes \mathcal{L}^\otimes d)$ is a finite $A$-module.

**Proof:** By (5.5.4.24), there exists a $d > 0$ and some immersion $i : X \to \mathbb{P}_A^n$ that $i^* \mathcal{O}_{\mathbb{P}_A^n}(1) \cong \mathcal{L}^\otimes d$, and $i$ is a closed immersion because $X$ is proper. Let $S = R[T_0, \ldots, T_n]$.

1: By projection formula (5.7.4.6),

$$i_*(\mathcal{F} \otimes \mathcal{O}_X \mathcal{L}^\otimes nd+q) = i_*(\mathcal{F} \otimes \mathcal{O}_X \mathcal{L}^\otimes q)(n).$$

Then by (5.7.4.2) and (5.7.2.5), for $n$ large enough, $H^p(X, \mathcal{F} \otimes \mathcal{L}^\otimes q) = 0$ for any $0 \leq q \leq d - 1$, $p > 0$.

2: By proof of item 1 and (5.7.2.5), we see $\oplus_{n \geq 0} A_{nd+q}$ is a finite graded $S$-module for any $q$, thus $A = \bigoplus_{q=0}^{d-1} \bigoplus_{n \geq 0} A_{nd+q}$ is a f.g. $R$-module.

3: Similarly, we see $\bigoplus_{d \geq k} H^0(X, \mathcal{F} \otimes \mathcal{L}^\otimes d)$ is a finite graded $S$-module, and the $S$-module structure factors through $S \to A$, thus it is a finite $A$-module. □

**Lemma (5.7.2.7).** For an invertible sheaf $\mathcal{L}$ on a qc scheme $X$, if for each Qco sheaf of ideals $\mathcal{I} \in \mathcal{O}_X$, there exists an $n$ that $H^1(X, \mathcal{I} \otimes \mathcal{L}^n) = 0$, then $\mathcal{L}$ is ample.

**Proof:** For any closed pt $P$, choose an open affine nbhd $U$ that $\mathcal{L}$ is trivial, let $Y = X - U$, by the exact sequence $0 \to \mathcal{I}_Y \cup \{p\} \to \mathcal{I}_Y \to k(P) \to 0$, for each $n$,

$$0 \to \mathcal{I}_Y \cup \{p\} \otimes \mathcal{L}^n \to \mathcal{I}_Y \otimes \mathcal{L}^n \to k(P) \otimes \mathcal{L}^n \to 0.$$

Thus by assumption for some $n$ the map $\Gamma(X, \mathcal{I}_Y \otimes \mathcal{L}^n) \to \Gamma(X, k(P) \otimes \mathcal{L}^n)$ is surjective. Now $k(P) \otimes \mathcal{L}^n \cong A/\mathfrak{m}_P$, so we let $s \in \Gamma(X, \mathcal{I}_Y \otimes \mathcal{L}^n)$ maps to a section in $\Gamma(X, k(P) \otimes \mathcal{L}^n)$ that corresponds to $1 \in A/\mathfrak{m}_P$, then $P \in \text{Supp}(s) \subset U$, and $\text{Supp}(s)$ is affine. So we find an affine nbhd $X_s$ for every closed pt of $X$.

Finally these $X_s$ cover $X$, because the complement of $\cup X_s$ is closed in $X$ thus qc, then it contains a closed point by (3.6.6.1). □
Prop. (5.7.2.8) [Serre’s Cohomological Criterion of Ampleness]. If \( X \) is proper over a Noetherian affine scheme, \( \mathcal{L} \) is an invertible sheaf, then the following is equivalent.

- \( \mathcal{L} \) is ample
- For any \( \mathcal{F} \in \text{Coh}(X) \), for \( n \) large enough, \( H^p(X, \mathcal{F} \otimes \mathcal{L}^n) = 0 \) for \( p > 0 \).
- For any \( \mathcal{O}_X \) sheaf of ideals \( \mathcal{I} \in \mathcal{O}_X \), there exists an \( n \geq 1 \) that \( H^1(X, \mathcal{I} \otimes \mathcal{L}^{\otimes n}) = 0 \) (Notice in this case \( H \)-ample \( \iff \) ample).

Proof: 1 \( \rightarrow \) 2: This follows from (5.7.2.6). 2 \( \rightarrow \) 3 is trivial. 3 \( \rightarrow \) 1: (5.7.2.7). \( \square \)

Lichtenbaum’s theorem

Lemma (5.7.2.9). Let \( X \) be a variety and \( \mathcal{F} \in \text{Coh}(\mathcal{O}_X) \). If \( H^d(X, \mathcal{F}) \neq 0 \), then \( \dim X \geq d \), and if equality holds, \( X \) is proper.

Proof: Cf. [Sta]0G1E. \( \square \)

Prop. (5.7.2.10) [Lichtenbaum]. Let \( X \) be a non-empty separated scheme of f.t. over a field \( k \) of dimension \( d \), then the following are equivalent:

- \( H^d(X, \mathcal{F}) = 0 \) for all \( \mathcal{F} \in \text{Coh}(X) \).
- \( H^d(X, \mathcal{F}) = 0 \) for all \( \mathcal{F} \in \text{QCoh}(X) \).
- No irreducible component of \( X \) of dimension \( d \) is proper over \( k \).

Proof: Cf. [Sta]0G1F. \( \square \)

3 Euler Characteristics

Def. (5.7.3.1) [Euler Characteristic]. Let \( X \) be proper over a field \( k \) and \( \mathcal{F} \in \text{Coh}(X) \), then the Euler characteristic of \( \mathcal{F} \) is defined to be:

\[
\chi(\mathcal{F}) = \sum (-1)^i \dim_k H^i(X, \mathcal{F}).
\]

It is definable by Grothendieck vanishing (5.3.5.22) and Grothendieck coherence theorem (5.7.4.12), and it is clearly an additive functor on \( \text{Coh}(X) \).

Prop. (5.7.3.2). For a proper scheme \( X \) over a field \( k \) and \( \mathcal{L}_i \) be invertible sheaves on \( X \). Then for any \( \mathcal{F} \in \text{Coh}(X) \),

\[
\chi(X, \mathcal{F} \otimes \mathcal{L}_1^{n_1} \otimes \cdots \otimes \mathcal{L}_r^{n_r})
\]

is a polynomial in \( (n_1, \ldots, n_r) \) of total degree at most \( \dim \text{Supp} \mathcal{F} \).

Proof: Cf. [Sta]0B1E. \( \square \)

Prop. (5.7.3.3). Let \( f : Y \rightarrow X \) be morphism between schemes proper over field \( k \) and \( \mathcal{F} \in \text{Coh}(X) \),

\[
\chi(Y, \mathcal{F}) = \sum (-1)^i \chi(X, R^if_*\mathcal{F}).
\]

In particular, if \( f \) is affine(finite), then \( \chi(Y, \mathcal{F}) = \chi(X, f_*\mathcal{F}) \).

Prop. (5.7.3.4). This formula makes sense by (5.7.4.4) and (5.7.4.12), and it is true by Leray spectral sequence (5.3.1.10).
Prop.(5.7.3.5). If $X$ is a proper scheme and $F \in \mathcal{Coh}(X)$ with $\dim \text{Supp}(F) = 0$, then $F$ is generated by global sections, $H^i(X,F) = 0$ for $i > 0$, and

$$\chi(X,F \otimes \mathcal{E}) = n\chi(X,F)$$

for any $\mathcal{E} \in \mathcal{V}ect^n(X)$.

Proof: The first two are clear as $F = i_* \mathcal{G}$ where $i : \text{Supp}(F) \to X$. The last assertion follows from the projection formula \(5.7.4.6\) $i_*(\mathcal{G} \otimes i^* \mathcal{E}) \cong F \otimes \mathcal{E}$.

Def.(5.7.3.6)[Arithmetic Genus]. The arithmetic genus of a proper scheme of dimension $r$ over a field is defined to be $p_a(X) = (-1)^r (\chi(\mathcal{O}_X) - 1)$ $(5.7.3.1)$. In particular, when $X$ is a complete curve over a field $k$, then $p_a(X) = \dim_k H^1(X, \mathcal{O}_X)$ $(5.10.1.12)$.

The arithmetic genus is stable under base change of fields, by flat base change theorem.

Prop.(5.7.3.7)[Arithmetic Genus of Product]. By Künneth formula, if $X,Y$ are proper schemes of dimension $r,s$ over a field $k$, then

$$H^n(X \otimes_k Y, \mathcal{O}_{X \otimes_k Y}) \cong \bigoplus_{0 \leq k \leq n} H^k(X, \mathcal{O}_X) \otimes H^{n-k}(Y, \mathcal{O}_Y).$$

Thus $\chi(X \times_k Y) = \chi(X)\chi(Y)$. In particular, we have

$$p_a(X \times Y) = p_a(X)p_a(Y) + (-1)^s p_a(X) + (-1)^r p_a(Y).$$

Prop.(5.7.3.8)[Arithmetic Genus of Complete Intersections]. Let $C$ be a smooth complete intersection of a degree $m$ surface $S_1$ and a degree $n$ surface $S_2$ in $\mathbb{P}_k^3$, then $p_a(C) = \frac{1}{2}(mn(m+n-4) + 2)$.

Proof: There are exact sequences $0 \to \mathcal{O}_{\mathbb{P}_k^3}(-S_1) \to \mathcal{O}_{\mathbb{P}_k^3} \to \mathcal{O}_{S_1} \to 0$, which gives

$$0 \to \mathcal{O}_{\mathbb{P}_k^3}(-S_2)|_{S_1} \to \mathcal{O}_{S_1} \to \mathcal{O}_{S_1 \cap S_2} \to 0.$$ 

So by adjunction formula,

$$K_C = K_{S_1}(S_1 \cap S_2)|_C = K_{\mathbb{P}_k^3}(S_1)(S_2)|_C = \mathcal{O}_C(m+n-4).$$

So $2g - 2 = mn(m+n-4)$.

Prop.(5.7.3.9)[Asymptotic Riemann-Roch]. If $X$ is a proper scheme over a field $k$ of dimension $d$ and $\mathcal{L}$ is an ample invertible sheaf, then $\dim \Gamma(X, \mathcal{L}^n) \sim cn^d$.

Proof: Cf. [Sta]0BJ8.

Hilbert Polynomials

References are [Hartshorne I.7] and [Vak17].

Prop.(5.7.3.10)[Hilbert Polynomial]. For a projective scheme over a field $k$ and a coherent sheaf $F$, there is a polynomial Hilbert polynomial $P \in \mathbb{Q}[\lambda]$ that $\chi(F(n)) = P(n)$, and $\deg P \leq \dim \text{Supp}(F)$.

This Hilbert polynomial is compatible with the definition in $(5.7.3.12)$, because by $(5.7.4.7)$, the higher cohomology group vanishes for $n$ large, so $\chi(F(n)) = \Gamma(F(n)) = \Gamma_*(F)_n$. 

Proof: 

Prop. (5.7.3.11). Let \( X \hookrightarrow Y \hookrightarrow \mathbb{P}^n_k \) be a sequence of closed embeddings, then \( P_X(m) \leq P_Y(m) \) for \( m \) large, and if equality holds for \( m \) large, then \( X = Y \).

Proof: Cf. [Vak17]P490.

Def. (5.7.3.12) [Hilbert Polynomial]. For a scheme projective over a field \( k \) of dimension \( r \), we define the Hilbert polynomial \( P_Y \) as the Hilbert polynomial of its homogenous coordinate ring \( \Gamma_*(Y) \). It has dimension \( r \) by (4.2.2.17).

The degree of \( Y \) is defined as the \( r! \) times the leading coefficients of \( P_Y \).

Prop. (5.7.3.13).
- The degree is a positive integer.
- If \( Y = Y_1 \cup Y_2 \) and \( \dim Y_1 \cap Y_2 < r \), then \( \deg Y = \deg Y_1 + \deg Y_2 \).
- If \( H \) is a hypersurface whose ideal is generated by a homogeneous polynomial of degree \( d \), then \( \deg H = d \).

Proof: Cf. [Hartshorne P52].

Prop. (5.7.3.14). For a variety of degree \( k \) and a general linear space, the intersection has \( k \) points.

Proof: 

4 Relative Cohomology

Prop. (5.7.4.1) [Filtered Colimits]. If \( f : X \to Y \) is qcqs, then \( R^if_* \) commutes with filtered colimits, by (5.3.1.7) and (5.7.1.5).

Prop. (5.7.4.2) [Sheaf Cohomology Commutes with Affine Map]. For \( f : X \to Y \) affine and \( \mathcal{F} \in \mathcal{Q}\text{Coh}(X) \), \( H^n(Y, \mathcal{F}) = H^n(X, f_*\mathcal{F}) \).

Proof: Because \( R^if_*\mathcal{F} = 0 \) by (5.7.1.3) and (5.3.1.8), we can then use (5.3.1.9) to conclude. 

Prop. (5.7.4.3) [Higher Direct Image Preserves Qco Sheaves]. If \( f : X \to S \) is qcqs then \( R^n f_* \) maps \( \mathcal{Q}\text{Coh}(X) \) to \( \mathcal{Q}\text{Coh}(S) \), and for \( U \subset S \) affine open, \( (R^n f_*\mathcal{F})|_U = (H^n(f^{-1}(U), \mathcal{F}))^\wedge \).

Proof: Firstly by (5.3.3.18), \( (R^n f_*\mathcal{F})|_U = R^n f_{U*}(\mathcal{F}|_U) \), so it suffices to prove for \( S \) affine. Then \( R^nf_*\mathcal{F} \) is the sheafification of the presheaf \( G : U \mapsto H^n(f^{-1}(U), \mathcal{F}) \) by (5.3.1.8).

If \( f \) is separated, then we can use Čech cohomology (5.7.1.2) to see that \( H^n(f^{-1}(D(f)), \mathcal{F}) = H^n(X, \mathcal{F})_f \) thus \( G \) is itself a sheaf and the conclusion follows.

In general we can choose a finite affine cover \( U_i \) of \( X \), then every intersection of \( U_i \) is quasi-compact and separated, and there is a spectral sequence convergence \( H^p(\{U_i \to X\}, H^q(\mathcal{F})) \Rightarrow H^{p+q}(X, \mathcal{F}) \), where the left can be calculated using Čech cohomology. Taking localization w.r.t. \( f \), we get the desired isomorphism \( H^n(f^{-1}(D(f)), \mathcal{F}) = H^n(X, \mathcal{F})_f \) also by comparison (3.4.7.5).

Prop. (5.7.4.4) [Cohomological Boundedness of \( Rf_* \)]. For a qcqs morphism \( f : X \to S \), if \( S \) is qc, there is an \( N \) that for every base change \( f' \) of \( f \), we have \( R^n f_*\mathcal{F} = 0 \) for every \( \mathcal{F} \in \mathcal{Q}\text{Coh}(X) \) and \( n \geq N \).

In particular, if \( f \) is affine, then \( R^n f_*\mathcal{F} = 0 \) for \( n > 0 \). And if \( f \) is projective, then \( R^n f_*\mathcal{F} = 0 \) for \( n \) bigger than the maximal dimension of the fiber of \( f \).
Proof: Check affine locally on $S$ and use (5.7.4.3), choose a finite affine cover $U$ of $X$. Then when $n$ is large, $(R^n f_* \mathcal{F})|_U = 0$ by (5.7.4.3) and (5.7.1.3) for any $i$, thus $R^n f_* \mathcal{F} = 0$. For base changes, notice the cardinality of the affine cover are the same.

\[\□\]

Cor. (5.7.4.5). For a qc separated scheme $X$, the cohomology vanish for $n$ large. And when $X$ is separated and can be covered by $r$ affine opens, then $N$ can chosen to be $r$.

Cor. (5.7.4.6) [Projection Formula].
- Let $f : X \to Y$ be a morphism of schemes, and $\mathcal{E}$ a locally free $\mathcal{O}_Y$-module, then for any $\mathcal{F} \in \text{Mod}(\mathcal{O}_X)$ and any $i$, there are natural isomorphisms.
  \[R^i f_*(\mathcal{F} \otimes f^* \mathcal{E}) \cong R^i f_*(\mathcal{F}) \otimes \mathcal{E}.\]
- If $f : X \to Y$ is a qcqs morphism of schemes, then for any $\mathcal{F} \in \text{Coh}(\mathcal{O}_X), \mathcal{E} \in \text{Coh}(\mathcal{O}_Y)$, there is a natural isomorphism
  \[R f_*(\mathcal{F} \otimes ^L f^* \mathcal{E}) \cong R f_*(\mathcal{F}) \otimes ^L \mathcal{E}.\]

Proof: 1 follows from (5.3.3.20) and 2 follows from (5.8.5.8).

Proper Morphism and $\text{Coh}(X)$

Prop. (5.7.4.7) [Relative Serre Vanishing]. If $f : X \to Y$ is a proper morphism of locally Noetherian schemes, $\mathcal{I}$ an invertible sheaf on $X$, then the following are equivalent:
- $\mathcal{L}$ is $f$-ample.
- For any $\mathcal{F} \in \text{Coh}(X)$, for $n$ sufficiently large, $R^i f_*(\mathcal{F} \otimes \mathcal{I}^\otimes n) = 0$ and $i > 0$.
- For any Qco sheaf of ideals $\mathcal{I} \subset \mathcal{O}_X$, there exists an $n \geq 1$ that $R^1 f_*(\mathcal{I} \otimes \mathcal{L}^\otimes n) = 0$.

Proof: 1 $\to$ 2: By (5.7.4.3), this follows from (5.7.2.8). 2 $\to$ 3 is trivial as $X$ is Noetherian. 3 $\to$ 1: Notice for any affine open subset $U$ of $Y$, $U \to Y$ is qc, thus $f^{-1}(U) \to X$ is quasi-compact, thus by (5.5.1.8), a Qco sheaf of ideals $\mathcal{I}$ on $f^{-1}(U)$ can be extended to a Qco sheaf of ideals on $X$. Then we can use (5.7.4.3) and Leray spectral sequence to reduce to (5.7.2.8).

Cor. (5.7.4.8). Let $X$ be proper over a Noetherian affine scheme with an ample invertible sheaf $\mathcal{L}$, then for any finite exact sequence in $\text{Coh}(X)$, if tensoring it with $\mathcal{L}^\otimes n$ for large $n$, the resulting global section is exact.

Cor. (5.7.4.9). Let $X$ be proper over a Noetherian affine scheme with an ample invertible sheaf $\mathcal{L}$, and $\mathcal{F}, \mathcal{G} \in \text{Coh}(X), i \geq 0$, then for $n$ large (depending on $\mathcal{F}, \mathcal{G}, i$),
\[\text{Ext}^i(\mathcal{F}, \mathcal{G}(n)) \cong \Gamma(X, \mathcal{E}xt^i(\mathcal{F}, \mathcal{G}(n))).\]

Proof: By (5.3.3.34)(5.7.1.6), there is a spectral sequence s.t. for $n$ large, all the small terms vanish.

\[\□\]

Lemma (5.7.4.10). If $f : X \to Y$ is projective and $Y$ locally Noetherian, then for any $n \in \mathbb{N}$, $R^n f_*$ maps coherent sheaves to coherent sheaves.

Proof: By (5.7.4.3), this problem is local on the target, so we may assume that $Y = \text{Spec} \ R$ and $X = \mathbb{P}^n_R$, in which case this follows from (5.7.2.5).
Prop. (5.7.4.11) [Grothendieck’s Coherence Theorem]. If \( f : X \to Y \) is proper and \( Y \) locally Noetherian, then for any \( n \in \mathbb{N} \), \( R^n f_* \) maps coherent sheaves to coherent sheaves.

Proof: By (5.7.4.3), this problem is local on the target, so we may assume \( Y \) is Noetherian, and then \( X \) is also Noetherian. We prove by devissage (5.5.1.55): 1 is trivial, for 2, for any closed subscheme \( i : Z \subset X \), denote \( g = f|_Z \), then it suffices to find a coherent sheaf \( \mathcal{G} \) on \( Z \) s.t.

1. \( \mathcal{G}_{\xi} \cong k(\xi) \).
2. \( R^p g_* \mathcal{G} \) are coherent for any \( p \geq 0 \).

Because then \( i_* \mathcal{G} \) is a coherent sheaf on \( X \) (5.5.1.32) that \( R^p f_*(i_* \mathcal{G}) = R^p g_* \mathcal{G} \) for any \( p \) by relative Leray spectral sequence (5.3.1.9) and (5.7.4.4), and also \( (i_* \mathcal{G})_{\xi} = \mathcal{G}_{\xi} \).

As \( g : Z \to Y \) is proper, by Chow’s lemma (5.4.5.23), there is a birational, \( H \)-projective map \( \pi : Z' \to Y \) over \( Y \). Then there is a closed immersion \( j : Z' \to \mathbb{P}^n_Y \) and an induced closed immersion \( j': Z' \to \mathbb{P}^n_Z \). Then \( \mathcal{L} = j^* \mathcal{O}_{\mathbb{P}^n_Y}(1) = (j')^* \mathcal{O}_{\mathbb{P}^n_Z}(1) \) is both \( g \circ \pi \)-relatively ample and \( \pi \)-relatively ample.

Hence by relative Serre vanishing (5.7.4.7) there exists an \( n \) that \( R^p \pi_* \mathcal{L}^\otimes n = 0 \) for any \( p > 0 \). Let \( \mathcal{G} = \pi_* \mathcal{L}^\otimes n \), then this \( \mathcal{G} \) satisfies the conditions: \( \mathcal{G}_{\xi} = \kappa(\xi) \) as \( \pi^{-1}(U) \to U \) is an isomorphism, and from relative Leray spectral sequence

\[
R^p g_* R^q \pi_* \mathcal{L}^\otimes n \implies R^n (g \circ \pi)_* \mathcal{L}^\otimes n,
\]

we see \( R^p g_* \mathcal{G} \cong R^p g'_* \mathcal{L}^\otimes n \), which are coherent by (5.7.4.10). \( \square \)

Cor. (5.7.4.12) [Coherent Cohomology Finite]. If \( \pi : X \to \text{Spec} \, A \) is proper over a Noetherian affine scheme \( A \) and \( \mathcal{F} \) is a coherent sheaf on \( X \), \( H^i(X, \mathcal{F}) \) are finite \( A \)-modules.

Proof: By (5.7.4.3), \( R^p \pi_* \mathcal{F} \) is the Qco sheaf \( H^p(X, \mathcal{F}) \), which is coherent iff \( H^p(X, \mathcal{F}) \) is a finite \( A \)-module. \( \square \)

Prop. (5.7.4.13). Given a proper morphism between locally Noetherian schemes \( f : X \to Y \), a coherent sheaf \( \mathcal{F} \) on \( X \) and a coherent sheaf of ideals \( \mathcal{I} \) of \( \mathcal{O}_Y \). Then \( \mathcal{M} = \bigoplus_{n \geq 0} R^p f_*(\mathcal{I}^n \mathcal{F}) \) is a Qco graded \( A = \bigoplus_{n \geq 0} \mathcal{T}^n \)-module of f.t..

Proof: By (5.7.4.3), this is local on \( Y \), so we may assume \( Y \) is affine, Cf.[Sta]02O8. \( \square \)

Prop. (5.7.4.14). Let \( f : X \to Y \) be a proper morphism between locally Noetherian schemes and \( \mathcal{F} \) a coherent sheaf on \( X \), \( y \in Y \). Consider the infinitesimal nbhds \( X_n = \text{Spec}( \mathcal{O}_{Y, y} / \mathfrak{m}^n_y ) \times_Y X \xrightarrow{i_n} X \) of the fiber \( X_1 = X_y \), and set \( \mathcal{F}_n = i_n^* \mathcal{F} \), then

\[
(R^n f_* \mathcal{F})_y \cong \lim_n H^n(X_n, \mathcal{F}_n)
\]
as \( \mathcal{O}_{Y, y} \)-modules.

Proof: Cf.[Sta]02OD. \( \square \)

Cor. (5.7.4.15) [Support of Higher Direct Images]. Let \( f : X \to Y \) be a proper morphism between locally Noetherian schemes and \( y \in Y \) s.t. \( \dim(X_y) = d \), then for any coherent sheaf \( \mathcal{F} \) on \( X \), \( (R^p f_* \mathcal{F})_y = 0 \) for \( p > d \).

Proof: Cf.[Sta]02V7. \( \square \)
5 Base Change

Prop. (5.7.5.1) [Flat Base Change]. For a Cartesian diagram of schemes

\[
\begin{array}{ccc}
X' & \xrightarrow{g'} & X \\
\downarrow{f'} & & \downarrow{f} \\
S' & \xrightarrow{g} & S
\end{array}
\]

If \(g\) is flat and \(f\) is qcqs, then for every Qco sheaf \(F\) on \(X\) with base change \(F'\) on \(X'\), there is a canonical isomorphism

\[g^* Rf_* F \cong Rf'_* F'.\]

By (5.3.3.18), when \(S, S'\) is affine, this reads:

\[H^i(X, F) \otimes A B \cong H^i(X \otimes A B, (g')^* F).\]

**Proof:** Firstly by (5.3.3.18)(5.7.4.3), it suffices to show for \(S, S'\) affine. If \(X\) is separated, then the then we can use Čech cohomology (5.7.1.2), and the Čech complex of \(K'\) is just the cohomology of the Čech complex tensored with \(B\), so it commutes with taking cohomology because \(B\) is \(A\)-flat.

Now if \(X\) is only qs, then we choose a finite affine open cover \(\{U_i\}\), then every intersection of \(U_i\) is quasi-compact and separated. and there is a spectral sequence convergence \(H^p(\{U_i \to X\}; H^q(F)) \Rightarrow H^{p+q}(X, F)\). Tensoring with \(B\), we also get the desired isomorphism \(H^i(X, F) \otimes A B \cong H^i(X \otimes A B, (g')^* F)\) by comparison (3.4.7.5).

□

Prop. (5.7.5.2) [Finite Locally Free Base Change]. For a Cartesian diagram of schemes

\[
\begin{array}{ccc}
X' & \xrightarrow{g'} & X \\
\downarrow{f'} & & \downarrow{f} \\
S' & \xrightarrow{g} & S
\end{array}
\]

If \(S = \text{Spec } A, S' = \text{Spec } B\) and \(B\) is finite locally free over \(A\), for every Qco sheaf \(F\) on \(X\) with base change \(F'\) on \(X'\), there is a canonical isomorphism

\[H^i(X, F) \otimes A B \cong H^i(X \otimes A B, (g')^* F).\]

**Proof:** If \(X\) is separated, then the then we can use Čech cohomology (5.7.1.2), and the Čech complex of \(K'\) is just the cohomology of the Čech complex tensored with \(B\), so it commutes with taking cohomology because \(B\) is \(A\)-flat and tensoring a f.p. ring map commutes with colimits of rings.

In general we choose an affine open cover \(\{U_i\}\), then every intersection of \(U_i\) is separated. and there is a spectral sequence convergence \(H^p(\{U_i \to X\}; H^q(F)) \Rightarrow H^{p+q}(X, F)\). Tensoring with \(B\), we also get the desired isomorphism \(H^i(X, F) \otimes A B \cong H^i(X \otimes A B, (g')^* F)\) by comparison (3.4.7.5).

□

Prop. (5.7.5.3) [Representing Higher Direct Image]. Let \(f : X \to S\) be a qcqs morphism of schemes. If \(S\) is qc and separated and \(F\) is a Qco sheaf on \(X\), there exists a \(K^\bullet \in K^+(\text{QCoh}(\mathcal{O}_S))\) s.t. for any morphism \(g : S' \to S\), the complex \(g^* K^\bullet\) is a representative for \(Rf'_* F'\), where the notation is as in (5.7.5.1).
Prop. (5.7.5.4) [Proper Flat Base Change]. If $f : X \to S$ is a proper morphism of f.p., then

- If $E$ a perfect object in $D(O_X)$, $\mathcal{G} \in D(O_X)$ is representable by a bounded complex of f.p. $O_X$-modules flat over $S$, then

$$Rf_* (E \otimes_{O_X} ^L \mathcal{G}^*) , \quad Rf_* R\mathcal{H}om (E, \mathcal{G}^*)$$

are perfect complexes in $D(O_S)$, and its formation commutes with base change.

- If $E$ a pseudo-coherent object in $D(O_X)$, $\mathcal{G} \in D(O_X)$ is representable by a bounded above complex of f.p. $O_X$-modules flat over $S$, then $Rf_* (E \otimes_{O_X} ^L \mathcal{G}^*)$ is a pseudo-coherent complex in $D(O_S)$, and its formation commutes with base change.

Proof: Cf. [Sta]0A1H, 0A1J, 0CSC.

Cor. (5.7.5.5). Let $f : X \to S$ be a proper morphism of f.p., then

- If $E \in D(O_X)$ is perfect(pseudo-coherent) and $f$ is flat, then $Rf_* E$ is a perfect(pseudo-coherent) object in $D(O_S)$, and its formation commutes with base change.

- If $\mathcal{G} \in \mathcal{Q}coh^f(O_X)$ and is flat over $S$, then $Rf_* \mathcal{G}$ is a perfect object of $D(O_S)$ and its formation commutes with base change.

Cor. (5.7.5.6). If $A \in \mathcal{C}Alg$, $X$ be a proper scheme of f.p. over $A$, then if $\mathcal{G} \in \mathcal{Q}coh^f(O_X)$ and is flat over $A$, there exists a finite complex of finite projective $A$-modules $L^\bullet$ that for any $A' \in \mathcal{C}Alg_A$, $M \in Mod_A$, by (5.7.5.5) and projection formula (5.7.4.6),

$$H^i(X_{A'}, \mathcal{F}_{A'}) = H^i(L^\bullet \otimes_A A'), \quad H^i(X, \mathcal{F} \otimes_A M) = H^i(L^\bullet \otimes_A M)$$

6 Semicontinuity

Prop. (5.7.6.1). $T^i$ is left exact iff $Coker d^{i-1}$ is a projective $A$-module, iff it is representable by a finite $A$-module.

Proof: Denote $W^i = Coker d^{i-1}$, then $Coker d^{i-1} \otimes_A M = W^i \otimes M$, because tensoring is right exact. Thus $T^i(M) = \ker (W^i \otimes M \to L^{i+1} \otimes M)$. Then for $M' \subset M$, there is a commutative diagram

$$
\begin{array}{cccc}
0 & \to & T^i(M) & \to & W^i \otimes M^' & \to & L^{i+1} \otimes M^' \\
& & \downarrow^{\alpha} & & \downarrow^{\beta} & & \downarrow^{\gamma} \\
0 & \to & T^i(M) & \to & W^i \otimes M & \to & L^{i+1} \otimes M \\
\end{array}
$$
γ is injective, so using spectral sequence, its clear α is injective iff β is injective, i.e. $W^i$ is flat, which is equivalent to finite projective (4.3.1.7).

To prove $T^i$ is representable, let $Q = \text{Coker}(L^{i+1, *} \rightarrow W^{i, *})$, then $Q$ is finite because $W^i$ is finite (4.3.1.18), and $0 \rightarrow \text{Hom}(Q, M) \rightarrow \text{Hom}(W^{i, *}, M) \rightarrow \text{Hom}(L^{i+1, *}, M)$, but by (4.3.1.19), the last two are just $W^i \otimes M$ and $L^{i+1} \otimes M$, $\text{Hom}(Q, M) = T^i(M)$ by what has already been proved. □

**Prop. (5.7.6.2).** $T^i$ is right exact iff the cup product $H^i(X, \mathcal{F}) \otimes_A M \rightarrow H^i(X, \mathcal{F} \otimes_A M)$ is an isomorphism for any $A$-module $M$.

*Proof:* Because $T^i$ and $\otimes$ commutes with direct limit, it suffices to prove for $M$ finite. In this case, choose a finite presentation $A^r \rightarrow A^s \rightarrow M \rightarrow 0$, then there is a diagram

$$
\begin{array}{ccc}
T^i(A) \otimes A^r & \rightarrow & T^i(A) \otimes A^s \\
\downarrow & & \downarrow \\
T^i(A^r) & \rightarrow & T^i(A^s) \\
\end{array}
$$

The first two vertical arrows are isomorphisms, so if $T^i$ is right exact, so does the third vertical arrow. Conversely, if $T^i(A) \otimes_A M \rightarrow T^i(M)$ are all isomorphisms, then by a similar diagram, we can show $T^i(M) \rightarrow T^i(M')$ are surjective for $M \rightarrow M'$ surjective. □

**Cor. (5.7.6.3).** $T^i$ is exact if it is right exact and $T^i(A) = H^i(X, \mathcal{F})$ is a finite projective $A$-modules.

*Proof:* When $T^i$ is right exact, $H^i(X, \mathcal{F} \otimes_A M) \cong H^i(X, \mathcal{F}) \otimes_A M$ by (5.7.6.2), so it is exact iff $H^i(X, \mathcal{F})$ is flat. Because it is in priori finite, this is equivalent to finite projective (4.3.1.7). □

**Def. (5.7.6.4).** For a point $y \in \text{Spec } A$, define $T^i_y(N) = H^i(L^*_y \otimes N)$, then $T^i$ is (left/right)exact at $y$ iff $T^i_y$ are all (left/right)exact (exact sequence is stalkwise (4.1.4.2)).

**Prop. (5.7.6.5).** If $T^i$ is (left/right)exact at a point $y$, then the same is true on a nbhd of $y$.

*Proof:* From (5.7.6.1), $(\text{Coker } d^{i-1})_y$ is a finite projective $A_y$ module, so it is free, and it is a coherent sheaf, so it is free at a nbhd of $y$ by (5.5.1.38), so the same is true on a nbhd of $y$. Now right exactness of $T^i$ is equivalent to left exactness of $T^{i+1}$, and exact is left exact + right exact, so we are done. □

**Prop. (5.7.6.6).** $T^i$ is right exact at $y$ iff $H^i(X, \mathcal{F}) \otimes k(y) \rightarrow H^i(X, \mathcal{F} \otimes_A k(y))$ is surjective.

*Proof:* Cf.[Hartshorne P289]. □

**Prop. (5.7.6.7)[Cohomology and Stalks].** Let $f : X \rightarrow Y$ be a proper morphism of locally Noetherian schemes and $\mathcal{F}$ is a coherent sheaf on $X$ flat over $Y$, $y \in Y$, then

- If the natural map
  $$\varphi^i(y) : R^if_*(\mathcal{F}) \otimes k(y) \rightarrow H^i(X_y, \mathcal{F}_y)$$
  is surjective, then it is an isomorphism, and and the same is true for $y'$ in an open nbhd of $y$.

- Assume $\varphi^i(y)$ is surjective, then $\varphi^{i-1}(y)$ is also surjective iff $R^if_*(\mathcal{F})$ is finite projective in a nbhd of $y$.

*Proof:* 1: This follows from (5.7.6.2) (5.7.6.6) and (5.7.6.5).

2: $\varphi^{i-1}(y), \varphi^i(y)$ are both surjective iff $T^i$ and $T^{i-1}$ are both right exact at $y$ (5.7.6.6), which is equivalent to $T^i$ exact at $y$. Then we finish by (5.7.6.3) □
Remark (5.7.6.8). How’s this related to (5.7.5.5)?

Prop. (5.7.6.9) [Semicontinuity of Cohomology]. Let $X \to Y$ be a projective morphism of locally Noetherian schemes and $\mathcal{F}$ is a coherent sheaf on $X$, flat over $Y$, then for each $i$, $h^i(y, \mathcal{F}) = \dim_{k(y)} H^i(X_y, \mathcal{F}_y)$ is an upper semicontinuous function on $Y$.

Proof: The question is local on $Y$, so we may assume $Y$ is affine Noetherian. By (5.7.5.1), $H^i(y, \mathcal{F}) = \dim_{k(y)} T^i(k(y))$. And as in the proof of (5.7.6.1), $T^i(M) = \ker(W^i \otimes M \to L^{i+1} \otimes M)$, and $W^i \to L^{i+1} \to W^{i+1} \to 0$ is exact, so $0 \to T^i(k(y)) \to W^i \otimes k(y) \to L^{i+1} \otimes k(y) \to W^{i+1} \otimes k(y) \to 0$, and counting dimension, $h^i(y, \mathcal{F}) = \dim W^i \otimes k(y) + \dim W^{i+1} \otimes k(y) - \dim L^{i+1} \otimes k(y)$. Notice the last term is constant as $L^{i+1}$ is free $A$-module and the first two terms are upper semicontinuous by (5.5.1.41), thus $h^i(y, \mathcal{F})$ is upper-semicontinuous. □

Cor. (5.7.6.10) [Grauert]. If $Y$ is integral and $h^i(y, \mathcal{F})$ is constant on $Y$, then $R^i f_*(\mathcal{F})$ is locally free on $Y$ and $R^i f_*(\mathcal{F}) \otimes k(y) \cong H^i(X_y, \mathcal{F}_y)$.

Proof: Cf. [Hartshorne P288]. □
5.8 Topics in Schemes

Main references are [Sta] and [Har77].

1 Cartier Divisors

Def.(5.8.1.1)[Cartier Divisor]. A Cartier divisor on a scheme $X$ is an element in $\Gamma(X, K^*_X/O^*_X)$.

An effective Cartier divisor is a Cartier divisor that is locally defined as $\{(U_i, f_i)\}$ where $f_i \in \Gamma(U_i, O_{U_i})$ are nonzero-divisors, equivalently, it is a closed subscheme whose ideal sheaf is an invertible sheaf. (Notice by definition, $K$ is the localization w.r.t. nonzero-divisors, and $f_i$ is invertible in $K^*$ so $f_i$ must be nonzero-divisors.)

The group of effective Cartier divisors is denoted by $\text{Cart}_{\text{eff}}(X)$.

The Cartier divisor group $\text{CaCl}$ is the quotient of $\Gamma(X, K^*) \to \Gamma(X, K^*/O^*_X)$.

Prop.(5.8.1.2)[Cartier Divisor is Nowhere Dense]. Let $D \subset X$ be an effective Cartier divisor, then it is nowhere dense in $X$, i.e. $X \setminus D \to X$ is scheme-theoretically dense.

Proof: It suffices to check affine-locally, it is qc so the scheme-theoretic closure of $\text{Spec } A_f \to \text{Spec } A$ is $V(\ker(A \to A_f)) = V(0)$ as $f$ is a nonzero-divisor. □

Prop.(5.8.1.3)[Closed Subschemes and Effective Cartier Divisors]. Let $X$ be a locally Noetherian scheme and $D \subset X$ is a closed subscheme corresponding to a Qco sheaf of ideals $\mathcal{I} \subset O_X$. If for any $x \in D$, the ideal $\mathcal{I}_x \subset O_{X,x}$ is generated by a single nonzero-divisor, then $D$ is an effective Cartier divisor.

Proof: Cf.[Sta]0AG8. □

Cor.(5.8.1.4)[Prime Divisor and Effective Cartier Divisor]. Let $X$ be a locally Noetherian scheme and $D$ is a prime Weil divisor on $X$ and $O_{X,x}$ are UFDs for any $x \in D$, then $D$ is an effective Cartier divisor.

Proof: For any $x \in D$, let $A = O_{X,x}$, and $p$ be the prime corresponding to the generic point of $D$, then $\dim A_p = 1$, so $p$ is principle as $A$ is a UFD, so $D$ is an effective Cartier divisor by(5.8.1.3). □

Prop.(5.8.1.5) [Cartier-Pic]. For an integral scheme $X$, the homomorphism $\text{CaCl}(X) \to \text{Pic}(X)(5.8.1.1)(5.5.3.10)$ induced from long exact sequence of $0 \to O^*_X \to K^*_X \to K^*_X/O^*_X \to 0$ is an isomorphism.

Explicitly, for a Cartier divisor $D = \{(U_i, f_i)\}$, the image is the invertible sheaf $O_X(D)(5.5.3.12)$.

Proof: It is clearly injective by definition, so it suffices to show any invertible sheaf can embed into the constant sheaf: for any invertible sheaf $\mathcal{L}$, tensor with $K$ and restrict to the stalk of the generic point, i.e. there is a compatible choice of homomorphisms into $K(X)$. □

Prop.(5.8.1.6). If $X$ is Noetherian and the diagonal map is affine, for a dense affine open $U$, if all the stalk of $X \setminus U$ are UFD, then $U$ is the complement of an effective Cartier divisor.

Proof: The irreducible complements of $X \setminus U$ is finite and has codimension 1 by(5.6.3.5) because $U \to X$ is affine, and it is an effective Cartier divisor by(6.1.5.1), so their sum will suffice. □

Prop.(5.8.1.7) [Pullback of Effective Cartier Divisors]. Let $f : X \to Y \in \text{Sch}$ and $D \in \text{Cart}_{\text{eff}}(Y)$, then the pullback of $D$ via $f$ is an effective Cartier divisor on $X$ in the following cases:
Prop. (5.8.1.10) [Fibral Criterion of Relative Effective Divisor]. If $X$ is a Noetherian scheme with an ample invertible sheaf $L$, then any line bundle in $\text{Pic}(X)$ is isomorphism to $\mathcal{O}_X(D - D')$ for some effective Cartier divisors $D, D'$ on $X$.

Proof: Cf. [Sta] OAYM.

Relative Effective Cartier Divisors

Def. (5.8.1.9) [Relative (Effective) Cartier Divisors]. Let $X$ be a scheme over $S$, then a relative effective (Cartier) divisor on $X/S$ is an effective Cartier divisor $D$ on $X$ that is flat over $S$.

Prop. (5.8.1.10) [Fibral Criterion of Relative Effective Divisor]. Let $f : X \to S$ be a morphism of locally Noetherian schemes locally of f.t., $D \subset X$ be a closed subscheme and $x \in D$, $s = f(x)$, then the following are equivalent:

- $D$ is a relative effective divisor at a nbhd of $x$.
- $X$ and $D$ are flat over $S$ at $x$, and the fiber $D_s$ is a Cartier divisor on $X_s$ at $x$.
- $X$ is flat over $S$ at $x$, and $D$ is cut out by an element that is regular on the fiber $X_s$.

In particular, a relative Cartier divisor pair can be regarded as a family of Cartier divisors pairs.

Proof: 1 $\to$ 2: Let $\mathcal{O}_{D,x} = b\mathcal{O}_{X,x}$, then there is an exact sequence $0 \to \mathcal{O}_{X,x} \xrightarrow{b} \mathcal{O}_{X,x} \to \mathcal{O}_{D,x} \to 0$, which induces a long exact sequence

$$
\text{Tor}_1^{\mathcal{O}_S,s}(\mathcal{O}_{X,x}, k(s)) \to \text{Tor}_1^{\mathcal{O}_S,s}(\mathcal{O}_{X,x}, k(s)) \to \text{Tor}_1^{\mathcal{O}_S,s}(\mathcal{O}_{D,x}, k(s)) \to \mathcal{O}_{X,x} \otimes k(s) \xrightarrow{b} \mathcal{O}_{X,x} \otimes k(s).
$$

Because $D$ is flat over $S$, $\text{Tor}_1^{\mathcal{O}_S,s}(\mathcal{O}_{D,x}, k(s)) = 0$, thus $b$ is regular in $\mathcal{O}_{X,x}$ and $D_s$ is an effective divisor on $X_s$ at $x$. Also the map $\text{Tor}_1^{\mathcal{O}_S,s}(\mathcal{O}_{X,x}, k(s)) \to \text{Tor}_1^{\mathcal{O}_S,s}(\mathcal{O}_{X,x}, k(s))$ is surjective, which is multiplication by $b$, and $b$ is in the maximal ideal, thus by Nakayama lemma, $\text{Tor}_1^{\mathcal{O}_S,s}(\mathcal{O}_{X,x}, k(s)) = 0$. Then $\mathcal{O}_{X,x}$ is $\mathcal{O}_{S,s}$-flat by local criterion (4.4.1.16).

2 $\to$ 3: Let $D$ corresponds to an ideal $I$ in $\mathcal{O}_{X,x}$, and because $D_s$ is effective divisor on $X_s$, there exists $b \in I$ s.t. the image of $b$ in $\mathcal{O}_{X,x} \otimes k(s)$ generate the ideal of $D_s$. Then it suffices to show that $b$ generates $I$. Notice there is an exact sequence $0 \to I \to \mathcal{O}_{X,x} \to \mathcal{O}_{D,x} \to 0$, and $\mathcal{O}_{D,x}$ is flat over $\mathcal{O}_{S,s}$, thus $I \otimes k(s) \to \mathcal{O}_{X,x} \otimes k(s)$ is injective, and the image is just the ideal of $D_s$, thus $b$ generates $I \otimes k(s)$. Thus by Nakayama, it also generates $I$.

3 $\to$ 1: The exact sequence $0 \to I \to \mathcal{O}_{X,x} \to \mathcal{O}_{D,x} \to 0$ induces the long exact sequence

$$
\text{Tor}_1^{\mathcal{O}_S,s}(\mathcal{O}_{X,x}, k(s)) \to \text{Tor}_1^{\mathcal{O}_S,s}(\mathcal{O}_{D,x}, k(s)) \to I \otimes k(s) \to \mathcal{O}_{X,x} \otimes k(s).
$$

$I \otimes k(s) \to \mathcal{O}_{X,x} \otimes k(s)$ is injective because its composition with $\mathcal{O}_{X,x} \otimes k(s) \to I \otimes k(s) \to \mathcal{O}_{X,x} \otimes k(s)$ is multiplication by $b$, thus injective as $b$ is regular on the fiber $X_s$. Thus $\text{Tor}_1^{\mathcal{O}_S,s}(\mathcal{O}_{D,x}, k(s)) = 0$, thus $D$ is flat at $x$ by local criterion (4.4.1.16). And also $I$ is flat over $\mathcal{O}_{S,s}$. Notice $b : \mathcal{O}_{X,x} \to I$ is isomorphism after tensoring $k(x)$ and $I$ is flat, so $\ker(b) = 0$ by Nakayama, and $b$ is regular.
Cor. (5.8.1.11). If \( D, E \) are relative effective Cartier divisors on \( X/S \), then \( D + E \) is also a relative Cartier divisor on \( X/S \).

\[
\text{Proof: } \text{This follows from item 3 of (5.8.1.10).} \quad \square
\]

Prop. (5.8.1.12) [Pullback of Divisors]. For \( S \in \text{Sch}, X \in \text{Sch}/S \) and \( Z \) an relative Cartier divisor on \( X/S \), then for any \( T \in \text{Sch}/S \), \( Z_T \) is a relative Cartier divisor on \( X_T/T \).

And if \( f : X' \to X \) is a flat morphism over \( S \), then \( f^*Z \) is also a relative Cartier divisor on \( X'/S \).

\[
\text{Proof: } \text{If } 0 \to O_X \xrightarrow{\mathcal{I}} O_X \to i_*O_Z \to 0, \text{ then } 0 \to O_{X_T} \xrightarrow{\mathcal{I}_T} O_{X_T} \to i_*O_{Z_T} \to 0 \text{ because } O_Z \text{ is flat over } O_S, \text{ so } \mathcal{I}_T \text{ is also an effective divisor on } X_T/T. \\
\text{The second case is similar.} \quad \square
\]

2 Blowing Up

Blowing-up serves as a way to magnify local properties to global ones.

Def. (5.8.2.1) [Blowing-Up]. Let \( X \) be a scheme and a closed subscheme \( Z \subset X \) defined by \( \mathcal{I} \), the blowing up of \( X \) along \( Z \) \( \text{Bl}_Z X \) is defined as the map \( \beta : \text{Proj}_{X}(\oplus_{d \geq 0} \mathcal{I}^d) \to X \).

The map \( \beta : \text{Bl}_Z X \to X \) pulls back \( Z \) to an effective Cartier divisor \( E_Z X \), called the exceptional divisor, and it has the universal property that any morphism \( Y \to X \) that pulls back \( Z \) to an effective Cartier divisor uniquely factors through \( \text{Bl}_Z X \).

\[
\text{Proof: } \text{Notice first an effective divisor is equivalent to an invertible sheaf of ideal. And any morphism } Z \to X \text{ pulls back } I \text{ to the image of } f^{-1}I \otimes_{O_X} O_Z \to f^{-1}I \cdot O_Z. \text{ This is just } O(1) \text{ on } \text{Bl}_X Z \text{ so invertible.} \\
\text{For the construction, the local uniqueness will implies the existence. Notice locally } \bar{X}_I \text{ is projective over } X. \text{ Now because the } Z \to X \text{ pulls back } I \text{ to an invertible sheaf and it is generated by } f^{-1}(a_i), \text{ we use?? to get another } \text{Proj}_{X}(\oplus_{d \geq 0} \mathcal{I}^d) \text{ and it factors through the closed subscheme } \bar{X}_I. \text{ If there is another morphism } g, \text{ then } f^{-1}I \cdot O_Z = g^{-1}(\pi^{-1}I \cdot O_{\bar{X}_I}) \cdot O_Z = g^{-1}(O_{\bar{X}_I}) \cdot O_Z \text{ surjective, and a surjective morphism between two invertible sheaves is an isomorphism, and they are both ideal sheaves, thus the same, so this morphism is unique as it is determined by the map on } O_X??. \quad \square
\]

Cor. (5.8.2.2). Let \( X \) be a scheme and \( Z \subset X \).

- If \( Z \) is itself an effective Cartier divisor, then the \( \text{Bl}_Z X = X \).
- If \( U \subset X \) is an open subscheme, then \( \text{Bl}_Z(U) = \beta^{-1}(U) \subset \text{Bl}_Z(X) \). In particular, Blowing-up is a local construction.
- If \( Z = X \), then \( \text{Bl}_Z X = \emptyset \).
- \( \beta \) is an isomorphism \( \beta^{-1}(X \setminus Z) \to X \setminus Z \) away from \( Z \).
- If \( X \) is reduced, then \( \text{Bl}_Z X \) is also reduced.
- If \( X \) is irreducible and \( Z \) doesn’t contain the generic point of \( X \), then \( \text{Bl}_Z X \) is irreducible.

\[
\text{Proof: } \text{1: By universal property.} \\
\text{2: This follows from universal property and the fact the restriction of an effective Cartier divisor is an effective Cartier divisor.}
\]
3: By universal property.
4: By item 2 and 3.
5: ?
6: ?

Cor. (5.8.2.3). \( \pi : \tilde{X}_I \to X \) is birational, proper thus surjective. If \( X \) is a (complete) variety, then so does \( \tilde{X}_I \).

Def. (5.8.2.4)[Strict Transform]. Let \( Z \subset X \) is a closed subscheme and \( f : Y \to X \) be a morphism, then \( Y \times_X \text{Bl}_Z X \) is called the total transform of \( Y \), and the strict transform of \( Y \) is the scheme-theoretic closure of \( Y \times_X \text{Bl}_Z X \) \( \setminus Y \times_X E_Z X \) in \( Y \times_X \text{Bl}_Z X \), or equivalently the closed subscheme of \( Y \times_X \text{Bl}_Z X \) cut out by the Qco ideal of sections supported on \( Y \times_X E_Z Y \).

Prop. (5.8.2.5)[Strict Transformation]. Let \( Z \subset X \) is a closed subscheme and \( f : Y \to X \) be a morphism, then the strict transform of \( Y \) is the blowing-up of \( Y \) at the closed subscheme \( f^{-1}Z \).

Proof: Cf.[Sta]080E. (Recall the definition of fiber product, we only need to check for \( Z, X \) affine and glue. For this, check \( B \otimes_A (\oplus I^d) \to \oplus (IB)^d \) defines the fiber map).

Prop. (5.8.2.6). If \( X \) is \( H \)-quasi-projective, then so does \( \tilde{X}_I \) and \( \pi \) is \( H \)-projective(5.5.2.19). And any birational projective morphism from another variety \( Z \) to \( X \) comes from a blowing-up.

Proof: Cf.[Hartshorne]P166.

Prop. (5.8.2.7)[Exceptional Divisor]. Let \( E = \pi^{-1}(x) \) for a blowing-up, called the exceptional divisor. Often the line bundle \( \mathcal{O}_\tilde{X}(E) \) associated with it is called denoted by \( E \).

There are canonical coordinates near \( E \): let \( \tilde{U}_i \) be \( \tilde{U} - \{ (l_i = 0) \} \), then endow \( \tilde{U}_i \) with the coordinate \( z(i) = (l_j/l_i, \ldots, z_i, \ldots, l_n/l_i) \), it is holomorphic to \( \mathbb{C}^n \). \( \pi \) in this coordinate is written as \( (z(1), \ldots, z(n)) \mapsto (z(i)z(z(1)), \ldots, z(i)z(i), \ldots, z(i)z(z(n))) \).

The transition function can be written, it is

\[
\varphi_j \circ \varphi_i^{-1}((z(i)_1, \ldots, z(i)_n)) = \left(\frac{z(i)_1}{z(i)_j}, \ldots, \frac{1}{z(i)_j}, \ldots, \frac{z(i)}{z(i)_j}, \ldots, \frac{z(i)_n}{z(i)_j}\right).
\]

Notice it is somewhat tricky because it has two different coordinates.

The defining function of \( E \) in this coordinate is \( (z(i)) = (z_i) \). So the line bundle \( \mathcal{O}_\tilde{X}(E) \) has transition function \( g_{ij} = z(i)/z(j) \), and it can be thought of as the line bundle that has line \([l] \) at the point \((z, [l]) \in \tilde{U} \). So it is kindof tautological, in fact its restriction on \( E \cong \mathbb{C}P^{n-1} \) is just the tautological line bundle.

Prop. (5.8.2.8). The canonical line bundle \( \mathcal{K}_\tilde{X} = \pi^* \mathcal{K}_X + (n - 1)E \), where \( n \) is the dimension of \( X \).

Proof: Away from \( E \), the \( \pi \) is a holomorphism, so it suffices to compare the two transition function of the two canonical maps near \( E \) using the coordinates in (5.8.2.7), with the local section given by \( dz_1 \wedge \ldots \wedge dz_n \) and \( dz(i)_1 \wedge dz(i)_n \) respectively. On \( \tilde{U}_i \), locally \( dz_1 \wedge \ldots \wedge dz_n \) is pulled by \( \pi^* \) to the trivial bundle on \( U' \), and by calculation, \( dz(j)_1 \wedge dz(j)_n = z(i)^{n-1}dz(i)_1 \wedge dz(i)_n \), so \( \mathcal{K}_\tilde{X} - (n - 2)E \) has a global section \( z(i)^n dz(i)_1 \wedge dz(i)_n \), so it is also trivial on \( \tilde{U} \), so \( \mathcal{K}_\tilde{X} = \pi^* \mathcal{K}_X + (n - 1)E \) is true.
Blowing up along a regular variety

Prop.(5.8.2.9). If $X$ is a regular variety over $k$ and $Y$ is a regular closed subvariety defined by $I$, then the blowing up along $I$ is also regular, and the inverse image $Y' \to Y$ is isomorphic to $P(I/I^2)$, the projective space associated to the locally free bundle $I/I^2$ on $Y$, and the normal sheaf $\mathcal{N}_{Y'/X'} \cong \mathcal{O}_{P(I/I^2)}(-1)$.

Proof: (Imagine the blowing up of $\mathbb{A}^2$ along $\{0\}$). $X' \cong \text{Proj} \oplus I$ and $Y' \cong \text{Proj} \oplus I/I^2$. Then since $Y$ is regular, (4.3.4.17) tells us $I$ is locally generated by a regular sequence and (4.3.4.16) tells $Y' = P(I/I^2)$. $Y'$ is regular by (4.3.5.18), and then (4.3.5.24) shows that $X'$ is regular also. For the normal sheaf, the defining sheaf $I' = \mathcal{O}_{X'}$ and then $I' \cong \mathcal{O}_{Y'} \sim \mathcal{O}_{P(I/I^2)(-1)}$.

□

Prop.(5.8.2.10). In a blowing up along a regular variety of codimension $r \geq 2$, there is an isomorphism $\text{Pic}X' \cong \text{Pic}X \oplus \mathbb{Z}$ induced by the Weil divisor exact sequence of $Y' \subset X'$. This is because $r \geq 2$ and (5.8.2.2).

We also have $\omega_{X'} = f^* \omega_X \otimes \mathcal{L}(r-1)Y'$ because $\mathcal{L}(Y') = \mathcal{O}(-1)$ and $\omega_Y \cong \omega_X \otimes \mathcal{L}(D) \otimes \mathcal{O}_Y$ by (5.10.1.17), so it suffices to prove $\omega_{Y'} \cong f^* \omega_X \otimes \mathcal{O}_{Y'}(-r)$. For this, notice for a closed pt of $Y$, the fiber is a $P^{r-1}$ because $I/I^2$ is locally free of rank $r$ by (5.10.1.16) and the functoriality of $\mathcal{O}(1)$.

3 Compatifications

Def.(5.8.3.1)[Compatifications]. Let $S \in \text{Sch}_{\text{qcqs}}$, $X \in \text{Sch}_{\text{sep}, \text{ft}}/S$, then the category of compatifications of $X/S$ is the category of pairs $(i, X)$, where $i: X \to X$ is an immersion and $X \to S$ is proper.

Thm.(5.8.3.2)[Nagata Compatification]. Situation as in (5.8.3.1), then $X/S$ has a compatification.

Proof: Cf.[Sta]0F41. □

4 Limits of Schemes

Prop.(5.8.4.1)[Noetherian Normalization]. Let $S$ be a qcqs scheme, then there exists a direct system $(S_i, f_{i'i})$ indexed over a set $I$ that

- $f_{i'i}$ are affine.
- $S_i$ are of f.t. over $\mathbb{Z}$.
- $S = \lim_i S_i$.

Proof: Cf.[Sta]01ZA. □

Prop.(5.8.4.2)[Characterizing Morphisms of F.P.]. Let $f : X \to S$ be a morphism of schemes, then the following are equivalent:

- $f$ is locally of finite presentation.
- For any directed inverse system $(T_i, f_{i'i})$ in $\text{Aff}_S$, we have

$$\text{Mor}_S(\lim_i T_i, X) = \lim_i \text{Mor}_S(T_i, X)$$
• For any directed inverse system \((T_i, f_{ii'})\) in \(\text{Sch}_S\) with \(T_i\) qcqs and \(f_{ii'}\) affine, we have

\[
\text{Mor}_S(\lim_{i} T_i, X) = \lim_{i} \text{Mor}_S(T_i, X)
\]

Proof: Cf.\cite[01IZC]{Sta}.

\textbf{Prop. (5.8.4.3) [Reduction to Finite Presented Morphisms].} Let \(f : X \to S\) be a morphism of schemes, if \(X\) is qcqs and \(S\) is qs, then \(X = \lim_{i} X_i\) is a limit of a directed system of schemes \(X_i\) of f.p. over \(S\) with affine morphisms over \(S\).

\[
\text{Mor}_S(\lim_{i} X_i, X) = \lim_{i} \text{Mor}_S(X_i, X)
\]

Proof: Cf.\cite[09MV]{Sta}.

\textbf{Prop. (5.8.4.4) [Integral and Finite].} Let \(f : X \to S\) be an integral morphism of schemes with \(S\) qcqs, then \(X = \lim_{i} X_i\) is a limit of a directed system of schemes \(X_i\) finite of f.p. over \(S\) with affine morphisms over \(S\).

Proof: Consider \(A = f_! \mathcal{O}_X\), which is a Qco sheaf of \(\mathcal{O}_S\)-modules. Then \(A = \lim_{i} A_i\) is a filtered colimit of finite and f.p. \(\mathcal{O}_S\)-modules by (5.5.1.13). Then \(X_i = \text{Spec}_S(A_i)\) satisfies the requirement by (5.2.7.12).

\section{5 \(D_{\mathcal{Q}\text{coh}}(X)\)}

\textbf{Def. (5.8.5.1) [Notations].} For a scheme \(X\),

Denote \(D^*_{\mathcal{Q}\text{coh}}(X) = D^*_{\mathcal{Q}\text{coh}}(X)(\text{Mod}(\mathcal{O}_X))(3.4.2.8)\). There is a natural functor \(D^*(\mathcal{Q}\text{coh}(X)) \to D^*_{\mathcal{Q}\text{coh}}(X)\).

Denote \(D^*_{\text{coh}}(X) = D^*_{\text{coh}}(X)(\text{Mod}(\mathcal{O}_X))(3.4.2.8)\). There is a natural functor \(D^*(\text{coh}(X)) \to D^*_{\text{coh}}(X)\).

By (5.3.1.6), these notions are affine local.

\textbf{Prop. (5.8.5.2) [Direct Sum].} Direct sum exists in \(D_{\mathcal{Q}\text{coh}}(X)\), and equals that in \(D(X)\).

Proof: By (3.4.2.15), direct sum exists in \(D(X)\) and are given by term-wise direct sums. Notice the direct sum of elements in \(D_{\mathcal{Q}\text{coh}}(X)\) is also in \(D_{\mathcal{Q}\text{coh}}(X)\) as direct sums are exact functor and \(\mathcal{Q}\text{coh}(X)\) is stable under direct sums.

\textbf{Prop. (5.8.5.3) [Affine Case].} Let \(X = \text{Spec} A\), there is a natural equivalence \(\sim : D(A) \to D(\mathcal{Q}\text{coh}(X))\). Then the functors \(R\Gamma(X, -) : D_{\mathcal{Q}\text{coh}}(X) \to D(A)\) is quasi-inverse to the inclusion functor \(D^*(\mathcal{Q}\text{coh}(X)) \to D^*_{\mathcal{Q}\text{coh}}(X)(5.8.5.1)\), and they are both isomorphism of triangulated categories.

Proof: Cf.\cite[06Z0]{Sta}.

\textbf{Prop. (5.8.5.4) [Derived Pullbacks].} Let \(f : X \to S\) be a qcqs morphism of schemes, then \(Lf^*\) maps \(D_{\mathcal{Q}\text{coh}}(X)\) into \(D_{\mathcal{Q}\text{coh}}(S)\), and affine locally it is just the derived tensor functor \(\bigotimes_A^L B : D(A) \to D(B)\) via identifications in (5.8.5.3), by (5.3.3.14)(5.3.3.15).

\textbf{Prop. (5.8.5.5) [Derived Products].} For \(X \in \text{Sch} \), \(D_{\mathcal{Q}\text{coh}}(X)\) is stable under derived tensor products, and affine locally it is just the derived tensor product \(\bigotimes^L\) via identifications in (5.8.5.3), by (5.3.3.6)(5.3.3.15).
Prop. (5.8.5.6) [Higher Direct Images]. Let \( f : X \to S \) be a qcqs morphism of schemes, then \( Rf_* \) maps \( D_{\text{QCoh}}(X) \) into \( D_{\text{QCoh}}(S) \). And if \( f \) is affine, affine locally it is just the restriction \( D(B) \to D(A) \) via identifications in (5.8.5.3), by (5.3.1.10).

Moreover, if \( S \) is qc, then there exists a \( N \in \mathbb{Z} \) s.t. \( Rf_*(D_{\text{QCoh}}^m(X)) \subset D_{\text{QCoh}}^{m+N}(S) \), and this \( N \) is invariant under base change.

**Proof:** Cf. [Sta]08D5. \( \square \)

Prop. (5.8.5.7). For \( f : X \to Y \) qcqs, \( Rf_* : D_{\text{QCoh}}(X) \to D_{\text{QCoh}}(Y) \) preserves direct sums.

**Proof:** Cf. [Sta]08DZ. \( \square \)

Prop. (5.8.5.8) [Projection Formula]. Let \( f : X \to Y \) be a qcqs morphism of schemes and \( E \in D_{\text{QCoh}}(X), K \in D_{\text{QCoh}}(Y) \), then the projection map (5.3.3.19)

\[
Rf_*(E) \otimes_{\mathcal{O}_Y} K \to Rf_*(E \otimes_{\mathcal{O}_Y} Lf^* K)
\]

is an isomorphism.

**Proof:** Cf. [Sta]08EU. \( \square \)

**Pseudo-Coherent and Perfect Complexes**

Prop. (5.8.5.9) [Affine Case]. If \( X = \text{Spec} A, M \in D(A) \) and \( E \) is the corresponding element in \( D(X) \), then

- \( E \) is an \((m)\)-pseudo-coherent object in \( D(X) \) iff \( M \) is an \((m)\)-pseudo-coherent object in \( D(A)(4.6.5.9) \).
- \( E \) has Tor-amplitude in \([a, b]\) iff \( M \) has Tor amplitude in \([a, b]\).
- \( E \) is a perfect object in \( D(X) \) iff \( M \) is a perfect object in \( D(A)(4.6.5.3) \).

**Proof:** Cf. [Sta]08E7, 08EB, 08E9,.

Prop. (5.8.5.10) [Noetherian Case]. Let \( X \) be a Noetherian scheme and \( \mathcal{E} \in D_{\text{QCoh}}(X) \), then the following are equivalent:

- \( \mathcal{E} \) is \( m \)-pseudo-coherent.
- \( \mathcal{E} \in D_{\text{QCoh}}^{-m}(X) \) and \( H^i(\mathcal{E}) \in \mathcal{Coh}(X) \) for \( i \geq m \).

In particular, \( E \) is pseudo-coherent iff \( E \in D_{\text{Coh}}^{-m}(X) \).

**Proof:** Cf. [Sta]08E8.

Prop. (5.8.5.11) [\( \mathcal{E} \text{xt} \)]. Let \( X \in \text{sch} \).

1. If \( X = \text{Spec} A \) and \( K, L \in D(A) \), then \( \mathcal{E}xt^n(\widetilde{K}, \widetilde{L}) \) is the sheaf extending the sheaf on the basis \( D(f) \mapsto \text{Ext}^n_A(K_f, L_f) \).
2. If \( X = \text{Spec} A \) and \( K, L \in D(A) \), then \( R\text{Hom}(\widetilde{K}, \widetilde{L}) = (R\text{Hom}_A(K, L))^\sim \) iff \( K \) is pseudo-coherent and \( L \in D_I(A) \), or \( K \) is perfect.
3. If \( \mathcal{L} \in D_{\text{QCoh}}(X) \) and \( K \in D(X) \) perfect, then \( R\text{Hom}(\mathcal{K}, \mathcal{L}) \in D_{\text{QCoh}}(X) \).
4. If \( \mathcal{L} \in D_{\text{QCoh}}^+(X) \) and \( K \in D(X) \) pseudo-coherent, \( R\text{Hom}(\mathcal{K}, \mathcal{L}) \in D_{\text{QCoh}}(X) \) and are locally bounded below.
Prop. (5.8.5.12) [Criterion for Relative Perfectness over Affine Base]. Let \( A \in \mathcal{C}_{\text{Alg}} \) and \( X \) be a separated, flat of f.p. scheme over \( A \), \( K \in D_{\mathcal{Qcoh}}(X) \). If \( R\Gamma(X,E \otimes^L K) \) is perfect in \( D(A) \) for any perfect object \( E \in D(X) \), then \( K \) is perfect over \( A \).

Proof: Cf. [Sta] 0GET.

\[ D_{\mathcal{Coh}}(X) \]

Prop. (5.8.5.13) [\( R\mathcal{H}om \) Preserves \( D_{\mathcal{Coh}}(X) \)]. If \( X \) is a locally Noetherian scheme and \( L \in D^+(\mathcal{Coh}(X)) \) and \( K \in D^-_{\mathcal{Coh}}(X) \), then \( R\mathcal{H}om(K,L) \in D^+_{\mathcal{Coh}}(X) \).

Proof: Cf. [Sta] 0D0C.

Prop. (5.8.5.14). Let \( X \) be a Noetherian scheme, then there are natural equivalences

\[ D^-(\mathcal{Coh}(X)) \cong D^-_{\mathcal{Coh}(X)}(\mathcal{Q}\mathcal{Coh}(X)) \cong D^-_{\mathcal{Coh}}(X), \quad D^b(\mathcal{Coh}(X)) \cong D^b_{\mathcal{Coh}}(X). \]

Proof: Cf. [Sta] 0FDA, 0FDB.

Prop. (5.8.5.15). Let \( S \) be Noetherian and \( f : X \to S \) be a proper morphism, then \( Rf_* \) maps \( D^b_{\mathcal{Coh}}(X) \) to \( D^b_{\mathcal{Coh}}(S) \).

Proof: Cf. [Sta] 08E2.

Prop. (5.8.5.16) [Perfect Complexes for Regular Schemes]. If \( X \) is a Noetherian regular scheme of finite dimension, then \( D^b_{\mathcal{Coh}}(X) \) consists exactly of the perfect objects in \( D(X) \), by (4.6.5.5) and (5.8.5.9).

Def. (5.8.5.17) [K-Groups of Schemes]. Let \( X \in \text{Sch} \), the Grothendieck group of \( X \) is defined to be \( K_0(X) = K_0(D_{\text{perf}}(X)) \). If \( X \) is locally Noetherian, also define the Grothendieck group of coherent sheaves on \( X \) to be \( K'_0(X) = K_0(\mathcal{Coh}(X)) \).

Prop. (5.8.5.18). If \( X \) is Noetherian, then

\[ K'_0(X) = K_0(\mathcal{Coh}(X)) = K_0(D^b(\mathcal{Coh}(X))) = K_0(D^b_{\mathcal{Coh}}(X)). \]

In particular, there is a map \( K_0(X) \to K'_0(X) \).

Proof: This follows from (3.4.2.13) and (5.8.5.14).

Prop. (5.8.5.19) \([K_0 \cong K'_0] \). If \( X \) is a Noetherian regular scheme of finite dimension, then the map \( K_0(X) \to K'_0(X) \) is an isomorphism, by (5.8.5.16).

Prop. (5.8.5.20). For \( X \in \text{Sch} \), \(- \otimes^L -\) defines a ring structure on \( K_0(X) \), by (3.4.1.30) and (3.4.4.12).
Prop. (5.8.5.21). If \( X = \text{Spec} R \), then \( K_0(X) = K_0(R) \). And if \( R \) is Noetherian, then \( K'_0(X) = K'_0(R) \).

Proof: Cf. [Sta] 0FDH.

Prop. (5.8.5.22) [Push and Pull]. Let \( f : X \to Y \) be a proper morphism of locally Noetherian schemes, then there is a map
\[
f_* : K'_0(X) \to K'_0(Y) : [\mathcal{F}] \mapsto \oplus_{i \geq 0} [R^{2i}f_*\mathcal{F}] - \oplus_{i \geq 0} [R^{2i+1}f_*\mathcal{F}],
\]
which is definable by (5.8.5.15). And there is an obvious map \( f^* : K'_0(Y) \to K'_0(X) \). They satisfy
\[
f_*(\alpha \cdot f^*\beta) = f_*\alpha \cdot \beta, \alpha \in K'_0(X), \beta \in K'_0(Y).
\]

Proof: The first assertion follows from long exact sequence for \( Rf_* \). The last assertion follows from projection formula (5.8.5.8).

Prop. (5.8.5.23) [Lambda Operators]. Let \( X \in \mathcal{S}ch \), there are functor \( \lambda^r : K_0(\mathcal{Coh}^{\text{free}}(X)) \to K_0(\mathcal{Coh}^{\text{free}}(X)) \) that sends \( [\mathcal{E}] \) to \( [\wedge^r \mathcal{E}] \).

Proof: Consider a map \( c : \mathcal{Coh}^{\text{free}}(X) \to K_0(\mathcal{Q Coh}^{\text{free}}(X))[t] : [\mathcal{E}] \mapsto \sum_{i=0}^{\infty} [\wedge^i \mathcal{E}] t^i \). It suffices to prove that for any exact sequence \( 0 \to \mathcal{E}' \to \mathcal{E} \to \mathcal{E}'' \to 0 \), \( c(\mathcal{E}) = c(\mathcal{E}') c(\mathcal{E}'') \), and then take \( \lambda^r \) as
\[
c(M) = \sum_{r>0} \lambda^r(M)t^r.
\]

To show this, notice that there is a filtration of \( \wedge^r \mathcal{E} \) with quotients
\[
\wedge^r \mathcal{E}', \wedge^{r-1} \mathcal{E}' \otimes \mathcal{E}'', \ldots, \wedge^r \mathcal{E}'',
\]
by (5.5.1.26).

Prop. (5.8.5.24) [Adam Operators]. Let \( X \in \mathcal{S}ch \), then there is are Adam operators
\[
\psi^{-1}, \psi^1, \psi^2 : K_0(X) \to K_0(X)
\]
s.t. for \( \mathcal{L} \in \text{Pic}(X) \),
\[
\psi^{-1}[\mathcal{L}] = [\mathcal{L}^{-1}], \quad \psi^1[\mathcal{L}] = [\mathcal{L}], \quad \psi^2[\mathcal{L}] = [\mathcal{L} \otimes^2].
\]

Proof: For any \( L \in K_0(X) \), there is an action of \( \{\pm 1\} \) on \( L \otimes^L L \) by switching factors. Denote \( (L \otimes^L L)^+, (L \otimes^L L)^- \) the fixed and anti-fixed parts of \( L \otimes^L L \), and define \( \psi^2[L] = [(L \otimes^L L)^+] - [(L \otimes^L L)^-] \).

Coherator

Prop. (5.8.5.25) [\( \mathcal{RQX} \)].

Prop. (5.8.5.26) [\( \mathcal{DQX} \)]. Let \( X \) be a qcqs scheme, then the inclusion functor \( D_{\mathcal{Q Coh}}(X) \to D(X) \) has a right adjoint, called the coherator, denoted by \( D_{\mathcal{Q} X} \).

Proof: Use (3.4.1.35). The conditions are satisfied as \( D_{\mathcal{Q Coh}}(X) \) is compactly generated and has direct sums that is preserved by inclusion by (5.8.5.30)(5.8.5.2).
Prop. (5.8.5.27). Let $f : X \to Y$ be a morphism of qcqs schemes, then

$$Rf_* \circ DQ_X = DQ_Y \circ Rf_* : D(X) \to D_{QCoh}(Y).$$

Proof: They are both right adjoint to $Lf^* : D_{QCoh}(Y) \to D(X)$, as $Lf^*$ maps $D_{QCoh}(Y)$ into $D_{QCoh}(X)$ (5.8.5.4).

Prop. (5.8.5.28) [Cohomological Boundedness of $DQ_X$]. Let $X$ be a qcqs scheme, then there exists $N \in \mathbb{Z}$ s.t. if $K \in D(X)$ satisfies $K|_U \in D^{[a,b]}(\mathcal{O}_U)$ for any affine open $U \subset X$, then $DQ_X(K) \in D^{[0, b+N]}_{QCoh}(X)$.

Proof: Cf. [Sta]0CSA.

Compact Generators

Prop. (5.8.5.29) [Perfect and Compact Objects]. Let $X$ be a qcqs scheme, then $K \in D(X)$ is perfect iff it is a compact object in $D_{QCoh}(X)$.


Prop. (5.8.5.30) [$D_{QCoh}(X)$ is Compactly Generated]. There is a perfect object $P \subset D_{QCoh}(X)$ that is a generator of $D_{QCoh}(X)$ (3.4.1.31).

Proof: Cf. [Sta]09IS.

Resolution Property

Def. (5.8.5.31) [Resolution Properties]. A scheme $X$ is said to have resolution property iff every $\mathcal{F} \in \mathcal{QCoh}^R(X)$ is a quotient of a locally free sheaf.

Prop. (5.8.5.32). If $X$ has an ample invertible sheaf, then $X$ has the resolution property by (5.5.4.5). In fact, every coherent sheaf is a quotient of a finite direct sum of $\mathcal{O}_X(−n)$.

Prop. (5.8.5.33) [Regular Scheme has Resolution property]. If $X$ is qc regular scheme with an affine diagonal, then $X$ has the resolution property, Cf. [Sta]0F8A? . Conversely, if $X$ is qcqs with the resolution property, then $X$ has affine diagonal. Cf. [Sta]0F8C.

Prop. (5.8.5.34) [Kleiman]. If $X$ is a qc irreducible and locally factorial scheme with affine diagonal map, then $X$ has the resolution property.

Proof: By (5.8.1.6), we have a basis of the form $X_s$ for $s \in \Gamma(X, \mathcal{L})$ for various invertible sheaves, then for any coherent sheaf, it is generated by f.m. sections in $\Gamma(U_i, \mathcal{F})$ and $U_i = X_s$ for $s \in \Gamma(X, \mathcal{L})$, and for each of them, we can use (5.5.3.5), we can extend these to global sections on $\Gamma(\mathcal{F} \otimes \mathcal{L}_s^n)$ for $n_i$ large. Then tensoring $\mathcal{L}_s^{-n_i}$, we find a $\oplus \mathcal{L}_s^{-n_i} \to \mathcal{F}$ surjective.

Prop. (5.8.5.35). When $X$ has the resolution property, $\mathcal{E}xt^*(-, \mathcal{G})$ is an universal $\delta$-functor for every $\mathcal{G} \in \mathcal{QCoh}(X)$, because locally free sheaf is adapted to $\mathcal{E}xt^*(-, \mathcal{G})$ by (5.3.3.25), so we can calculate $\mathcal{E}xt(\mathcal{F}, \mathcal{G})$ using a finite locally free resolution of $\mathcal{F}$.

Prop. (5.8.5.36). If $X$ is a qcqs scheme with the resolution property, then the map $K_0(\text{Vect}(X)) \to K_0(X)$ is an isomorphism.

Proof: Cf. [Sta]0FDJ.
6 Duality for Schemes

Main references are [Hartshorne Residues and Duality, Hartshorne], [Sta] Chap48 and [Grothendieck Duality and Base Change, Conrad]

Right Adjoints of Pushforwards

Prop. (5.8.6.1) [Right Adjoints of Pushforwards Exist]. Let \( f : X \to Y \) be a morphism between qcqs schemes, then the functor \( Rf_* : \mathcal{D}_{\text{qcqs}}(X) \to \mathcal{D}_{\text{qcqs}}(Y) \) has a right adjoint, denoted by \( f^! \).

Proof: Use (3.4.1.35). The conditions are satisfied as \( \mathcal{D}_{\text{qcqs}}(X) \) is compactly generated and has direct sums by (5.8.5.30)(5.8.5.2), and \( Rf_* \) preserves direct limits (5.8.5.7).

Prop. (5.8.6.2). Let \( f : X \to Y \) be a morphism between qcqs schemes, then \( f^! \) maps \( \mathcal{D}_{\text{qcqs}}^+(Y) \) into \( \mathcal{D}_{\text{qcqs}}^+(X) \).

Proof: This follows from the fact \( Rf_* \) has finite cohomological dimension \( N(5.8.5.6) \) and (3.4.2.18).

Prop. (5.8.6.3). Let \( f : X \to Y \) be a morphism of qcqs schemes, then for \( K \in \mathcal{D}_{\text{qcqs}}(X), L \in \mathcal{D}_{\text{qcqs}}(Y) \), there is a canonical map

\[
Rf_* R\mathcal{H}om_{\mathcal{O}_X}(L, f^! K) \to R\mathcal{H}om_{\mathcal{O}_Y}(Rf_* L, Rf_* f^! K) \to R\mathcal{H}om_{\mathcal{O}_Y}(Rf_* L, K),
\]

by (5.3.3.31) and adjunction.

Then this map becomes isomorphism after applying the coherator \( \mathcal{D}Q_X(5.8.5.26) \).

Proof: By Yoneda lemma, it suffices to show that for any \( M \in \mathcal{D}_{\text{qcqs}}(Y) \),

\[
\text{Hom}_Y(M, Rf_* R\mathcal{H}om_{\mathcal{O}_X}(L, f^! K)) \cong \text{Hom}_Y(M, R\mathcal{H}om_{\mathcal{O}_Y}(Rf_* L, K)) :
\]

\[
\text{Hom}_Y(M, Rf_* R\mathcal{H}om_{\mathcal{O}_X}(L, f^! K)) = \text{Hom}_X(Lf^* M, R\mathcal{H}om_{\mathcal{O}_X}(L, f^! K)) = \text{Hom}_X(Lf^* M \otimes L, f^! K)
\]

(by \( Lf^* M \otimes L \in \mathcal{D}_{\text{qcqs}}(X) \) by (5.8.5.4)(5.8.5.5)) = \text{Hom}_Y(Rf_*(Lf^* M \otimes L), K) = \text{Hom}_Y(M \otimes Rf_* L, K) = \text{Hom}_Y(M, R\mathcal{H}om_{\mathcal{O}_Y}(Rf_* L, K))

\( \square \)

Cor. (5.8.6.4). By (5.8.5.6), this adjointness is true without coherator if both \( R\mathcal{H}om_{\mathcal{O}_X}(L, f^! K) \) and \( R\mathcal{H}om_{\mathcal{O}_Y}(Rf_* L, K) \) are in \( \mathcal{D}_{\text{qcqs}}(Y) \). This is the case if \( L, Rf_* L \) are perfect or \( K \in \mathcal{D}_{\text{qcqs}}^+(Y) \) and and \( L, Rf_* L \) are pseudo-coherent, by (5.8.5.11).

In particular, this holds if \( f : X \to Y \) is a proper morphism of Noetherian schemes and \( L \in \mathcal{D}_{\text{qcqs}}^-(X) \) and \( S \in \mathcal{D}_{\text{qcqs}}^+(S) \), by (5.8.5.15) and (5.8.5.10).

Cor. (5.8.6.5) [Global Sections]. Let \( f : X \to Y \) be a morphism of qcqs schemes, then for \( K \in \mathcal{D}_{\text{qcqs}}(X), L \in \mathcal{D}_{\text{qcqs}}(Y) \), there is a canonical isomorphism

\[
R\mathcal{H}om_{\mathcal{O}_X}(L, f^! K) \to R\mathcal{H}om_{\mathcal{O}_Y}(Rf_* L, Rf_* f^! K) \to R\mathcal{H}om_{\mathcal{O}_Y}(Rf_* L, K)
\]
Proof: This is because for any \( E \in D(X) \), \( H^i(X, E) = \text{Ext}^i_{\mathcal{O}_X}(\mathcal{O}_X, E) = \text{Hom}(\mathcal{O}_X[-i], E) = \text{Hom}(\mathcal{O}_X[-i], D\mathcal{O}(E)) \) only depends on \( D\mathcal{O}(E) \).

\[ \square \]

**Prop. (5.8.6.6) [Proper Flat \( f^* \)].** Let \( f : X \to Y \) be a proper flat morphism of f.p. between qcqs schemes, then \( f^* \) is compatible with base change between qcqs schemes.

Proof: Cf. [Sta] 0AAB. \[ \square \]

**Upper Shriek**

**Def. (5.8.6.7) [\( \mathcal{S} \mathcal{C}_{S}^{f.t, \text{sep}} \)].** For a locally Noetherian scheme \( S \), let \( \mathcal{S} \mathcal{C}_{S}^{f.t, \text{sep}} \) be the full subcategory of \( \mathcal{S} \mathcal{C} / S \) consisting of schemes separated of f.t. over \( S \).

**Prop. (5.8.6.8) [Lower Shriek].** Let \( f : X \to Y \in \mathcal{S} \mathcal{C}_{S}^{f.t, \text{sep}} \), take a compactification \( \overline{f} : \overline{X} \to Y \) of \( X/Y \), then we can define the functor

\[
\overline{f}^! : D^+_{\text{QCoh}}(Y) \to D^+_{\text{QCoh}}(X) : f^! K = \overline{f}^!(K)|_X.
\]

and this functor is independent of the compactification chosen.

Proof: Cf. [Sta] 0AA0. \[ \square \]

**Prop. (5.8.6.9).** If \( f : X \to Y, g : Y \to Z \in \mathcal{S} \mathcal{C}_{S}^{f.t, \text{sep}} \), then there is a canonical isomorphism of functors \( (g \circ f)^! \cong f^! \circ g^! \).

Proof: Cf. [Sta] 0ATX. \[ \square \]

**Prop. (5.8.6.10) [Properties of \( f^! \)].** Let \( S \in \mathcal{S} \mathcal{C} \) be Noetherian, then for \( X, Y \in \mathcal{S} \mathcal{C}_{S}^{f.t, \text{sep}} \),

- If \( j : X \to Y \) is an open immersion, then \( j^! = j^* \).
- If \( i : X \to Y \) is a closed immersion, then \( i^! = R\mathcal{H}om(\mathcal{O}_X, -) \).
- \( f^! \) maps \( D^+_{\text{QCoh}}(Y) \) into \( D^+_{\text{QCoh}}(X) \).
- If \( f : X \to Y \) is a local complete intersection morphism, then \( f^! \mathcal{O}_Y \) is an invertible object of \( D(X) \), and \( f^! \) preserves perfect complexes.
- If \( f : X \to Y \) is finite, then \( f_* f^!(-) = R\mathcal{H}om_{\mathcal{O}_Y}(f_* \mathcal{O}_X, -) \).
- If \( f : X \to Y \) is an effective Cartier divisor, then \( f^!(-) = Lf^*(-) \otimes^L \mathcal{O}_X \wedge^c \mathcal{N}[-1] \).
- If \( f : X \to Y \) is a Koszul regular immersion of codimension \( c \), then \( f^!(-) = Lf^*(-) \otimes^L \Omega^d_{X/Y}[d] \).

Proof: Cf. [Sta] 0AU0, 0AA2, 0AU1, 0B6V, 0AU3? \[ \square \]

**Dualizing Complexes**

**Def. (5.8.6.11) [Dualizing Complex].** Let \( X \) be a locally Noetherian scheme, then a complex \( K \in D_{\text{QCoh}}(X) \) is called a **dualizing complex** if it satisfies the following equivalent conditions:

- For any affine open \( U = \text{Spec} \ A \subset X \), \( K|_U \) is a dualizing complex in \( D(A) \).
There exists an affine open covering \( U_i = \text{Spec} \ A_i \) of \( X \) s.t. \( K|U_i \) is a dualizing complex in \( D(A_i) \) for any \( i \).

Proof: This follows from (4.6.8.2).

**Prop. (5.8.6.12) [Dualizing]**. Let \( X \) be a locally Noetherian scheme and \( \omega_X \) be a dualizing complex, then \( D = R\text{Hom}_{\mathcal{O}_X}(-, \omega_X) \) is an anti-equivalence of \( D_{\text{QCoh}}(X) \) with itself, and there is a canonical isomorphism \( \text{id} \cong D^\otimes_2 \).

Moreover, if \( X \) is qc, then \( D \) exchanges \( D^+_{\text{QCoh}}(X) \) and \( D^-_{\text{QCoh}}(X) \), and induces an equivalence \( D : D^b_{\text{QCoh}}(X) \to D^b_{\text{QCoh}}(X) \).

Proof: Cf. [Sta]0A89.

**Thm. (5.8.6.13) [Grothendieck Duality]**. Let \( S \) be a Noetherian scheme, then

- \( f^! \) makes \( D^+_{\text{QCoh}} \) a pseudo-functor on \( \text{Sch}^\text{ft,sept}_S \).
- If \( f : X \to Y \in \text{Sch}^\text{ft,sept}_S \) is proper, then \( f^! \) is the right adjoint of \( Rf_* \), and there is a canonical isomorphism
  \[ Rf_* R\text{Hom}_{\mathcal{O}_X}(K, f^! M) \cong R\text{Hom}_{\mathcal{O}_Y}(Rf_* K, M) \]
  for any \( K \in D^-_{\text{coh}}(X) \) and \( M \in D^+_{\text{QCoh}}(Y) \), by ??
- If \( X \in \text{Sch}^\text{ft,sept}_S \) has a dualizing complex \( \omega_X \), then \( D_X = R\text{Hom}(-, \omega_X) \) defines an involution of \( D^\text{coh}_X \) switching \( D^+_{\text{coh}}(X) \) and \( D^-_{\text{coh}}(X) \) and fixing \( D^b_{\text{coh}}(X) \).
- If \( Y \) has a dualizing complex \( \omega_Y \), then
  
  - \( \omega_X = f^! \omega_Y \) is a dualizing complex for \( X \),
  
  - for \( M \in D^+_{\text{coh}}(Y) \), there is a canonical isomorphism \( D_X(f^! M) \cong Lf^* D_Y(M) \).
  
  - If moreover \( f \) is proper, then \( Rf_* R\text{Hom}_{\mathcal{O}_X}(K, \omega_X) = R\text{Hom}_{\mathcal{O}_Y}(Rf_* K, \omega_Y) \) for \( K \in D^-_{\text{coh}}(X) \).

Proof: Cf. [Sta]0AU3.

**Thm. (5.8.6.14) [Over a Dualizing Basis]**.

Proof: Cf. [Sta]0AUE.

**Dualizing Modules**

**Prop. (5.8.6.15) [Relative Dualizing Modules]**. Let \( f : X \to Y \) be a locally quasi-finite morphism of locally Noetherian schemes, then there exists a unique coherent \( \mathcal{O}_Y \)-module \( \omega_{X/Y} \in \text{Coh}(Y) \) that affine locally is given by the dualizing sheaf \( \omega_{B/A}(4.6.8.4) \).

Proof: Cf. [Sta]0BVG.

**Relative Dualizing Complex**

**Def. (5.8.6.16) [Relative Dualizing Complexes]**. For a separable f.t. morphism of Noetherian schemes \( f : X \to S \), the relative dualizing complex is defined to be \( \omega_{X/S} = f^! \mathcal{O}_S \).

**Prop. (5.8.6.17)**. Let \( Y \) be a qcqs scheme and \( f : X \to Y \) be a proper flat morphism of f.p., then

- \( \omega_{X/Y} \) is perfect over \( Y \).
Prop. (5.8.6.18)[Serre Duality (Proper over Fields case)]. Let \( X \) be a proper scheme over a field \( k \) of dimension \( d \), then there exists a unique dualizing complex \( \omega_X \) with the following properties:

- \( H^i(\omega_X) \neq 0 \) only for \( i \in \{ -\dim(X), 0 \} \).
- \( [\omega_X] = H^{-d}(\omega_X) \) is a coherent \((S_2)\)-module whose support is the irreducible components of \( X \) of dimension \( d \).
- \( \dim \text{Supp}(H^i(\omega_X)) \leq -i \).
- For \( x \in X \) closed, \( H^i(\omega_{X,x}) \oplus \cdots \oplus H^0(\omega_{X,x}) \neq 0 \) iff \( \text{depth}(\mathcal{O}_{X,x}) \leq -i \).
- For \( K \in D_{\text{QCoh}}(X) \), there is a functorial isomorphisms

\[
\text{Ext}^{-i}_X(K, \omega_X) \cong \text{Hom}_k(H^i(X, K), k)
\]

compatible with shifts and distinguished triangles, which characterizes \( \omega_X \) uniquely.

- There are functorial isomorphisms \( \text{Hom}(\mathcal{F}, [\omega_X]) = \text{Hom}_k(H^d(X, \mathcal{F}), k) \) for \( \mathcal{F} \in \text{Coh}(X) \).
- If \( X \) is C.M., equidimensional, then \( \omega_X = [\omega_X][d] \).
- If \( X \) is smooth over \( k \), then \( \omega_X = K_{X/k}[d] \).

**Proof:** As \( f^* \) commutes with base change \((5.8.6.6)\), it suffices to assume that \( Y = \text{Spec} A \).

1. By \((5.8.6.4)(5.3.4.23)\) and \((5.7.5.5)\), for any perfect object \( E \in D(X) \), there are canonical isomorphisms:

\[
Rf_*(E \otimes^L \omega_{X/Y}) = Rf_*R\mathcal{H}om_{\mathcal{O}_X}(E^\vee, \omega_{X/Y}) = R\mathcal{H}om_{\mathcal{O}_Y}(Rf_*E^\vee, \mathcal{O}_Y) = (Rf_*E^\vee)^\vee,
\]

which is perfect. So \( \omega_{X/Y} \) is perfect over \( S \) by \((5.8.5.12)\).

2. By \((5.8.5.8)\),

\[
\mathcal{H}om_Y(\mathcal{O}_Y[-i], Rf_*\omega_{X/Y}) = \mathcal{H}om_Y(Rf_*Lf^*\mathcal{O}_Y[-i], \mathcal{O}_Y) = \mathcal{H}om_Y((Rf_*\mathcal{O}_X)[-i], \mathcal{O}_Y).
\]

By proper flat base change \((5.7.5.5)\), \( Rf_*\mathcal{O}_X \) is perfect in \( Y \), so it can be represented by a finite complex of finite projective \( A \)-modules, so by \((5.3.4.22)\), \( R^if_*\omega_{X/Y} = 0 \) for \( i > 0 \).

3: For any perfect object \( E \in D(X) \), by \((5.8.6.4)(5.3.4.23)(5.7.5.5)(5.3.4.23)\) and \((5.3.1.10)\), there are canonical isomorphisms

\[
\mathcal{H}om_X(E, R\mathcal{H}om_{\mathcal{O}_X}(\omega_{X/Y}, \omega_{X/Y})) = \mathcal{H}om_Y(Rf_*(E \otimes^L \omega_{X/Y}), \mathcal{O}_Y)
\]

\[
= \mathcal{H}om_Y(Rf_*\mathcal{H}om(E^\vee, \omega_{X/Y}), \mathcal{O}_Y)
\]

\[
= \mathcal{H}om_Y(\mathcal{H}om(Rf_*E^\vee, \mathcal{O}_Y), \mathcal{O}_Y)
\]

\[
= R\Gamma(Y, Rf_*E^\vee)
\]

\[
= \mathcal{H}om_X(E, \mathcal{O}_X)
\]

So by \((5.8.5.30)\), perfect objects generate \( D_{\text{QCoh}}(X) \), so \( R\mathcal{H}om_{\mathcal{O}_X}(\omega_{X/Y}, \omega_{X/Y}) \cong \mathcal{O}_X \).

**Prop. (5.8.6.18)[Serre Duality (Proper over Fields case)]** Let \( X \) be a proper scheme over a field \( k \) of dimension \( d \), then there exists a unique dualizing complex \( \omega_X \) with the following properties:

- \( H^i(\omega_X) \neq 0 \) only for \( i \in \{ -\dim(X), 0 \} \).
- \( [\omega_X] = H^{-d}(\omega_X) \) is a coherent \((S_2)\)-module whose support is the irreducible components of \( X \) of dimension \( d \).
- \( \dim \text{Supp}(H^i(\omega_X)) \leq -i \).
- For \( x \in X \) closed, \( H^i(\omega_{X,x}) \oplus \cdots \oplus H^0(\omega_{X,x}) \neq 0 \) iff \( \text{depth}(\mathcal{O}_{X,x}) \leq -i \).
- For \( K \in D_{\text{QCoh}}(X) \), there is a functorial isomorphisms

\[
\text{Ext}^{-i}_X(K, \omega_X) \cong \text{Hom}_k(H^i(X, K), k)
\]

compatible with shifts and distinguished triangles, which characterizes \( \omega_X \) uniquely.

- There are functorial isomorphisms \( \text{Hom}(\mathcal{F}, [\omega_X]) = \text{Hom}_k(H^d(X, \mathcal{F}), k) \) for \( \mathcal{F} \in \text{Coh}(X) \).
- If \( X \) is C.M., equidimensional, then \( \omega_X = [\omega_X][d] \).
- If \( X \) is smooth over \( k \), then \( \omega_X = K_{X/k}[d] \).
Proof: Cf.[Sta]0FVV, 0AWT.? □

Cor. (5.8.6.19) [Serre Duality (Smooth over Fields case)]. If \( k \in \text{Field}, X \in \text{Sch}/k \) is a smooth proper scheme over \( k \) of dimension \( d \), then for any locally free sheaf \( \mathcal{F} \), there is a functorial isomorphism:
\[
H^i(X, \mathcal{F}) \cong (H^{n-i}(X, \mathcal{F}^\vee \otimes \mathcal{K}_{X/k}))^\vee.
\]

Cor. (5.8.6.20). For a smooth proper variety \( X \) over a field \( k \) of dimension \( n \), \( H^n(X, \mathcal{K}_X) = k \), by (5.10.1.12).

Cor. (5.8.6.21). For a smooth proper variety \( X \) over a field \( k \) of dimension \( n \), \( \Omega_{X/k}^n \) is locally free by (5.6.4.15), thus by (5.5.1.25), \( \Omega_{X/k}^{n-p} \cong (\Omega_{X/k}^p)^\vee \otimes \mathcal{K}_X \). So by (5.8.6.19):
\[
H^q(X, \Omega_{X/k}^p) \cong (H^{n-q}(X, \Omega_{X/k}^{n-p}))^\vee.
\]

Cor. (5.8.6.22). If \( X \) is a closed subscheme of \( P^n_k \) of codimension \( r \), then \( X \) has a dualizing sheaf \([\omega_X] = \text{Ext}^r_p(i_*\mathcal{O}_X, \mathcal{K}_{P^n/k}), \) and \( \text{Ext}^i(i_*\mathcal{O}_X, \mathcal{K}_{P^n/k}) = 0 \) for \( i < r \).

Proof: This follows from (5.8.6.18) and (5.8.6.13). □

Prop. (5.8.6.23) [Characterizing Cohen-Macaulay Schemes]. Let \( X \) be projective of dimension \( n \) over a field \( k \) and \([\omega_X]\) be the dualizing sheaf, then for \( \mathcal{F} \in \text{Coh}(X) \), there is a natural map
\[
\text{Ext}^i(\mathcal{F}, [\omega_X]) \to (H^{n-i}(X, \mathcal{F}))^\vee
\]
And the following are equivalent:
- For any \( \mathcal{F} \) locally free on \( X \), \( H^i(X, \mathcal{F}(-q)) = 0 \) for \( i < n \) and \( q \) large.
- \( H^i(X, \mathcal{O}_X(-q)) = 0 \) for \( i < n \) and \( q \) large.
- This is an isomorphism of \( \delta \)-functors.
- \( X \) is C.M. and equidimensional.

Proof: Notice the left side is an universal \( \delta \)-functor in \( \mathcal{F} \) by (5.8.5.35), so the map exist, and
2 \( \Rightarrow 3 \): This implies that the right is also universal by (5.8.5.32).
3 \( \Rightarrow 1 \): For \( \mathcal{F} \) locally free, by (5.3.3.33),
\[
H^i(X, \mathcal{F}(-q)) = (\text{Ext}^{n-i}(\mathcal{F}(-q), \omega_X)) = (H^{n-i}(X, \mathcal{F}^\vee \otimes \omega_X(q)))^\vee
\]
which is 0 for \( q \) large.
4 \( \Rightarrow 1 \): Embed \( X \) in \( P = P^N_k \), for \( \mathcal{F} \) locally free, since \( X \) is catenary, equidimensional is equivalent to \( \dim \mathcal{F}_x = n \) for all closed pt \( x \), and C.M. says depth \( \mathcal{F}_x = n \). Thus by (4.3.5.26), \( pd_{\mathcal{O}_{P,x}} \mathcal{F}_{x} = N - n \). Thus \( \text{Ext}^k_p(\mathcal{F}, -) \) vanish for \( k > N - n \) checked on stalks.
Now \( H^i(X, \mathcal{F}(-q)) \) is dual to \( \text{Ext}^{N-i}_p(\mathcal{F}, \omega_p(q)) \) by the proof of (5.8.6.22), which is isomorphic to \( \Gamma(P, \text{Ext}^{N-i}_p(\mathcal{F}(-q), \omega_p(q))) \) for \( q \) large by (5.7.4.9), so it vanish when \( i < n \) by what we proved.
1 \( \Rightarrow 4 \): The same as the proof of 4 \( \Rightarrow 1 \), then for \( i < n \),
\[
\Gamma(P, \text{Ext}^{N-i}_p(\mathcal{F}, \omega_p(q))) = 0 = \Gamma(P, \text{Ext}^{N-i}_p(\mathcal{F}, \omega_p)(q))
\]
for \( q \) large, so \( \text{Ext}^{N-i}_p(\mathcal{F}, \omega_p) = 0 \) as it is coherent. Then the stalk is \( \text{Ext}^{N-i}_{\mathcal{O}_{P,x}}(\mathcal{O}_{X,x}, \mathcal{O}_{P,x}) \), so \( pd_{\mathcal{O}_{P,x}} \mathcal{F}_{x} \leq N - n \) by (4.3.5.27), so depth \( \mathcal{O}_{X,x} \geq n \), we must have equality, thus \( X \) is C.M. and equidimensional, as it suffice to check at closed pts. □
Cor. (5.8.6.24) [Enriques-Severi-Zariski]. Let $X$ be a normal projective scheme that every irreducible component has dimension $\geq 2$, then for any $\mathcal{F} \in \text{Vect}(X)$, $H^1(X, \mathcal{F}(-q)) = 0$ for $q$ large. 

Proof: Just notice that $\dim \mathcal{F}_x \geq 2$, and Serre criterion shows depth $\mathcal{F}_x \geq 2$, the rest is the same as $4 \to 1$ in the proof of (5.8.6.23).

Prop. (5.8.6.25) [Ample Effective Divisor Connected]. Let $X$ be a proper connected CM. equidimensional scheme over $k$ of dimension at least 2 and $D$ is an ample effective Cartier divisor, then $D$ is connected.

In particular, if $X$ is a smooth complete variety of dimension $\geq 2$, $D$ is also a complete variety. 

Proof: Let $D = V(s)$, where $s$ is a section of an ample invertible sheaf, then there is an exact sequence 

$$0 \to \mathcal{O}_X(-nD) \to \mathcal{O}_X \to i_*\mathcal{O}_{V(s^n)} \to 0,$$

which gives a long exact sequence 

$$0 \to H^0(X, \mathcal{O}_X(-nD)) \to H^0(X, \mathcal{O}_X) \to H^0(V(s^n), \mathcal{O}_{V(s^n)}) \to H^1(X, \mathcal{O}_X(-nD)).$$

But by Serre duality (5.8.6.19) and (5.7.2.6), $H^0(X, \mathcal{O}_X(-nD)) = H^{\dim X}(X, [\omega_X] \otimes \mathcal{O}_X(nD)) = 0$ for $n$ sufficiently large, and $H^1(X, \mathcal{O}_X(-nD)) = H^{\dim X-1}(X, [\omega_X] \otimes \mathcal{O}_X(nD)) = 0$ for $n$ sufficiently large, so $H^0(V(s^n), \mathcal{O}_{V(s^n)}) \cong H^0(X, \mathcal{O}_X)$ has no idempotents for $n$ sufficiently large, so $V(s^n)$ is connected, and $D$ is also connected. 

Cor. (5.8.6.26). Any global complete intersection in $\mathbb{P}^n$ is connected.

Topological Sheaves

Prop. (5.8.6.27) [Global Verdier Duality]. If $f : X \to Y$ is a map between locally compact spaces with finite dimension, then there exists a functor $f^! : D^+(S\text{Ab}_Y) \to D^+(S\text{Ab}_X)$ that 

$$R\text{Hom}(Rf_*\mathcal{F}^*, G^*) \cong R\text{Hom}(\mathcal{F}, f^!G^*).$$

In particular, $f^!$ is right adjoint to $Rf_!$. Cf. [Gelfand P228].

There is also a local form of Verdier duality, which implies the global version by taking global section, Cf. [Cohomology of Sheaves Iversen P330].

Prop. (5.8.6.28). When $X \to Y$ is an inclusion of open subset, $f_!$ is just $j_!$ defined in (5.2.6.2) and $f^!$ is the restriction. When it is an inclusion of closed subset of locally compact spaces, it is the direct image $f_*$ and $f^!$ is the $j^!$ previously defined in (5.2.6.2). They are not barely defined on $D^+(S\text{Ab})$ but on $S\text{Ab}$.

Prop. (5.8.6.29). We consider the case where $f : X \to \text{pt}$, and let $G = \mathbb{Z}$, denote $f^!(\mathbb{Z})$ by $\mathcal{D}^X_\bullet$, called the dualizing complex, then there is a duality: 

$$R\text{Hom}(R\Gamma_c(X, \mathcal{F}^*), \mathbb{Z}) \cong R\text{Hom}(\mathcal{F}^*, \mathcal{D}^X_\bullet).$$

for $\mathcal{F}^* \in D^+(\text{Sh}(X))$. 
Prop. (5.8.6.30). When $X$ is a $n$ dimensional topological manifold with boundary, then $D^n_X = \omega_X[n]$, where the sheaf $\omega_X$ is defined by
$$\Gamma(U, \omega_X) = \text{Hom}_{\text{Ab}}(H^n_c(U, \mathbb{Z}), \mathbb{Z}).$$

Cf.[Gelfand P234]. If we replace $\mathbb{Z}$ by a field $k$, then $w_X$ is the sheaf of $k$-orientations of $\text{int}(X)$, thus the constant sheaf when $X$ is oriented or $\text{char} k = 2$.

In particular, place $k$ in dimension $i$ then we get an isomorphism
$$\text{Hom}_k(H^i_c(X, \mathcal{F}), k) = \text{Ext}^{n-i}(\mathcal{F}, \omega_X)$$
(because $k$ is a field thus injective). Gelfand even gives an interpretation of this pair in [Gelfand P236].

And if $\mathcal{F} = \omega_X$ and $X$ oriented or $\text{char} k = 2$, we have $\text{Ext}^{n-i}(k_X, k_X[n]) = H^{n-i}(X, k_X)$ using the adjointness of constant sheaf, so we get the Poincare duality:
$$H^i_c(X, k_X)^\vee \cong H^{n-i}(X, k_X).$$

Prop. (5.8.6.31). Compact cohomology commute with colimits, Cf.[Cohomology of Sheaves Iversen P173].

7 Discriminant and Different

Trace Elements

Def. (5.8.7.1) [Traces]. Let $f : X \to Y$ be a finite locally free morphism, the trace of $f$ is defined to be
$$\text{tr}_f : f_* \mathcal{O}_X \to \mathcal{O}_Y.$$

Then $\text{tr}_f \circ f^\# = [\text{deg}(f)] : \mathcal{O}_Y \to \mathcal{O}_Y$. Let the trace pairing be
$$Q_f : f_* \mathcal{O}_X \otimes f_* \mathcal{O}_X \to \mathcal{O}_Y : (s, t) \mapsto \text{tr}_f(st)$$
which is equivalent to a map $Q_f : f_* \mathcal{O}_X \to f_* \mathcal{O}_X^\vee$, so the determinant of which is
$$\det(Q_f) : \wedge(f_* \mathcal{O}_X) \to \wedge(f_* \mathcal{O}_X)^{-1},$$
a section of the line bundle $\wedge(f_* \mathcal{O}_X)^{-2}$. Then the discriminant of $f$ is defined to be the closed subscheme $D_f$ of $Y$ cut out by this section $\det(Q_f)$.

Def. (5.8.7.2) [Trace Element of Rings]. Let $A \to B$ be a flat quasi-finite map of Noetherian rings, $[\omega_B/A]$ the dualizing module (4.6.8.4), then there exists a unique element $\tau_{A/B} \in \omega_B/A$ s.t. for any Noetherian $A$-algebra $A_1$ s.t. $B \otimes_A A_1 = C \times D$ with $C$ finite over $A_1$, the image of $\tau_{B/A}$ in $[\omega_{C/A_1}]$ is $\text{tr}_{C/A}$, called the trace element.

Def. (5.8.7.3) [Trace Element of Morphisms]. Let $f : X \to Y$ be a flat quasi-finite morphism of locally Noetherian schemes, then denote $\tau_{X/Y} \in \Gamma(X, [\omega_{X/Y}])$ the trace element of $f$ affine locally given by the trace element $\tau_{B/A}(5.8.7.2)$.

Prop. (5.8.7.4) [Discriminant and ÉtaleLocus]. If $f : X \to Y$ is finite locally free, then $f$ is étale iff $D_f = \emptyset$.

Proof: $f$ is flat, so it suffices to check fiberwise. Then this follows from (4.4.7.21). □
**Differents**

**Def.(5.8.7.5) [Kähler Different].** Let \( f : X \to Y \) be a morphism of schemes locally of f.t., the **Kähler different** of \( f \) is the 0-th fitting ideal \( \text{Fit}_0(\Omega_{X/Y}) \in \mathcal{O}_{\text{Coh}}(X) \).

**Prop.(5.8.7.6).** Let \( f : X \to Y \) be a morphism of schemes locally of f.t., then the closed subscheme cut out by the Kähler different is stable under base change.

**Proof:** Cf.[Sta]0BVX.

**Prop.(5.8.7.7).** If \( X = \text{Spec } A[X_1,\ldots,X_n]/(f_1,\ldots,f_m) \), then the Kähler different of \( X \to \text{Spec } A \) is just the ideal generated by the Jacobians \( \det(\frac{\partial f_i(j)}{\partial X_j})_{0 \leq j \leq n} \).

**Proof:** Because \( \Omega_{X/A} \) has a presentation

\[
0 \to \bigoplus_{0 \leq i \leq m} f_i \overset{d}{\to} \bigoplus_{0 \leq j \leq n} dX_j \to \Omega_{X/A} \to 0.
\]

**Prop.(5.8.7.8) [Kähler Different and Unramified Locus].** Let \( f : X \to Y \) be a morphism of schemes locally of f.t., then the closed subscheme cut out by the Kähler different contains exactly the points that \( f \) is not unramified.

**Proof:** Cf.[Sta]0C3J.

**Def.(5.8.7.9)[Differents].** Let \( f : X \to Y \) be a flat quasi-finite morphism between locally Noetherian schemes, define the **different** of \( f \) to be the annihilator of \( [\omega_{X/Y}]/\tau_{X/Y} \), which is a coherent ideal \( \mathcal{D}_f \subset \mathcal{O}_X \).

**Prop.(5.8.7.10)[Differents and Étale(Unramified) Locus].** Let \( f : X \to Y \) be a flat quasi-finite morphism between locally Noetherian schemes, then the closed subscheme of \( X \) cut out by the different \( \mathcal{D}_f \) contains exactly the set of points that \( f \) is not étale(unramified).

**Proof:** Cf.[Sta]0BW9.

**Prop.(5.8.7.11).** If \( f : X \to Y \) is a quasi-finite syntomic morphism between locally Noetherian schemes, then the different \( \mathcal{D}_f \) equals the Kähler different of \( f \).

**Proof:** Cf.[Sta]0BWG.

**Prop.(5.8.7.12) [Differents for Smooth Schemes].** Let \( S \) be a locally Noetherian scheme and \( X,Y \) be smooth scheme of relative dimension \( n \) over \( S \), and \( f : X \to Y \) is a quasi-finite morphism, then \( f \) is syntomic, and the closed subscheme \( R \) cut out by the different \( \mathcal{D}_f \) of \( f \) is the locally principal vanishing locus of

\[
\wedge^n(df^*) \in \text{Hom}(f^*\Omega^n_{Y/S},\Omega^n_{X/S}) = \Gamma(Y, (f^*\Omega^n_{Y/S})^{-1} \otimes \Omega^n_{X/S}).
\]

And if \( f \) is étale at the associated points of \( X \), then \( R \) is an effective Cartier divisor, and

\[
f^*\Omega^n_{Y/S} \otimes \mathcal{O}(R) \cong \Omega^n_{X/S}.
\]

**Proof:** Cf.[Sta]0BWJ.
8 Fourier-Mukai Transform

Cf. [Sta] Chap 56.

9 Deformation Theory

Basic references are [Sta] Chap 36.

Def. (5.8.9.1) [Thickenings]. We call $X'$ a thickening of a $X$ iff $X$ is a closed subscheme of $X'$ that their underlying topological space are the same. Morphisms of thickenings are defined routinely.

A thickening is said to have order $n$ iff the ideal sheaf $\mathcal{I}$ satisfies $\mathcal{I}^{n+1} = 0$.

Base change and composition of a (order $n$)thickening is also a (order $n$)thickening, because closed immersion and surjective do.

Prop. (5.8.9.2). Any thickening of an affine scheme is also affine.

Proof: This is a special case of (5.4.4.36).

Prop. (5.8.9.3) [Picard Group of Thickenings]. Let $X \subset X'$ be a first order thickening with ideal sheaf $\mathcal{I}$, then there is a canonical long exact sequence of Abelian groups:

\[
0 \to H^0(X, \mathcal{I}) \to H^0(X', \mathcal{O}_{X'}) \to H^0(X, \mathcal{O}_X^*) \to H^1(X, \mathcal{I}) \to \text{Pic}(X') \to \text{Pic}(X) \to H^2(X, \mathcal{I}) \to \ldots
\]

Proof: This follows from taking cohomology of the exact sequence $0 \to \mathcal{I} \to \mathcal{O}_{X'} \to i_*\mathcal{O}_X \to 0$, where $\mathcal{I} \to \mathcal{O}_{X'}$ is given by $a \mapsto 1 + a$. \hfill $\square$

Prop. (5.8.9.4). Let $X \subset X'$ be a thickening with ideal sheaf $\mathcal{I}$ and $n$ is invertible in $\mathcal{O}_X$, then $\text{Pic}(X)[n] \to \text{Pic}(X')[n]$ is an isomorphism.

Proof: By taking cohomology of the exact sequence $0 \to (1 + \mathcal{I})^* \to \mathcal{O}_{X'} \to i_*\mathcal{O}_X \to 0$, it suffices to show that $n : (1 + \mathcal{I})^* \to (1 + \mathcal{I})^*$ is an isomorphism, which is true by (4.1.1.17). \hfill $\square$

Def. (5.8.9.5) [Infinitesimal Neighbourhood]. Let $Z \subset U \subset X$ be a closed immersion of the open subscheme $U$ that $Z$ corresponds to the ideal $\mathcal{I}$ on $U$, then a $n$-th infinitesimal neighbourhood of $Z$ in $X$ is the closed subscheme of $U$ corresponding to $\mathcal{I}^n$.

The infinitesimal neighbourhood of $Z$ in $X$ has the universal property s.t. for any infinitesimal thickening $T \subset T'$ of order $n$ over $X$ and a map $T \to Z \in \text{Sch}_X$ extension to a morphism of infinitesimal thickenings ($T \subset T'$) \to ($Z \to Z'$) over $X$.

Def. (5.8.9.6) [Infinitesimal Extension]. Let $X$ be a scheme algebraic over a field $k$ and $\mathcal{F}$ is a coherent sheaf on $X$, then a infinitesimal extension of $X$ by the sheaf $\mathcal{F}$ is a scheme $X'$ over $k$ that has a sheaf of ideals $\mathcal{I}$ that $\mathcal{I}^2 = 0$ and $(X', \mathcal{O}_{X'}/\mathcal{I}) \cong (X, \mathcal{O}_X)$, and moreover, $\mathcal{I}$ with the $\mathcal{O}_X$-structure is isomorphic to $\mathcal{F}$.

There is a trivial extension, that is $(X', \mathcal{O}_{X'}) \cong (X, \mathcal{O}_X \oplus \mathcal{F})$, where the multiplication is $(a, f)(a', f') = (aa', af' + a'f)$.

Def. (5.8.9.7) [Deformation]. Let $X$ be a scheme algebraic over a field $k$, an infinitesimal deformation of $X$ is a scheme $X'$ flat over $D = k[t]/(t^2)$ that $X' \otimes_D k = X$. An infinitesimal deformation is a first order thickening, by (5.8.9.1).

If $Y$ is a closed subscheme of $X$, then we define the infinitesimal deformation of $Y$ in $X$ to be a closed subscheme $Y' \subset X \otimes_D D$ which is flat over $D$ and $Y' \otimes_D k = Y$.

A scheme algebraic over a field $k$ is called rigid if it has no infinitesimal deformations.
Prop.(5.8.9.8) [Affine Case]. Any thickening of an affine scheme is affine. (Immediate from (5.4.4.36)).

Prop.(5.8.9.9). Let $X$ be a nonsingular variety over an alg.closed field $k$, infinitesimal deformation of $X$ is the same as an infinitesimal extension of $X$ by the sheaf $\mathcal{O}_X$. Thus we get the set of infinitesimal deformations of $X$ is parametrized by $H^1(X, T_X)$, by (5.8.9.11) below.

Proof: For an infinitesimal deformation, tensoring $\mathcal{O}_X'$ with the exact sequence $0 \to k \xrightarrow{\iota} D \to k \to 0$, we get (by flatness)

$0 \to \mathcal{O}_X \xrightarrow{\iota} \mathcal{O}_X' \to \mathcal{O}_X \to 0$,

and conversely, an extension is locally free (because it is f.g. so flat over $D$ is equivalent to free).

Prop.(5.8.9.10). If $X$ is an affine regular scheme algebraic over an alg.closed field $k$, then any extension by coherent sheaf is trivial.

Proof: For any infinitesimal extension, the morphism $X \to X'$ is a closed immersion and surjection, so $X'$ is also affine by (5.8.9.8), = Spec $A'$. Now the rest follows from??.

Cor.(5.8.9.11) [Infinitesimal Extension and Cohomology]. Let $X$ be a nonsingular variety over an alg.closed field $k$, then the set of infinitesimal extensions by a coherent sheaf $F$ is parametrized by $H^1(X, F \otimes T_X)$.

If $Y$ is a closed subscheme of $X$, then the set of infinitesimal deformation of $Y$ in $X$ is parametrized by $H^0(Y, N_{Y/X})$.

Proof: By the proposition, we know that an infinitesimal extension is locally isomorphic to $(U, \mathcal{O}_X(U) \otimes F(U))$, by a section $F(U) \to \mathcal{O}_X(U)$.

But there is a twist, because there can because different sections. But the different sections different at a $\text{Hom}_{\mathcal{O}_X(U)}(\Omega_{\mathcal{O}_X(U)/k}, F(U)) = (T \otimes F)(U)$. These forms a Čech cocycle for $F \otimes T_X$, and the converse is also true. Finally, use the fact that $X$ is separated so Čech and sheaf cohomology coincide.

For the subscheme, ?

Formal Properties

Def.(5.8.9.12) [Formal Properties]. Let $f : X \to S$ be a morphism of schemes, then $f$ is called a formally unramified/smooth/étale if for any first order thickening of affine schemes $T \to T'$ and a morphism $(T \to T') \to (X \to S)$, there exists at most one/exists one/exists exactly one lifting $T' \to X$.

Formally unramified/smooth/étale morphisms are stable under base change and compositions.

Prop.(5.8.9.13).  
- A morphism is (G-)unramified iff it is formally unramified and locally of f.t.(f.p.).
- A morphism is étaleiff it is formally étale and locally of f.p.
- A morphism is smooth it is formally smooth and locally of f.p.

Proof: [Sta]
5.9 Resolution of Singularities

References are [K-M85].

Def. (5.9.0.1) [Desingularizations]. Let $X \in \text{Sch}$ be reduced and locally Noetherian, then a desingularization of $X$ is a modification (5.4.5.10) $Z \to X$ s.t. $Z$ is regular. A strong desingularization is a desingularization $\pi : Z \to X$ that $\pi$ is an isomorphism over any regular point $x \in X$.

Thm. (5.9.0.2) [Hironaka]. Let $X$ be a reduced scheme locally of f.t. over an excellent, reduced, locally Noetherian scheme of characteristic 0 (i.e. $\text{char} \kappa(x) = 0$ for any $x \in X$), then $X$ admits a strong desingularization over $S$.


Thm. (5.9.0.3) [de Jong]. Let $R$ be a CDVR or a field, $X \in \text{Sch}_{\text{int}}^{\text{ft,sep}} / R$, then $X$ admits an alteration $Y \to X$ over $R$ s.t. $Y$ is integral.

5.10 Varieties

Basic references are [Sta] and [Har77].

The materials distinguishes here in the fact that most schemes considered have geo.reduced, geo.connected or geo.integral properties in nature.

1 Varieties

Classical varieties

Prop. (5.10.1.1) [Soberization Functor]. For a sep.closed field \( k \), the soberization functor \( t \) induce a fully faithful functor from classical varieties over \( k \) to quasi-projective integral schemes over \( k \). It maps projective varieties to projective integral schemes and preserves fiber products ?.

Proof: We assign the irreducible closed subsets space \( t(X) \) and show that this embeds \( X \) in \( t(X) \), and for an affine variety \( (V, \mathcal{O}_V) \), the regular function sheaf is isomorphic to the pullback sheaf on \( t(V) = \text{Spec}(A) \).

By definition \( t(X) \) is quasi-projective, which is separated, the set of geometric pts of any closed variety is dense so \( t(V) \) is homeomorphic to \( X \). And because they are both reduced, they are isomorphic. So it is essentially surjective.

It is fully faithful by (5.10.1.11).

Prop. (5.10.1.2). The soberization of a classical variety \( X \) is regular at a closed point iff the local defining functions has rank \( n - \dim X \).

Proof: Consider the space of closed point of \( X \), they correspond to classical points because \( k \) is alg.closed. Let \( a_p = (x_1 - a_1, \ldots, x_n - a_n) \) and \( b \) be the locally defining ideal. Then the differential defines an isomorphism of vector space \( a_p/a_p^2 \cong k^n \), and the local ring at \( p \) is \( m/m^2 \cong (a_p/b)/(a_p/b)^2 \cong a_p/(b + a_p^2) \). The rank of the defining functions is \( b + a_p^2/a_p^2 \). Counting dimension gives us the result. (Use (5.6.3.3) also).

Varieties

Def. (5.10.1.3) [Varieties]. A variety is a geo.integral separated scheme algebraic over a field \( k \). An prevariety is an integral separated scheme algebraic over a field \( k \). A complete variety is a variety that is also proper(i.e. universally closed). The category of varieties over \( k \) is denoted by \( \mathcal{V} \text{ar}_k \).

A classical variety is an abstract variety because quasi-projective is f.t. and separated (5.4.5.19).

A non-singular variety is a regular variety.

A curve over \( k \) is a variety of dimension 1.

If \( X \) is a (complete)variety over \( k \) and \( K/k \) is a field extension, then \( A_K \) is a (complete)variety over \( K \), by (5.4.3.17).

Remark (5.10.1.4). Notice the prevariety is the same as the variety defined in [Sta].

Cor. (5.10.1.5). Any variety is birational to an integral H-quasi-projective scheme. A complete variety is birational to an integral projective scheme by Chow’s lemma (5.4.5.23)(5.4.5.3).
**Prop. (5.10.1.6).** By valuation criterion, for a complete variety, every valuation of the function fields of $K/k$ dominate a unique point of $X$. So the points of $X$ correspond to valuations of $K$ containing $k$.

**Prop. (5.10.1.7) [Generically Smoothness].** A variety is generically smooth, by (5.6.4.21).

**Prop. (5.10.1.8) [Nagata].** By Nagata compactification (5.8.3.2), any variety can be embedded as an open subset of a complete variety.

**Proof:**

**Prop. (5.10.1.9) [Product of Varieties].** The product of two (complete) varieties over $k$ is also a (complete) variety.

**Proof:** It is geometrically integral by (5.4.3.17), it is separated because separatedness is stable under composition and base change (5.4.4.2). So does properness.

**Def. (5.10.1.10) [Arithmetic Points].** An arithmetic point of a scheme $X$ over a field $k$ is an element of $X(k_s)$. When $X$ is a variety, the arithmetic points of $X$ is dense in $X$, by (5.4.3.3).

An geometric point of a scheme $X$ is an element of $X(k)$.

**Prop. (5.10.1.11).** To verify two morphisms $f, g$ between two varieties $X$ and $Y$ are equal, it suffices to prove that they are equal on the set of arithmetic points of an open subscheme $U$ (5.10.1.10).

**Proof:** Because the equalizer is a closed subscheme of $X$ (5.2.7.18), and it contains all geometric pts of an open subset of $X$, so it must by $X$, as the geometric-points are dense in $U$ (5.10.1.10), and $X$ is reduced and irreducible.

**Prop. (5.10.1.12) [Global Sections].** Let $X$ be a proper scheme over a field $k$, then

- $A = H^0(X, \mathcal{O}_X)$ is a finite $k$-algebra hence is a finite product of Artinian local $k$-algebras, one for each connected component of $X$.
- If $X$ is reduced, then $A = \prod k_i$ is a finite product of finite field extensions of $k$.
- If $X$ is geo.reduced, then $k_i$ are all separable over $k$.
- If $X$ is geo.connected, then $A$ is geo.irreducible over $k$ (4.3.6.1).
- If $X$ is geo.integral (i.e. a complete variety), then $\Gamma(X, \mathcal{O}_X) = k$.

**Proof:**

1: $H^0(X, \mathcal{O}_X)$ is finite $k$-algebra by (5.7.4.11), thus it is Artinian (4.1.3.4). The connected components of $X$ clearly corresponds to idempotents of $A$, which corresponds to Artinian local $k$-algebras, as a local ring is connected.

2: This follows from (4.1.3.5).

3: $A \otimes_k \overline{k} = H^0(X_{\overline{k}}, \mathcal{O}_{X_{\overline{k}}})$ is also reduced by flat base change (5.7.5.1), so each $k'/k$ is geo.reduced (4.3.6.2), thus separable by (4.3.9.4).

4: By hypothesis $A \otimes_k \overline{k} = H^0(X_{\overline{k}}, \mathcal{O}_{X_{\overline{k}}})$ is an Artinian local ring, thus it has only one point, so irreducible, so it is geo.irreducible (4.3.6.3).

5: By item3, 4, $A = k'$ is a finite separable field extension of $k$ that $\text{Spec}(k' \otimes_k \overline{k})$ is irreducible, but $k' \otimes_k \overline{k}$ is a finite product of $\overline{k}$, thus $k' = k$. 

□
Prop.(5.10.1.13) [Check Properties on Geometric/Closed Points]. A nice property of varieties is that identity of two morphisms of products of varieties can be checked at the geometric pts(5.10.1.10), by(5.10.1.11) and(5.10.1.9).

Surjectiveness of a map between varieties can be checked on closed points, by(5.4.1.29).

Also surjective and injective of Qco sheaves need only be checked at closed pts by(5.5.1.38)(5.4.1.26).

Canonical Sheaves

Prop.(5.10.1.14)[Canonical Sheaves]. For a smooth variety $X$ over a field $k$ and $Y$ a local complete intersection of $X$ of codimension $r$, by(5.6.4.2) and(5.6.4.16) and(5.6.8.10), $\mathcal{K}_{X/k}$ and $I/I^2$ is locally free, so we can define the following locally free sheaves:

- The canonical sheaf $\mathcal{K}_{X/k} = \wedge^n \Omega_{X/k}$ on $X$.
- The tangent sheaf $\mathcal{T}_X = (\mathcal{K}_{X/k})^{-1}$ on $X$.
- The conormal sheaf $\mathcal{C}_{Y/X} = I/I^2$ on $Y$.
- The normal sheaf $\mathcal{N}_{Y/X} = \mathcal{C}_{Y/X}^{-1}$ on $Y$.

Prop.(5.10.1.15) [Kodaira-Spencer map]. There is another characterization of tangent vector fields. (Note: this should be a special case of Prop8.5.9 in [FGA]). Let $X$ be a variety over $k$ and $S = k[\varepsilon]$ the dual numbers. Then $H^0(X, \mathcal{T}_X) \cong \text{Aut}^{(1)}(X_S/S)$, where $\text{Aut}^{(1)}(X_S/S)$ means that the automorphisms of $X_S$ over $S$ that is identity on $X$ (inclusion to $X_S$ induced by $\text{Spec} k \subset \text{Spec} S$).

Proof: First the case $X = \text{Spec} A$ is affine, then because $H^0(X, \mathcal{T}_X) = \text{Hom}_k(\mathcal{K}_{A/k}, A) = \text{Der}(A, A)$, so this is equivalent to $\text{Der}(A, A) \cong \text{automorphisms of } A[\varepsilon]$ that is identity under pass to quotients to $A$. For this, a $d \in \text{Der}(A, A)$ is mapped to $a + b\varepsilon \mapsto a + b\varepsilon + d(a)\varepsilon$. This is checked to be a ring morphism, and any desired morphism are like these.

The above construction is natural and functorial in $A$, so it glue together to give the global case.

□

Prop.(5.10.1.16) [Smoothness and Conormal Sheaves]. Let $X$ be a smooth variety over a field $k$, then an irreducible closed subscheme $Y$ of codimension $r$ in $X$ is smooth iff $\mathcal{K}_{Y/k}$ is locally free and(5.5.5.13) is exact on the left.

In this case, $I$ is locally generated by $r$ elements and $\mathcal{C}_{Y/X}$ is a locally free sheaf of rank $r$ on $Y$ by(5.6.8.10).

Proof: Cf.[Hartshorne P178]. Should has something to do with(5.6.4.2),(5.6.4.16) and(5.6.4.15).

□

Prop.(5.10.1.17) [Adjunction Formulas]. For a smooth variety $X$ over a field $k$ and $Y$ a smooth subvariety of codimension $r$. There is an exact sequence

$$0 \to I/I^2 \to \mathcal{K}_{X/k} \otimes \mathcal{O}_Y \to \mathcal{K}_{Y/k} \to 0$$

by(5.5.5.14). Taking the highest exterior power(5.5.1.25), we get:

$$\mathcal{K}_Y = \mathcal{K}_X \otimes \wedge^r \mathcal{N}_{Y/X} = \mathcal{K}_X \otimes (\wedge I/I^2)^{-1}$$
In particular, if \( r = 1 \) then \( Y \) is a divisor \( D \) in \( X \), the canonical sheaf

\[
\mathcal{K}_Y \cong (\mathcal{K}_X \otimes \mathcal{L}(D))_Y, \quad \mathcal{K}_{\mathbb{P}_k^n/k} = \mathcal{O}(-n - 1)(5.5.5.7).
\]

because \( \mathcal{I}_Y \cong \mathcal{L}(-Y) \) in this case so \( \mathcal{I}_Y/\mathcal{I}_Y^2 = \mathcal{L}(-Y) \otimes \mathcal{O}_Y \).

Taking dual, we get:

\[
0 \to \mathcal{T}_Y \to \mathcal{T}_X \otimes \mathcal{O}_Y \to \mathcal{N}_{Y/X} \to 0
\]

Prop. (5.10.1.18)[Geometric Genus]. For a smooth proper variety over a field \( k \), the geometric genus \( p_g \) is defined as the rank of the global section of the invertible canonical sheaf \( \mathcal{K}_X = \Lambda^n\mathcal{K}_{X/k} \).

It is a birational invariance. With the same methods, we can prove the rank of global sections of any other functorially defined bundles of \( \mathcal{K}_X \) is birational invariance, e.g. Hodge numbers.

**Proof:** For any rational map \( U \to Y \), there is a subset \( V \subset U \) and a local isomorphism \( V \to f(V) \), that will define an isomorphism of global sections. Because a nonzero section of an invertible sheaf cannot vanish on a dense open set \( f(V) \), the morphism of global sections is injective into \( \Gamma(U, \mathcal{O}_U) \).

Now we find a \( U \) that \( \text{codim}(X - U) > 1 \), then we can use(4.3.5.11) to get \( \Gamma(U) = \Gamma(X) \), then \( p_g(X) \geq p_g(X') \), and the converse is also true. For this, we use valuation criterion of properness, then for any codimension 1 point, the stalk is a DVR, thus we find a Spec\( \mathcal{O}_p \to X' \), this extends to a nbhd of \( p \) because \( X' \) is of f.t.

\[
\mathcal{K}_{\mathbb{P}_k^n} \cong \mathcal{O}(-n - 1), \quad \text{so it has no global section by(5.7.2.1),} \quad p_g(\mathbb{P}_k^n) = 0.
\]

Hence every rational variety over a field \( k \), i.e. one that is birational to \( \mathbb{P}_k^n \), has geometric genus 0.

**Complete Varieties**

Lemma (5.10.1.20)[Rigidity Lemma]. Let \( X, Y \) be varieties over a field \( k \) and \( f : X \times Y \to Z \) a morphism of schemes over \( k \) s.t. \( Z \) is separated. If \( X \) is complete with a rational point \( p \) and \( y \) is a rational point of \( Y \) s.t. \( f(\cdot, y) : X \to Z \) is constant, then \( f \) factors through the projection \( \text{pr}_Y : X \times Y \to Y \).

**Proof:** The equalizer is a closed subscheme of \( X \times Y \) as \( Z \) is separated(5.4.4.89), and \( X \times Y \) is a variety(5.10.1.9), thus we can check on closed points. Let \( g(y) = f(p, y) : Y \to Z \), then we want to show \( f = g \circ \text{pr}_Y \).

Let \( U \) be affine open in \( Z \), then because \( X \) is universally closed, \( \text{pr}_Y \) is closed, so \( V = \text{pr}_Y(f^{-1}(Z \setminus U)) \) is closed in \( Y \). But if \( y \notin V(\mathbb{F}) \), then \( f(X, y) \subset U \), and \( X \) is complete and connected, so \( f(\cdot, y) \) is constant(5.4.5.4), and \( f(x, y) = f(p, y) \). Thus \( f = g \circ \text{pr}_Y \) on a non-empty open subset of \( X \times Y \), which is a variety, so this is true on all of \( X \times Y \) by(5.10.1.11).

Prop. (5.10.1.21)[See-Saw Principle]. Let \( X \) be a complete variety over a field \( k \) and \( Y \) a \( k \)-scheme, then for any line bundle \( \mathcal{L} \) on \( X \times Y \), there is a closed subscheme \( Y_1 \subset Y \) s.t. for any morphism \( f : S \to Y \), \( (1 \times f)^*\mathcal{L} \) is trivial on \( X \times S \) iff \( f \) factors through \( Y_1 \).

**Proof:** This \( \mathcal{L} \) corresponds to a morphism \( Y \to \text{Pic}_X/k \), and clearly \( Y_1 \) is the fiber of \( Y \) over \( e \in \text{Pic}_X/k \).

Cor. (5.10.1.22). Let \( X \) be a complete variety over a field \( k \) and \( Y \) a reduced locally algebraic \( k \)-scheme, if \( \mathcal{L}, \mathcal{M} \) are two line bundles on \( X \times Y \) s.t. \( \mathcal{L}_y \cong \mathcal{M}_y \) for all closed points \( y \in Y \), and for some \( x \in X(k) \), \( \mathcal{L}_x \cong \mathcal{M}_x \), then \( \mathcal{L} \cong \mathcal{M} \).
Prop. (5.10.1.23) [Theorem of the Cube]. If $X, Y$ are complete varieties over a field $k$, and $Z$ is a connected, locally Noetherian $k$-scheme, if $x, y$ are rational points of $X, Y$ resp. and $z \in Z$. Supposed $\mathcal{L} \in \text{Pic}(X \times Y \times Z)$ that is trivial on $x \times Y \times z, X \times y \times Z, X \times Y \times z$, then $\mathcal{L}$ is trivial.

Proof: Let $Z'$ be the maximal closed subscheme of $Z$ given by (5.10.1.21). We show that $Z'$ is open, thus it is all of $Z$. If $\zeta \in Z'$, let $I \subset \mathcal{O}_{Z,\zeta}$ be the ideal defining $Z'$, we show $I = (0)$, which is equivalent to $Z'$ containing a nbhd of $\zeta$ (locally Noetherian used). If not, then because $\cap \mathfrak{m}^n = 0$ by Krull’s theorem (locally Noetherian used), there is an $n \geq 1$ that $I \subset \mathfrak{m}^n, I \not\subset \mathfrak{m}^{n+1}$. Let $a_1 = (I, \mathfrak{m}^{n+1})$, and $\mathfrak{m}^{n+1} \subset a_2 \subset a_1$ that $\dim_{k(\zeta)}(a_1/a_2) = 1$ (so $a_1 = a_2 + k(\zeta)a$ for some $a \in a_2$), and let $Z_i \subset \text{Spec} \mathcal{O}_{Z,\zeta}$ be the closed subscheme defined by $a_i$. Let $\mathcal{L}_i$ be the restriction of $L$ on $X \times Y \times Z_2$. If we show that $\mathcal{L}_2$ is trivial, then $Z_2$ is contained in $Z'$, which is contradiction because $I \not\subset a_2$.

For this, notice that $\mathcal{L}_1$ is trivial, and to show that $\mathcal{L}_2$ is trivial, it suffices to lift a non-vanishing global section $s$ of $\mathcal{L}_1$ to $\mathcal{L}_2$, because $Z_1, Z_2$ has the same underlying set.

For this, notice there is an exact sequence $0 \to k(\zeta) \xrightarrow{\Delta} \mathcal{O}_Z \to \mathcal{O}_{Z_2} \to 0$, where $k(\zeta)$ is the skyscraper sheaf at $\zeta$. So the obstruction of the lifting is an element $\xi \in H^1((X \times Y)_{k(\zeta)}, \mathcal{O}_{(X \times Y)_{k(\zeta)}})$. But now the conditions show that $\xi$ is zero under the pullback along $x \times Y \hookrightarrow X \times Y$ and $X \times y \hookrightarrow X \times Y$. So by Kunneth formula (5.7.1.9) and (5.10.1.12), $\xi$ vanishes.

2 Projective Varieties

Example (5.10.2.1) [Non-Projective Smooth Proper Varieties]. There are proper smooth complex varieties that are not projective. Examples are given in [Har77]?.

Prop. (5.10.2.2) [Affine Dimension Theorem]. Suppose $X, Y$ are subschemes of $\mathbb{A}^n_k$ of codimensions $d$ and $e$ resp., and $d + e \leq n$, then every non-empty irreducible component of $X \cap Y$ has dimension $\geq n - d - e$.

Proof: If $Y$ is an intersection of $e$ hypersurfaces, then this follows from Krull’s height theorem (4.2.4.18). In general, notice the diagonal map $\Delta : \mathbb{A}^n_k \to \mathbb{A}^n_k \times \mathbb{A}^n_k$ is an isomorphism onto the diagonal $T$ defined by $\{X_i = Y_i\}_{i=1,\ldots,n}$, thus it is a complete intersection in $\mathbb{A}^n_k \to \mathbb{A}^n_k \times \mathbb{A}^n_k$, and $\Delta$ induces an isomorphism $X \cap Y \cong X \times Y \cap T$, so we are done.

Cor. (5.10.2.3) [Projective Dimension Theorem]. Suppose $X, Y$ are subvarieties of $\mathbb{P}^n_k$ of codimensions $d$ and $e$ resp., and $d + e \leq n$, then $X$ and $Y$ intersect.

Proof: Take the affine cone, then item2 shows any irreducible component of $X \cap Y$ containing the origin has dimension $\geq 1$, which means $X \cap Y \neq \emptyset$.

Prop. (5.10.2.4) [Transversal Intersection]. Show that if $X$ is a closed subscheme of $\mathbb{P}^n_k$ of dimension $r$, then there is an intersection of $r + 1$ non-empty hypersurfaces missing $X$. And if $k$ is infinite, these hypersurfaces can be chosen to be hyperplanes.

If $k$ is infinite, there is an intersection of $r$ non-empty hypersurfaces intersecting $X$ at f.m. points.

Proof: Let $\eta_1, \ldots, \eta_n$ be the generic points of $X$, we want to find a hypersurface $F$ that doesn’t contain any of these generic points. We use induction on $n$. If $n = 1$, then there is clearly a hyperplane missing $\eta_1$. If we find a hypersurface missing $\eta_1, \ldots, \eta_{n-1}$, if it also misses $\eta_n$, we are done, if it contains $\eta_n$, we can change $\eta_n$ to $\eta_i$ and consider again. If we find polynomials...
Prop. (5.10.4.3). Let \( \varphi : X \to X' \) be a birational map of \( K \)-varieties with \( X \) smooth. If the base change \( \varphi_K \) extends to a morphism \( X_K \to X'_K \), then \( \varphi \) extends to a morphism \( X \to X' \).

Proof: Let \( U \) be an open dense subset that \( \varphi \) is defined. For a point \( x \), let \( x' = \varphi_K(x) \), then \( x' \) is in the closure of \( \varphi(U) \). By (5.4.6.2), it suffices to construct a morphism \( \mathcal{O}_{X',x'} \to \mathcal{O}_{X,x} \), i.e., to prove for any rational function \( f \) regular at \( x' \), \( \varphi \circ f \) is regular at \( x \). The argument is the same as that of (5.4.5.14).

For any such \( f \), \( f_K \circ \varphi_K \) is regular at \( x \), thus no pole of \( \text{div}(f_K \circ \varphi_K) \) passes through \( x \). For the rest, Cf. [Diophantine Geometry, P576].

Prop. (5.10.4.4)[Generic Separable Degree]. Let \( \varphi : X \to X' \) be a dominant morphism of varieties over a field \( k \) of the same dimension, then there exists an open dense subscheme \( U' \) of \( X' \) s.t. \( \varphi^{-1}(U') \to U' \) is finite and the fibers all have cardinality \( \deg_s(\varphi) \).

Proof: By (5.10.3.2), we can decompose \( \varphi \) and assume it is either separable or purely inseparable, and also primitive. If it is separable, let it be generated by \( t \). After shrinking (and cutting closure of images), we may assume the coefficients of \( t \) are regular functions, and \( \Gamma(X) = \Gamma(X')[t]/(q(t)) \). As \( q \) is separable, there exists \( a, b \in K(X') \) s.t. \( aq + bq' = 1 \). We may shrink \( X' \) and assume \( a, b \in \Gamma(X') \), so \( q \) is also separable over any fiber of \( X \), which means the fibers all have cardinality \( \deg_s(\varphi) \).

If it is purely inseparable, let \( q(t) = t^q - h \) be the minimal polynomial of \( t \) over \( K(X') \), \( h \in K(X') \). Then after shrinking, we may assume \( h \in \Gamma(X') \), thus \( q(t) \) is purely inseparable over any fiber of \( X \), which means  

4 Others

Prop. (5.10.4.1). Varieties are triangulable.

Proof: Cf. [Triangulation of Algebraic Sets, Hironaka].
Fano Varieties

Def. (5.10.4.2) [Fano Varieties]. A Fano variety is a complete smooth variety $X$ over a field $K$ s.t. $\mathcal{K}_X$ is ample.

Prop. (5.10.4.3). a smooth complete intersection of hypersurfaces in $\mathbb{P}^n_K$ is Fano if and only if the sum of their degrees is at most $n$.

Prop. (5.10.4.4) [Kollár-Miyaoka-Mori]. Fano varieties over an alg.closed field are rationally chain connected.

Proof: Cf. [Rational connectedness and boundedness of Fano manifolds, Kollár]. □

Rationally Connected Varieties

Def. (5.10.4.5) [Rationally Connected Varieties]. A variety $X$ over $K$ is called rationally connected if any two points of $X(\overline{K})$ can be connected by a rational curve (5.11.1.1) over $\overline{K}$.

5 Relative Varieties

Def. (5.10.5.1) [Varieties over Schemes]. Let $S \in \text{Sch}$, a (proper/smooth) variety over $S$ is a (proper/smooth) flat morphism $f : X \to S$ s.t. all the geometric fibers of $f$ are geo.integral over the resp. residue field $k(s)$. It can be regarded as a family of (proper/smooth)varieties parametrized by $S$.

Being a (proper/smooth) variety is stable under base change.

Prop. (5.10.5.2) [Global Sections]. Let $S \in \text{Sch}$ be locally Noetherian and $X$ a proper variety over $S$, then $\mathcal{O}_S \to f_*\mathcal{O}_X$ is an isomorphism.

Proof: For any closed point $s \in S$, $k(s) \to H^0(X_s, \mathcal{O}_{X_s})$ is an isomorphism by (5.10.1.12), and this isomorphism factors through $k(s) \to f_*(\mathcal{O}_X) \otimes k(s) \to H^0(X_s, \mathcal{O}_{X_s})$. So $f_*(\mathcal{O}_X) \otimes k(s) \to H^0(X_s, \mathcal{O}_{X_s})$ is surjective, thus it is an isomorphism by item 4 → 3 of (7.7.3.16). Thus the first map is also an isomorphism.

Now $\mathcal{O}_S \to f_*(\mathcal{O}_X)$ is a surjection at $s$ by Nakayama. Let $\mathcal{Q}$ be the coherent sheaf on $S$ associated to $\mathcal{F}$, then by (7.7.3.16), it is free at $s$, and $\mathcal{Q}_s = H^0(X_s, \mathcal{O}_{X_s})$ is of rank 1, but also $\mathcal{Q}^\vee \cong f_*(\mathcal{O}_X)$, so $\mathcal{O}_S \to f_*(\mathcal{O}_X)$ is in fact a surjection at $s$. Now $s$ is arbitrary, so $\mathcal{O}_S \to f_*(\mathcal{O}_X)$ is an isomorphism. □

Prop. (5.10.5.3). Let $(R, K, k)$ be a DVR and $X$ is a smooth $R$-scheme s.t. $X_K$ is geo.integral and $X_k$ is proper, then $X$ is a proper smooth variety over $R$.

Proof: Cf. [Good Reduction of Abelian Varieties, P495] □
5.11 Curves

Main references are [黎曼曲面, 伍鸿熙], [Vak17]Chap19, [G-H78], [Har77]Chap4 and [Sta]Chap53.

In this section, properties to morphisms of relative dimension \( \leq 1 \) are studied.

Notations (5.11.0.1).
- Use notations defined in Cohomology of Schemes.
- Use notations defined in Varieties.

1 Basics

Def. (5.11.1.1) [Rational Curve]. A rational curve over a field \( k \) is a curve that is birational to \( \mathbb{P}^1_k \).

Lemma (5.11.1.2). If \( X \) is an integral separated scheme and \( U \subset X \) is an non-empty affine open that \( X \setminus U \) is a finite set of points with \( O_{X,x} \) Noetherian of dimension 1, then there exists a base-point free invertible sheaf \( \mathcal{L} \in \text{Pic}(X) \) and a section \( s \) s.t. \( U = X_s \).

Proof: Cf. [Sta]09NB. \( \square \)

Prop. (5.11.1.3). A Noetherian separated scheme of dimension \( \leq 1 \) has an ample invertible sheaf.

Proof: First reduce to the case when \( X_{\text{red}} \), because (5.11.2.19) shows any invertible sheaf on \( X_{\text{red}} \) is a pullback of a sheaf of \( X \) and (5.5.4.15) shows this sheaf is ample.

Second we reduce to the case \( X \) is integral. Let \( X_i \) are the integral irreducible components of \( Z \), Cf. [Sta]09NX?

Finally, for \( X \) integral, the assertion follows from (5.11.1.2) and (5.5.4.10). \( \square \)

Cor. (5.11.1.4) [Complete Precurves are Projective]. A separated algebraic scheme \( X \) of dimension 1 over a field \( k \) is \( H \)-(quasi)projective, by (5.11.1.3) and (5.5.4.22). If \( X \) is proper, then it is projective.

Prop. (5.11.1.5) [Completion of Curves]. For a separated algebraic \( k \)-scheme \( X \) of dimension \( \leq 1 \), there is an open immersion \( j : X \to \overline{X} \) that

- \( \overline{X} \) is \( H \)-projective over \( k \).
- \( j(X) \subset \overline{X} \) is dense and schematically dense open subscheme.
- \( \overline{X} \setminus X \) consists of f.m. closed points \( \{x_i\} \) of \( \overline{X} \), called the completion curve of \( X \). And when \( X \) is reduced, the stalk at \( x_i \) are DVRs. In particular, It is non-singular if \( X \) is non-singular.

Proof: By (5.11.1.3), we can assume \( X \) is a locally closed subscheme of \( \mathbb{P}^n_k \). Let \( \overline{X} \) be the scheme theoretic image (5.4.4.62) of the inclusion, then 1,2 holds by (5.4.4.70). 3 holds because \( \overline{X} \setminus X \) is Noetherian of dimension 0.

For the last assertion, Cf. [Sta]0BXW. \( \square \)

Cor. (5.11.1.6). A morphism of prevarieties \( X \to Y \) with \( X \) a precurve (thus reduced) and \( Y \) proper over a field \( k \) factors through the completion \( \overline{X} \) of \( X \) by (5.4.5.14).

Prop. (5.11.1.7) [Affine or Projective]. A precurve over a field \( k \) is either affine (not proper) or \( H \)-projective (proper).
Cor. (5.11.1.8). Let $X$ be a separated scheme algebraic over a field $k$. If $\dim X \leq 1$ and no irreducible component of $X$ is proper of dimension 1, then $X$ is affine.

Proof: Let $X_i$ be f.m. irreducible components of $X$, then they are precurves in the induced reduced structure, so they are affine by (5.11.1.7). Now $\coprod X_i \to X$ is a finite surjective morphism, so $X$ is affine by (5.4.4.36).

Prop. (5.11.1.9). A map from a proper connected scheme to a precurve is either constant or surjective.

Proof: Because the closed subset of a precurve is either itself or f.m. closed points.

Prop. (5.11.1.10) [Constant or Finite]. Let $f : X \to Y$ be a morphism of schemes over a field $k$ that $Y$ is separated and $X$ is proper of dimension $\leq 1$. If the image of every irreducible component of $X$ is not a pt, then $f$ is finite. If $Y$ is a precurve, then it is moreover surjective.

Proof: Cf. [Sta] 0CCL.

Def. (5.11.1.11) [Separable Morphisms]. Let $f : X \to Y$ be a non-constant morphism of precurves, then $f$ is finite surjective by (5.11.1.10). so $\deg(f)$ is finite (5.4.4.55), and we can define separable/purely separable morphisms as in (5.4.4.55).

Non-Singular Curves

Def. (5.11.1.12) [Uniformizer]. Let $C$ be a precurve over a field $k$, then the local rings of $C$ at a non-singular closed point $p$ is a DVR by (10.3.3.4). Then an element $t \in K(C)$ with valuation 1 is called a uniformizer at $p$.

Prop. (5.11.1.13). Let $C$ be a precurve over a field $K$, and $t \in K(C)$ is a uniformizer at some non-singular point, then $K(C)$ is a finite separable extension of the subfield generated by $t$.

Proof: $K(C)$ is a finite extension of $K(t)$, because $\tr \deg(K(C)/K) = 1$ and $t$ is not algebraic over $K$ by valuation reasons. Then it suffices to show for any $x \in K(C)$, $x$ is separable over $K(t)$. Let $\Phi(X, T) = \sum a_{ij} T^i X^j$ be a minimal polynomial of $x$ over $K(T)$. It is separable iff for some $(j, p) = 1$ and some $i$, $a_{ij} \neq 0$. If it is not separable then we can write $\Phi(X, T) = \sum_{k=0}^{p-1} \varphi_k(X, T) T^k$. But each $\varphi_k(x, t)^{p^k}$ has distinct valuations, unless they are all zero, contradicting the fact $\Phi$ is a minimal polynomial.

Prop. (5.11.1.14) [Non-singular Complete Precurves and DVRs]. Let $C$ be a non-singular complete precurve, then all valuation rings of $K(C)$ containing $k$ are DVRs, and the set of closed points of $C$ correspond to the set of DVRs in $K(C)$ containing $k$, which is denoted by $\Sigma^0_{K(C)}$.

Proof: This is a consequence of the valuation criterion (5.4.5.13). Notice that the local rings of $C$ at closed points are all DVRs (10.3.3.4), thus they must equal to the valuation ring given.

Prop. (5.11.1.15) [Extension of Rational Maps]. Rational map from a non-singular precurve to a complete prevariety is the same as a morphism, by (5.4.5.15).

Cor. (5.11.1.16). Two birationally equivalent normal proper precurves over a field is isomorphic.

Thus if a normal precurve is birationally equivalent to another normal complete curve, then it is an open immersion, by (5.11.1.5).
Prop. (5.11.1.17) [Category of Non-singular Projective Precurves]. Let \( k \) be a field, the following categories are equivalent:

1. The opposite category of f.g. field extensions of \( k \) of trans.deg 1 with injective \( k \)-homomorphisms.

2. The category of precurves and dominant rational maps.

3. The category of normal complete precurves over \( k \) with non-constant morphisms.

4. The category of nonsingular projective precurves over \( k \) with non-constant morphisms.

Proof: 1 and 2 are equivalent by (5.10.3.2).

3 and 4 are equivalent by (5.11.1.7) and the fact normal and regular are the same (5.4.2.10).

For the rest, Cf. [Sta]0BY1. \( \square \)

Cor. (5.11.1.18) [Non-singular Projective Model]. Comparing this and (5.10.3.2), we see that every precurve over \( k \) is birational to a unique non-singular proper precurve over \( k \) with the same function field, which is called the non-singular projective model.

Prop. (5.11.1.19) [Flatness and Associated Points]. \( f : X \to Y \) with \( Y \) integral and regular of dimension 1. Then \( f \) is flat iff every associated prime of \( X \) is mapped to the generic point of \( Y \).

In particular when \( X \) is reduced, this is equivalent to every irreducible component of \( X \) dominants \( Y \), by (4.2.5.25).

Proof: If \( x \) is mapped to a closed pt of \( Y \), then \( O_{y,Y} \) is a DVR, let \( t \) be a uniformizer, then \( t \) is not a zero-divisor, and \( f^\sharp(t) \in \mathfrak{m}_x \) is also not a zero-divisor. So \( x \) is not an associated point.

Conversely, to show \( f \) is flat, if \( y \) is the generic point, then \( O_{y,Y} \) is a field, so it is flat. When \( y \) is a closed pt, \( O_{y,Y} \) is a DVR, so by (4.4.1.11), we need to show that it is torsion free. If it is not, then \( f^\sharp(t) \) must be a zero-divisor for a uniformizer \( t \) of \( O_{y,Y} \). But then it is contained in some associated prime \( p \) of \( O_{x,X} \) (4.2.5.17). Now \( p \) is mapped to \( y \), which is a contradiction. \( \square \)

Cor. (5.11.1.20) [Morphism to a Non-singular Curve is Flat]. If \( f : X \to Y \) is a dominant morphism from a prevariety to a non-singular curve over \( k \), then \( f \) is flat.

Cor. (5.11.1.21) [Flat Specializations along Curves]. Let \( Y \) be integral and regular of dimension 1 and \( P \) a closed pt. \( X \) is a closed subscheme in \( \mathbb{P}^n_Y - P \) that is flat over \( Y - P \), then there is a unique closed subscheme \( \overline{X} \) closed in \( \mathbb{P}^n_Y \) that is flat over \( Y \) and restrict to \( X \) on \( \mathbb{P}^n_Y - P \).

Proof: Choose the scheme-theoretic closure of \( X \) in \( \mathbb{P}^n_Y \). Cf. [Hartshorne P258]. \( \square \)

Cor. (5.11.1.22) [Finite Flatness]. Any non-constant morphism from a precurve to a nonsingular precurve is finite locally free, by (5.11.1.19) and (5.11.1.10).

Prop. (5.11.1.23). A projective non-degenerate non-singular curve of degree \( d \) in \( \mathbb{P}^n_k \) is isomorphic to the \( n \)-tuple embedding, and \( d = n \).

This has easy generalizations to surfaces and higher dimensions.

Proof: (5.5.3.16) shows \( O_X(1) \cong O(d) \) over \( \mathbb{P}^1_k \), and the restriction of global sections is injective. So the global section is an isomorphism, and it defines the embedding up to a linear automorphism. \( \square \)
Prop. (5.11.1.24) [Genera Equal]. For a complete smooth curve $X$ over a field $k$,

$$p_a(X) = p_g(X) = \dim_k H^1(X, \mathcal{O}_X)$$

by Serre duality (5.8.6.19) and (5.10.1.18) (5.7.3.6). So from now on we use genus to denote the arithmetic genus.

Cor. (5.11.1.25) [Topological Genus]. By GAGA, for a complex complete smooth curve, the genus also equals the topological genus.

Morphisms Between Non-singular Curves

Prop. (5.11.1.26) [Degree and Analytic Degree]. Let $f : C \to C'$ be a non-constant morphism between smooth complex curves, then the degree defined in (5.4.4.55) is the same as the degree as map of Riemann surfaces.

Proof: This is because the map is finite locally free (5.11.1.22), thus for an affine open subset $U = \text{Spec} A$ of $C'$, the $f^{-1}(U) = \text{Spec} B$ where $B \cong A^\otimes n$ as $A$-modules, where $n$ is the degree. Then clearly for most $x \in U$, $\sharp f^{-1}(x) = n$ (look at the minimal polynomial of a family of generators for $B$ over $A$).

Def. (5.11.1.27) [Ramification Degrees]. Let $f : X \to Y$ be a morphism of non-singular precurves over a field $k$, let $P \in X$ be a closed point and $f(P) = Q$. Because the local rings are DVRs, we define the ramification degree $e_P(f)$ where $f^\sharp(m_Q)\mathcal{O}_{X,P} = n_P^e(f)$.

$f$ is called weakly unramified at $P$ if $e_P(f) = 1$, and it is called unramified at $P$ if moreover $\kappa(P)/\kappa(f(P))$ is separable. $f$ is called tamely unramified at $P$ if $e_P(f) = 1$.

Notice that unramifiedness just means the morphism is unramified, by (5.6.5.8) and (5.11.1.22).

Prop. (5.11.1.28). Let $f : X \to Y$ be a non-constant morphism of non-singular precurves over a field $k$, then

- If $g : Y \to X$ be another morphism of non-singular precurves, then for any $P_1 \in X$, $e_{P_1}(g \circ f) = e_P(g \circ f)(g)$.
- for any closed point $Q \in C_2$, $\sum_{P \in f^{-1}(Q)} e_P(f)[k(P) : k(Q)] = \deg(f)$.
- If $k$ is alg.closed, then for a.e. closed point $Q \in C_2$, $\# f^{-1}(Q) = \deg_s(f)$.

Proof: 1: Trivial.
2: This follows from (5.11.1.44).
3: This follows from (5.10.3.4).

Prop. (5.11.1.29). If $f : X \to Y$ is a non-constant morphism of percurves over a field $k$ s.t. $X$ is smooth and $Y$ is non-singular, then $Y$ is also smooth, by (5.1.5.28).

Prop. (5.11.1.30). Let $X$ be a smooth curve over a field $k$, $x \in X$ and $\mathfrak{p} \in X_k$ is a point mapping to $x$, then the ramification degree of $\mathcal{O}_{X,x} \subset \mathcal{O}_{X_\mathfrak{p}}$ equals the inseparable degree of $k(x)/k$.

Proof: By (5.6.6.7), we can find a étalemap $X \to \mathbb{A}^1_k$, which has ramification degree 1 and separable, so we may assume $X = \mathbb{A}^1_k$. Then the assertion is clear.

Prop. (5.11.1.31) [Separable Morphisms]. Let $f : X \to Y$ be a morphism of smooth curves over $k$, then the following are equivalent:
1. $f$ is finite separable.
2. $df^* : f^*\Omega_{Y/k} \to \Omega_{X/k}$ is non-zero.
3. $\Omega_{X/Y}$ is supported on a proper closed subscheme of $X$.
4. There exists a non-empty open subset $U \subset X$ s.t. $f$ is unramified.
5. There exists a non-empty open subset $U \subset X$ s.t. $f$ is étale.

**Proof:** As $X, Y$ are smooth, $\Omega_{X/k}, \Omega_{Y/k}$ are invertible sheaves, and the exact sequence

$$f^*\Omega_{Y/k} \to \Omega_{X/k} \to \Omega_{X/Y} \to 0$$

shows 2, 3 are both equivalent to $\Omega_{X/Y} = 0$.

3, 4, 5 are equivalent as $f$ is automatically flat (5.11.1.20).

1, 5 are equivalent by (5.6.5.9). $\square$

**Prop. (5.11.1.32) [Riemann-Hurewitz for Separable Maps].** If $f : X \to Y$ is a non-constant separable map between two complete smooth curves over a field $k$, then

$$2g_X - 2 = \deg(f)(2g_Y - 2) + \sum_{x \in X} d_x[\kappa(x) : k],$$

where $d_x = \text{length}_{\mathcal{O}_{X,x}}(\Omega_{X/Y,x}) \geq 0$ satisfies $d_x \geq e_x(f) - 1$, and equality holds iff $f$ is tamely unramified at $P$.

**Proof:** By (5.8.7.12), in this case the vanishing locus $R$ of $df^*$ is an effective Cartier divisor, and $f^*K_{Y/k} \otimes \mathcal{O}(R) \cong K_{X/k}$, so by (5.11.2.10)(5.11.2.3)(5.11.2.7),

$$2g_X - 2 = \deg(K_{X/k}) = \deg(f^*K_{Y/k} \otimes \mathcal{O}(R)) = \deg(f) \deg(K_{Y/k}) + \deg(R) = \deg(f)(2g_Y - 2) + \deg(R).$$

For analysis of $d_x$, Cf. [Sta]0C1F. $\square$

**Cor. (5.11.1.33).** The only geo.integral unramified finite covering of $\mathbb{P}^1_k$ is itself.

**Thm. (5.11.1.34) [De Franchis].** Let $k \in \text{Field}$ and $C, C'$ are two complete smooth curves over $k$. Then if $g(C) \geq 2$, there are only f.m. non-constant maps $C' \to C$.

In particular, $\# \text{Aut}(C) < \infty$.

**Proof:** We prove for $k = \mathbb{C}$? Cf. [Mil08]P146.

Any automorphism of $C$ fixes its set of Weierstrass sets, which is finite, so we only need to consider the case that it fixes all Weierstrass points.

If $C$ is hyperelliptic, consider a hyperelliptic map, this covering has an involution of $C$, and this is just $C \mapsto C/\tau$. So modulo $\tau$, it suffices to show $\mathbb{P}^1$ has f.m. automorphisms fixing the branch points. But this is true, as $2g + 2 > 3$.

If $C$ is non-hyperelliptic, then there are more than $2g + 2$ Weierstrass points. But we can find a function $f$ on $C$ with $g + 1$ zeros and poles, by Riemann-Roch, then for an automorphism $\varphi$ of $C$, $f - \varphi^*f$ has no more than $2g + 2$ poles, so also has no more than $2g + 2$ zeros. But $\varphi$ fixes all Weierstrass points, so it has more than $2g + 2$ zeros, contradiction. $\square$

**Prop. (5.11.1.35) [Hurewitz’s Automorphism Theorem].** If $C$ is a complete smooth curve of genus $g \geq 2$ over a field of characteristic 0, then $\# \text{Aut}(C) \leq 84(g - 1)$. 
Proof: We may pass to the alg. closure. By (5.11.1.34), \( \# \text{Aut}(C) < \infty \). In fact, let \( G \) be a finite group acting on \( C \), let \( C' \) be the non-singular precurve corresponding to \( C' \), then by (2.2.7.4), \( C \to C' \) is a Galois cover with Galois group \( G \). Now by Dedekind extension theory, \( G \) acts transitively on the preimage of a given point. Suppose there are \( n \) branched points with ramification degrees \( r_i \), then by Riemann-Hurwitz (5.11.1.32) (notice in this case it is tamely unramified):

\[
(2g - 2) = |G|(2g(C') - 2 + \sum_{i=1}^{n} \frac{r_i - 1}{r_i}).
\]

Then a combinatorial argument shows the maximal possible \(|G|\) is obtained when \( g(C') = 0, n = 3 \) and \((r_1, r_2, r_3) = (2, 3, 7)\).

Remark (5.11.1.36). In the case char \( k \neq 0 \), there may be more automorphisms. For example, if \( p \in \mathbb{P} \setminus \{2\} \), the completion of the affine curve \( y^{p^n} = x + x^{p^n+1} \) has genus \( g = p^3(p^n - 1)/12 \) and \( \# \text{Aut}(C) = p^{3n}(p^{3n} + 1)(p^{2n} - 1) \), Cf.[H.Stichtenoth,UberdieAutomorphismengruppeeinesalgebraischenFunktionenkoerpersvonPrimzahlcharakteristik. I. Eine Abschatzung der Ordnung der Automorphismengruppe, Arch. Math. (Basel) 24 (1973), 527–544.].

Prop. (5.11.1.37) [Frobenius Map]. Let \( C \) be a smooth curve over a field \( k \) of characteristic \( p \), and \( C \xrightarrow{F_{X/k,r}} C^{(r)} \) be the Frobenius, where \( C^{(r)} = C \otimes_{k,Frob^e} k \), then \( F_{X/k,r} \) is purely inseparable, and \( \deg(F_{X/k,r}) = p^r \). And it is a topological homeomorphism by (4.1.7.26).

Proof: To show inseparability, we can base change to \( \overline{k} \), then the field map is \( f/g \mapsto f(X^{p^r})/g(X^{p^r}) \), which is just \( K(C_{\overline{k}})^{p^r} \), so purely inseparable of degree \( p^r \).

Prop. (5.11.1.38) [Inseparable Decomposition]. Let \( k \) be a field of characteristic \( p > 0 \). If \( C_1 \) is a smooth complete precurve, then any map of non-singular complete precurves \( f : C_1 \to C_2 \) over \( k \) factors as

\[
C_1 \xrightarrow{F_{X/k,r}} C_1^{(r)} \xrightarrow{\lambda} C_2
\]

where \( C_1^{(r)} = C_1 \otimes_{k,Frob^e} k \), and \( \lambda \) is separable.

Proof: By (5.11.1.17), it suffices to show any inseparable morphism is a Frobenius. It suffices to show that any subfield of \( K(X) \) of index \( p \) equals \( K(X^{(1)}) = kK(X)^p \). For this, Cf.[Sta]0CCY?

Cor. (5.11.1.39). If \( C \to C' \) is a non-constant separable map between complete smooth curves, then \( g(C) \geq g(C') \).

Proof: This follows from (5.11.1.38)(5.11.1.32) and the fact \( C_1^{(r)} \) is smooth and have the same genus as \( C_1 \) by flat base change.

Divisors on Curves

Def. (5.11.1.40) [Divisors on Curves]. If \( X \) is a locally algebraic integral scheme of dimension 1 over an alg. closed field, then a Weil divisor on \( X \) are just a locally finite formal sum of closed pts.

If \( X \) is integral algebraic over a field \( k \) of dimension 1, then the sum is in fact finite, we can define the degree of a Weil divisor \( D = \sum n_PP \) as \( \deg(D) = \sum n_P[k(P) : k] \).

Similarly, for a Cartier divisor \( D \) on \( X \), the degree of \( D \) is defined to be \( \dim_k \Gamma(D, \mathcal{O}_D) \).

By (6.1.5.1), a Cartier Divisor on \( X \) is equivalent to an effective Weil divisor, and the definition of degrees are compatible.
Cor. (5.11.1.41) [Non-singular Case]. As a nonsingular precurve $C$ is locally factorial, (5.5.3.15) shows in this case a line bundles on $C$ is equivalent to a Weil divisor on $C$.

Prop. (5.11.1.42) [Pullback of Divisor]. For a non-constant morphism $f$ between two non-singular curves over alg.closed field, e.g. dominant morphism between complete non-singular curves, $\deg f^*D = \deg f \cdot \deg D$. This is because $f$ is finite locally free (5.11.1.22), thus this follows from [Sta]02RH?

Prop. (5.11.1.43). An element $\xi \in k$ in the function fields of a projective non-singular curve over an alg.closed $k$ defines an inclusion $k(f) \subset K(X)$ thus a morphism from $X$ to $P^1_k$ (5.10.3.2), and $(f) = \varphi^*([0] - \{\infty\})$.

Prop. (5.11.1.44). Let $\pi : C \to C'$ be a non-constant separable morphism of precurves over a field $k$ that $C'$ is nonsingular, $p \in C'$ is a closed point, then $\pi$ is finite locally free by (5.11.1.22), and

- $\dim_k(\Gamma(\pi^{-1}(p))) = (\deg \pi)(\deg p)$.
- Let $\varpi$ be a uniformizer of the DVR $\mathcal{O}_{C',p}$, then $\deg \pi = \sum_{x \in \pi^{-1}(p)} [k(x) : k(p)] \text{ord}_{\mathcal{O}_{C,x}}(f^*\varpi)$.

Proof: Look affine locally, then these follow from the fundamental identity (4.2.7.18).

Prop. (5.11.1.45). For a 1-dimensional integral scheme $c : X \to k$ proper over a field $k$ and a function $f \in K(X)^*$, $\sum_{x \text{ closed}} [k(x) : k] \text{ord}_{\mathcal{O}_{X,x}}(f) = 0$. In other words, the number of zeros of $f$ equals the number of poles of $f$.

Proof: It suffices to show that the pushforward $c_* \text{div}(f) = 0 \in \text{CH}_0(\text{Spec } k)$. consider $Y$ the closure of the graph of $f$ in $X \times P^1_k$, then there is a commutative diagram

\[
\begin{array}{ccc}
Y & \xrightarrow{pr_1} & X \\
\downarrow{pr_2} & & \downarrow{c} \\
P^1_k & \xrightarrow{c'} & \text{Spec } k
\end{array}
\]

and $\text{div}_X(f) = \text{pr}_{1*} \text{div}_Y(f)$ by (6.1.2.22). We may assume $f$ is not constant, then $\text{pr}_2$ is finite locally free of degree $d$, and $\text{div}_Y(f) = \text{pr}_2^*([0] - [(\infty)])$, so $\text{pr}_{2*} \text{div}_Y(f) = d([0] - [(\infty)])$ is mapped to $0 \in \text{CH}_0(\text{Spec } k)$.

2 Vector Bundles

Degrees and Riemann-Roch

Def. (5.11.2.1) [Degrees]. The degree of a locally free sheaf $\mathcal{E}$ of rank $n$ on a proper scheme $X$ of dimension $\leq 1$ over a field $k$ is defined to be $\deg(\mathcal{E}) = \chi(X,\mathcal{E}) - n\chi(\mathcal{O}_X)$ (5.7.3.1).

If $X$ is integral (e.g. a complete precurve), this definition can extends to any coherent sheaves $\mathcal{F}$, if we define $\text{rank}(\mathcal{F}) = \dim_k(\eta) \mathcal{F}_\eta$.
Prop. (5.11.2.2) The degree function is additive, stable under base change of fields, and stable under birational equivalence of proper scheme $X$ of dimension 1 over a field $k$.

Proof: The base change follows from flat base change (5.7.5.1), the additivity follows from the additivity of rank and Euler characteristic (5.7.3.1).

For the birational equivalence, if $f : X \to Y$ is a birational map between proper schemes of dimension $\leq 1$ over $k$, then $f$ is proper with finite fibres, so $f$ is finite (5.4.5.5), thus for any $E \in \mathcal{O}_{Y}^{\text{free, n}}(Y)$, $f_{*}f^{*}E = E \otimes_{O_{Y}} f_{*}O_{X}$, and there is an exact sequence

$$0 \to \mathcal{K} \to O_{Y} \to f_{*}O_{X} \to Q \to 0$$

where $\mathcal{K}$, $Q$ are coherent sheaves on $Y$ with supported dimension 0. Then by (5.7.3.5) and (5.7.3.3),

$$\chi(Y, E) - \chi(X, f^{*}E) = \chi(Y, E) - \chi(Y, f_{*}f^{*}E) = \chi(Y, \mathcal{K} \otimes E) - \chi(Y, Q \otimes E) = n \chi(Y, \mathcal{K}) - n \chi(Y, Q) = n \chi(Y, O_{Y}) - n \chi(X, O_{X}) \square$$

Prop. (5.11.2.3) [Non-reduced Riemann-Roch]. If $X$ is a proper scheme over a field $k$ of dimension $\leq 1$ with integral components $C_{i}$ of $X$ of dimension 1 with generic points $\eta_{1}, \ldots, \eta_{r}$ and multiplicity $m_{i}$, and $E \in \text{Vect}^{n}(C), F \in \text{Coh}(C)$, then

$$\chi(E \otimes F) = \sum_{i} (\text{length}_{\mathcal{O}_{X,m_{i}}} F_{\eta_{i}}) \text{deg}(E|_{C_{i}}) + n \chi(F).$$

Proof: We use dévissage (5.5.1.55), the condition 1 are true by additivity of $\chi$, and for condition 2, take $G = i_{*}O_{Z}$, the equation holds by (5.7.3.5) and projection formula. □

Cor. (5.11.2.4). Let $X$ be a proper scheme of dimension $\leq 1$ over a field $k$, and $C_{i}$ are the irreducible components of $X$ of dimension 1 with the induced reduced structure and multiplicity $m_{i}$, then for $E \in \text{Coh}^{\text{free}}(X)$,

$$\text{deg}(E) = \sum m_{i} \text{deg}(E|_{C_{i}}).$$

Cor. (5.11.2.5). Let $X$ be a proper scheme of dimension $\leq 1$ over a field $k$, then

- If $E \in \text{Coh}^{\text{free, m}}(X), F \in \text{Coh}^{\text{free, n}}(X)$, then $\text{deg}(E \otimes F) = m \text{deg}(F) + n \text{deg}(E)$.

- If $L, M \in \text{Pic}(X)$, then $\text{deg}(L \otimes M) = \text{deg}(L) + \text{deg}(M)$.

- If $L \in \text{Pic}(X)$, then $\text{deg}(L) = - \text{deg}(L^{-1})$.

- If $E \in \text{Coh}^{\text{free}}(X)$, then $\text{deg}(E) = \text{deg}(\wedge E)$.

Proof: By (5.11.2.4), we can assume $X$ is integral. Then 1, 2 follow from (5.11.2.3), and 3 follows from the fact there is a modification $X' \to X$ s.t. $f^{*}E$ has a filtration with invertible sheaves $L_{i}$ as quotients (5.5.1.30). Then by (5.11.2.2), we can work on $X'$. Then $\text{deg}(E) = \otimes_{i} L_{i}$, and the assertion follows from additivity and (5.11.2.3). □

Prop. (5.11.2.6). If $D$ is an effective Cartier divisor on a proper scheme of dimension $\leq 1$ on a field $k$, then for $E \in \text{Coh}^{\text{free, n}}(X)$,

$$\text{deg}(E(D)) = n \dim_{k} \text{deg}(D) + \text{deg}(E)$$

In particular, $\text{deg}(L(D)) = \text{deg}(D)$. 
Proof: By (5.8.1.2), $D$ is nowhere dense in $X$, thus $D$ is finite over $k$, and there is an exact sequence

$$0 \to \mathcal{E} \to \mathcal{E}(D) \to \mathcal{E}(D)|_D \to 0.$$ 

So the assertion follows from (5.7.3.5).

Prop. (5.11.2.7). Let $f : X \to Y$ be a non-constant map of complete precurves over a field $k$ and $\mathcal{E} \in \mathcal{Coh}^{\text{free}}(Y)$, then $\deg(f^*\mathcal{E}) = \deg(f) \deg(\mathcal{E})$.

Proof: By (5.11.1.10) and (5.11.2.3),

$$\chi(X, f^*\mathcal{E}) = \chi(Y, \mathcal{E} \otimes f_*\mathcal{O}_X) = \deg(f) \deg(\mathcal{E}) + \text{rank}(\mathcal{E}) \chi(X, \mathcal{O}_X).$$

Prop. (5.11.2.8) [Degree and Sections]. Let $C$ be a complete precurve over a field $k$ and $\mathcal{L} \in \text{Pic}(C)$, then

- If $\mathcal{L}$ has a non-zero section, then $\deg(\mathcal{L}) \geq 0$.
- If $\mathcal{L}$ has a non-zero section that vanishes at some point, then $\deg(\mathcal{L}) \geq 1$.
- If both $\mathcal{L}, \mathcal{L}^{-1}$ have non-zero sections, then $\mathcal{L} \cong \mathcal{O}_X$.
- If $\text{deg}(\mathcal{L}) \leq 0$ and $\mathcal{L}$ has a non-zero section, then $\mathcal{L} \cong \mathcal{O}_X$.
- If $\mathcal{N} \to \mathcal{L}$ is a non-zero map of invertible sheaves, then $\deg(\mathcal{L}) \geq \deg(\mathcal{N})$, with equality iff this is an isomorphism.

Proof: If $s$ is a section of $\mathcal{L}$ with vanishing locus $D$, then $D$ is an effective Cartier divisor and $\mathcal{L} \cong \mathcal{O}_D$, so $\deg(\mathcal{L}) = \deg(D)$ by (5.11.2.6), so these are all simple now.

Prop. (5.11.2.9) [Riemann-Roch]. Let $D$ be a Weil divisor on a complete non-singular precurve $X$ of genus $g$, then

- If $l(D) = \dim_k H^0(X, \mathcal{L}(D))$, $l(D)$ is finite by (5.7.4.11).
- $[\omega_X]$ is an invertible sheaf by [Sta]0BFQ.
- $l(D) - l([\omega_X] - D) = \deg D + 1 - g$.
- $\deg(D) = \deg(\mathcal{L}(D))$

Notice when $X$ is smooth, $[\omega_X]$ is just $K_X(5.8.6.18)$.

Proof: 4 is equivalent to 3 by Serre duality (5.8.6.18), and 3 follows from (5.11.2.6).

Cor. (5.11.2.10). $\deg([\omega_C]) = 2g - 2$.

Proof: By (5.11.2.9) and Serre-duality (5.8.6.18),

$$\deg([\omega_C]) = h^0(X, [\omega_X]) - h^0(X, \mathcal{O}_X) + g - 1 = h^1(X, \mathcal{O}_X) - h^0(X, \mathcal{O}_X) + g - 1 = 2g - 2.$$

Prop. (5.11.2.11) [Twisting Sheaves]. Let $\mathcal{L}$ be a line bundle on a complete nonsingular precurve $C$, and $p \in C$ is a closed point of degree $d$, then $0 \leq h^0(\mathcal{L}) - h^0(\mathcal{L}(-p)) \leq d$ for any $\mathcal{L} \in \text{Pic}(C)$.

In particular, by (5.11.2.8), if $C$ is a complete non-singular curve, then $h^0(\mathcal{L}) \leq \deg L + 1$ for any $\mathcal{L} \in \text{Pic}(C)$. 

Proof: There is an exact sequence \( 0 \to \mathcal{O}_C(-p) \to \mathcal{O}_C \to \mathcal{O}_C|_p \to 0 \), tensoring with \( \mathcal{L} \) and taking the cohomology, we get an exact sequence
\[
0 \to h^0(\mathcal{L}, \mathcal{L}(-p)) \to h^0(\mathcal{L}, \mathcal{L}) \to H^0(C, \mathcal{L}|_p),
\]
and notice that \( h^0(C, \mathcal{L}|_p) = d \).

\[ \square \]

**Prop. (5.11.2.12)** [Riemann-Roch for High Degree \( D \)]. If \( \deg(D) \geq 2g - 1 \), then \( \deg([\omega_X] - D) < 0 \), so by \( (5.11.2.8) \), \( l([\omega_X] - D) = 0 \), thus \( l(D) = d - g + 1 \).

**Cor. (5.11.2.13)** [Characterizing \( [\omega_C] \)]. Any degree \( 2g - 2 \) divisor \( D \) satisfies \( l(D) = g - 1 \) or \( g \), and the latter case happens iff \( D = [\omega_C] \).

**Proof:** \( l([\omega_C] - D) = 1 \) iff \( [\omega_C] = D \) by \( (5.11.2.8) \).

\[ \square \]

**Def. (5.11.2.14)** [Special Divisors]. A special divisor on a complete non-singular curve is a divisor \( D \) that \( h^0([\omega_C] - D) > 0 \).

**Prop. (5.11.2.15).** For any complete smooth curve \( C \) of genus \( g > 1 \) over a field \( k \), there is a closed point on \( C \) of degree \( \leq 2g - 2 \). And if \( g \geq 2 \), we can assume this point is a geometric point.

**Proof:** The canonical sheaf \( K_C \) is a line bundle of degree \( 2g - 2 \) and \( h^0(K_C) = g \geq 1 \), so we can assume \( K_C \) is an effective divisor, then one of its support point has degree \( \leq 2g - 2 \).

For the last assertion, Cf. [Sta]0CD4.

**Vector Bundles**

**Prop. (5.11.2.16)** [Torsion-Free Sheaves]. Let \( C \) be a non-singular precurves over a field \( k \), then

- Any torsion-free coherent sheaf \( \mathcal{F} \) on \( C \) is locally free.
- Any \( \mathcal{F} \in \operatorname{Coh}(X) \) factors as \( 0 \to \mathcal{F}_{tor} \to \mathcal{F} \to \mathcal{F}_{lf} \to 0 \), where \( \mathcal{F} \) is a torsion sheaf \( (5.5.1.44) \) and \( \mathcal{F}_{lf} \) is \( \mathbb{Q} \)co and locally free, by \( (5.5.1.47) \)

**Proof:**

\[ \square \]

**Prop. (5.11.2.17) [Pic\(^0(C)\)].** For a smooth complete curve \( C \) over a field \( k \) with a rational point, \( \operatorname{Pic}^0(C) \) are exactly the set of line bundles of degree 0, by \( (13.5.13.1) \). In particular, there is an exact sequence
\[
0 \to \operatorname{Pic}^0(C) \to \operatorname{Pic}(C) \to \mathbb{Z} \to 0.
\]

**Prop. (5.11.2.18) [Torsion Elements].** Let \( C \) be a smooth complete curve of genus \( g \) over an alg. closed field, then for \( m \in \mathbb{Z} \cap k^* \), \( \operatorname{Pic}(C)[m] = \operatorname{Pic}^0(C) \cong (\mathbb{Z}/(m))^{2g} \).

**Proof:** This follows from \( (13.5.13.1)(5.11.2.17) \) and \( (13.5.6.14) \).

**Prop. (5.11.2.19).** If \( Z \to X \) is a closed immersion and \( \dim X \leq 1 \), then \( \operatorname{Pic} X \to \operatorname{Pic} Z \) is a surjection.

**Proof:** Use the exact sequence \( 0 \to (1 + t) \cap \mathcal{O}_X^* \to \mathcal{O}_X^* \to i_* \mathcal{O}_Z^* \to 0 \), \( \dim X \leq 1 \) and the Grothendieck vanishing theorem gives the desired result, also notice \( i \) is affine.

\[ \square \]
Ample Line Bundles

**Prop. (5.11.2.20).** A line bundle \( \mathcal{L} \) over a complete precurve \( C \) over a field \( k \) is ample iff \( \deg(\mathcal{L}) > 0 \).

**Proof:** If \( C \) is non-singular, the proof is easy: \( \mathcal{L} \) is ample iff \( \mathcal{L}^\otimes n \) is very ample for \( n \) large\(^{(5.5.4.22)} \). If \( \deg(\mathcal{L}) < 0 \), this cannot happen, by\(^{(5.11.2.8)} \). For \( \deg \mathcal{L} \geq 0 \), \( \mathcal{L}^\otimes n \) is very ample for \( n \) large by\(^{(5.11.2.26)} \).

In general, Cf.\([Vakil, P509]\)? □

**Cor. (5.11.2.21) [Ample and Nef Line Bundles].** Let \( \mathcal{L} \) be an invertible \( \mathcal{O}_X \)-module over a proper scheme of dimension \( \leq 1 \) over \( k \), let \( C_i \) be the integral components of \( X \) of dimension \( 1 \), then \( \mathcal{L} \) is a ample iff \( \deg(\mathcal{L}|_{C_i}) > 0 \) for all \( i \).

**Proof:** This follows from\(^{(5.5.4.14)} \) applied to the reduced structure of the irreducible components of \( X \), together with the fact a line bundle on an irreducible component \( \text{Spec} \ k(x) \) of dimension \( 0 \) is obviously ample. □

**Prop. (5.11.2.22).** Let \( \mathcal{L} \) be a line bundle on a complete non-singular precurve \( C \) of degree \( d \) that is basepoint-free, then it determines a morphism \( \pi : C \to \mathbb{P}^1_k \) of degree \( d \).

**Proof:** This follows from\(^{(5.11.1.44)} \). □

**Prop. (5.11.2.23).** Let \( C \) be a complete precurve over a field \( k \) with genus \( g > 0 \), and \( p, q \) are rational points on \( C \), then \( \mathcal{O}_C(p) \cong \mathcal{O}_C(q) \) iff \( p = q \), and \( h^0(C, \mathcal{O}_C(p)) = 1 \).

**Proof:** The hypothesis shows \( \mathcal{L} = \mathcal{O}_C(p) \) has degree \( 1 \) and is basepoint-free, thus defines a degree \( 1 \) map \( C \to \mathbb{P}^1_k \), which is an isomorphism, by\(^{(5.11.1.15)} \) and\(^{(5.11.1.17)} \), contradiction.

If \( h^0(C, \mathcal{O}_C(p)) \geq 2 \), then for any section \( s \), \( \text{div}(s) = q \) for some rational point \( q \), so by the above argument, \( q = p \), so any two such \( f \) is proportional. □

**Prop. (5.11.2.24).** Let \( C \) be a complete curve over a field \( k \) with genus \( g > 0 \), and \( \mathcal{L} \) is a line bundle of degree \( 2 \), then \( h^0(C, \mathcal{L}) \leq 2 \), and if the equality holds, then it is basepoint-free.

**Proof:** We can base change to \( \overline{k} \). \( h^0(C, \mathcal{L}) \leq 3 \) by\(^{(5.11.2.11)} \). If equality holds, then \( h^0(C, \mathcal{L}(-p)) = 2 \) for some \( p \), contradiction by\(^{(5.11.2.23)} \). If \( h^0(C, \mathcal{L}) = 2 \), then \( h^0(C, \mathcal{L}(-p)) < 2 \) for any \( p \), so it is basepoint-free. Conversely, if it is basepoint free, then \( \mathcal{L} \cong \mathcal{O}(p) \) for some rational point \( p \), and \( h^0(C, \mathcal{L}) = h^0(C, \mathcal{O}_C) + 1 = 2 \). □

**Prop. (5.11.2.25) [Criterion of Very Ample].** Let \( \mathcal{L} \) be a line bundle on a curve over an alg.closed field \( k \), then

- \( \mathcal{L} \) is basepoint-free iff \( h^0(\mathcal{L}) - h^0(\mathcal{L} - p) = 1 \) for any closed point \( p \in \mathcal{L} \).
- \( \mathcal{L} \) is very ample iff \( h^0(\mathcal{L}) - h^0(\mathcal{L} - p - q) = 2 \) for any closed points \( p, q \in \mathcal{L} \).

**Proof:** Cf.\([Vakil, P509]\)? □

**Cor. (5.11.2.26).** Any line bundle \( \mathcal{L} \) on a complete non-singular curve of genus \( g \) that \( \deg(\mathcal{L}) \geq 2g \) is basepoint-free, and if \( \deg(\mathcal{L}) \geq 2g + 1 \), then it is very ample.

**Proof:** When \( k = \overline{k} \), this follows from\(^{(5.11.2.25)} \) and Riemann-Roch\(^{(5.11.2.9)} \). For general \( k \), use the fact being basepoint-free, closed embedding and degree are all stable and reflective under base change of fields\(^{(5.11.2.2)}(5.5.3.3)(5.1.5.26) \). □
**Proposition (5.11.2.27) [Very Ample Line Bundles]**. Let $X$ be a complete curve over a field $k$, then
- If $\mathcal{L}$ is effective and $H^1(X, \mathcal{L}) = 0$, then $\mathcal{L}^{\otimes 6}$ is very ample.
- If $\mathcal{L}$ is globally generated and $H^1(X, \mathcal{L}) = 0$, then $\mathcal{L}^{\otimes 2}$ is very ample.

**Proof**: Cf. [Sta] 0E8V, 0E8W. \(\square\)

**Curves in Low Dimension**

**Proposition (5.11.2.28) [Projection Along a Point]**. Let $C \subset \mathbb{P}^n_k$ be a non-singular precurve, then for any rational point $p \in C$, there is a projection along $p$ map $v_p : C \to \mathbb{P}^{n-1}_k$ that is the projection along $p$ for $q \in C \setminus \{p\}$, and extend to whole $C$ by (5.11.15), which corresponds to the line bundle $\mathcal{O}_C(1)(-p)$.

**Proposition (5.11.2.29)**. Let $C$ be a smooth plane precurve of degree $e > 2$ and $D_1, D_2$ are two polynomials of degree $d$ not vanishing on $C$. Suppose there is a divisor $E$ on $C$ of degree $de - 1$ and rational points $p_i$ on $C$ that $D_i|_C = E + p_i$, then $\mathcal{O}_C(-E)$ is not base-free.

**Proof**: Notice by genus formula $g > 0$, and $\mathcal{O}_C(-E) \cong \mathcal{O}_C(p_i)$ has degree 1, then $p_1 = p_2$ by (5.11.2.23). \(\square\)

**Proposition (5.11.2.30)**. Let $C$ be a smooth conic plane curve over a field of characteristic $\neq 2$, show the dual variety of $C$ is also a smooth conic. In particular, for a general point in the plane, there are two tangents to $C$. (This can be also proved using Riemann-Hurwitz by projection through this point).

**Proof**: \(\square\)

**Proposition (5.11.2.31)**. The number of plane conics containing $i$ generally chosen points and $5 - i$ generally chosen lines is $1, 2, 4, 4, 2, 1$ resp. for $i = 0, 1, \ldots, 4, 5$. (The duality comes from the duality between the conic and the dual conic (5.11.2.30)).

**Proof**: \(\square\)

**Proposition (5.11.2.32) [Curves in $\mathbb{P}^1 \times \mathbb{P}^1$]**. Let $C$ be a curve in $\mathbb{P}^1 \times \mathbb{P}^1$ given by a bi-homogenous polynomial of type $(a, b)$. Then $g(C) = (a - 1)(b - 1)$.

**Proof**: We have $K_C = (K_{\mathbb{P}^1 \times \mathbb{P}^1} + C)|_C$ (5.10.1.17). We have $\text{Pic}(\mathbb{P}^1 \times \mathbb{P}^1) \cong \mathbb{Z}H_1 \oplus \mathbb{Z}H_2$, thus

$$\deg(K_C) = \deg((K_{\mathbb{P}^1 \times \mathbb{P}^1} + C)|_C)$$

$$= \deg((-2H_1 - 2H_2 + aH_1 + bH_2)|_C)$$

$$= \deg(((a - 2)H_1 + (b - 2)H_2)|_C)$$

$$= (a - 2)b + (b - 2)a = 2ab - 2a - 2b$$

$$= 2g - 2.$$

Thus $g = (a - 1)(b - 1)$.

? For non-smooth case, see AG psets. \(\square\)

**Proposition (5.11.2.33) [Genus Formula]**. Let $C$ be a closed subscheme of $\mathbb{P}^2_k$ defined by a homogenous polynomial $f(x_0, x_1, x_2)$ of degree $d$, then it has arithmetic genus $p_a(C) = (d - 1)(d - 2)/2$. 

? For non-smooth case, see AG psets. \(\square\)
5.11. CURVES

**Proof:** This follows from (5.7.2.4). □

**Cor. (5.11.2.34).** Let $C$ be a complete smooth plane curve of degree $d$, then it has genus $g = (d-1)(d-2)/2$.

**Proof:** Alternative proof: By adjunction formula, $\mathcal{K}_C = \mathcal{K}_{\mathbb{P}^2}(C)|_C = \mathcal{O}_C(d-3)$ which has degree $d(d-3)$. But this also equals $2g - 2(5.11.2.10)$, thus $g = (d-1)(d-2)/2$. □

**Prop. (5.11.2.35)** [Cubic Curves in $\mathbb{P}^3$]. A twisted cubic (rational) $C$ in $\mathbb{P}^3$ is contained in a quadric.

**Proof:** Calculate that $h^0(\mathcal{O}_{\mathbb{P}^3}(2)) = C^2 = 10$ and $\deg(\mathcal{O}_C(2)) = 6$, thus $h^0(\mathcal{O}_C(2)) = 6 + 1 = 7$ by Riemann-Roch. Then $C$ is contained in 3 quadrics. □

3 Singularity and $\delta$-Invariants

**Def. (5.11.3.1)** [Different Kinds of Singularities]. Let $X$ be a curve over an alg. closed field $k$, a point $p \in X$ is called a

- **node** if the completion of $\mathcal{O}_{X,p}$ at $m_{X,p}$ is isomorphic to $k[[x,y]]/(xy)$ as topological local rings.
- **cusp** if the completion of $\mathcal{O}_{X,p}$ at $m_{X,p}$ is isomorphic to the completion of $k[x,y]/(x^2 - y^3)$ at $(x,y)$.
- **tacnode** if the completion of $\mathcal{O}_{X,p}$ at $m_{X,p}$ is isomorphic to the completion of $k[x,y]/(x^2 - y^4)$ at $(x,y)$.
- **triple point** if the completion of $\mathcal{O}_{X,p}$ at $m_{X,p}$ is isomorphic to the completion of $k[x,y]/(x^3 - y^3)$ at $(x,y)$.

**Def. (5.11.3.2)** [$\delta$-Invariants].

4 Linear Series

**Def. (5.11.4.1)** [Moduli Spaces]. Define the Hilbert scheme $\mathcal{H}_{d,g,r} = \{\text{Curves } C \text{ of degree } d \text{ and genus } g\}$.

Define the moduli space of curves $\mathcal{M}_g = \{\text{isomorphism classes of smooth projective curves of genus } g\}$.

Define $W^r_d(C) = \{L \in \text{Pic}^d(C), h^0(L) \geq r + 1\}$.

**Def. (5.11.4.2)** [Linear Series]. A linear series is a line bundle $L$ together with a vector space $V \subset H^0(L)$.

A $g^r_d$ is a line bundle $L$ together with a vector space $V \subset H^0(L)$ of dimension $r + 1$.

For a line bundle $\mathcal{L}$, denote by $|L|$ the linear series $(L, H^0(L))$.

**Cor. (5.11.4.3)** [$r \leq d$]. If $g^r_d$ exists on a complete curve $C$, then $r \leq d$. And if $r = d$, then $g(C) = 0$.

**Proof:** Let $s$ be a section of $\mathcal{L}$, then the vanishing locus of $s$ is an effective Cartier divisor $D$, $\mathcal{L} \cong \mathcal{L}(D)$, and there is an exact sequence

\[0 \to \mathcal{O}_X \to \mathcal{L} \to \mathcal{L}|_D \to 0.\]

As $D$ is an Artinian scheme, $\mathcal{L}|_D$ is trivial as $D$ is discrete, so by (5.11.2.6), $h^0(\mathcal{L}|_D) = \deg(D)$, and $h^0(X, \mathcal{O}_X) = 1$, so $r = h^0(X, \mathcal{L}) \leq d.$
If the equality holds, then \( H^0(X, \mathcal{L}) \to H^0(X, \mathcal{L}|_D) \) is surjective, so to show \( g(C) = 0 \), it suffices to show that \( h^0(X, \mathcal{L}) = 0 \). As \( \mathcal{L}|_D \) is trivial, there is a section \( t \) of \( \mathcal{L} \) that generate \( \mathcal{L}|_D \). Consider the exact sequence
\[
0 \to \mathcal{L} \to \mathcal{L}^2 \to \mathcal{L}^2|_D \to 0,
\]
\( H^0(X, \mathcal{L}^2) \to H^0(X, \mathcal{L}|_D) \) is surjective because \( \sigma \otimes t \) is mapped to \( \sigma \). Then by (5.11.2.5),
\[
h^0(X, \mathcal{L}^2) = 2r + 1 = \deg(\mathcal{L}^2) + 1.
\]
So we may replace \( \mathcal{L} \) by arbitrarily large powers of \( \mathcal{L} \). Now \( \mathcal{L} \) is ample by (5.11.2.20), so for \( r \) large, \( H^1(X, \mathcal{L}^r) = 0 \).

**Prop. (5.11.4.4) [Linear Series and Maps].** For any \( g_d^r(L, V) \) on a non-singular precurve \( C \), there is a map \( \varphi : C \to \mathbb{P}^r \) and a map \( \varphi^*\mathcal{O}_{\mathbb{P}^r}(1) \to \mathcal{L} \) s.t. the coordinates \( T_0, \ldots, T_r \) are mapped to a basis of \( V \).

This map is injective iff for any \( p \neq q \), \( V_{p+q} \) has codimension 2. This map is an immersion iff for all \( p \), \( V_{2p} \) has codimension 2. So in particular, this map is an embedding iff for any effective divisor \( D \) of degree 2, \( V_D \) has codimension 2.

**Proof:** Take a basis \( s_0, s_1, \ldots, s_r \in V \), as \( C \) is non-singular, the image of the map \( (s_0, \ldots, s_r) : \mathcal{O}_X^{r+1} \to \mathcal{L} \) is an invertible sheaf as it is torsion-free. Then take the corresponding embedding induced by (5.5.2.4).

**Cor. (5.11.4.5).** If \( \mathcal{L} \) is a very ample line bundle of degree \( d \) on a curve \( C \), then \( \varphi_{|\mathcal{L}|} \) embeds \( C \) as a closed subscheme of degree \( d \).

**Proof:** Use (5.11.4.4), The pullback of \( \mathcal{O}_{\mathbb{P}^r}(1) \) under \( \varphi \) is just \( \mathcal{L} \), so the assertion follows from (5.11.2.7).

**Lemma (5.11.4.6).** Let \( \mathcal{L} \in \text{Pic}^d(C) \) be general, then \( h^0(\mathcal{L}) = \max\{1, d - g + 1\} \).

**Proof:** If \( D = \sum p_i \) is a general effective divisor, notice \( h^0(K) = g \), \( h^0(K - p_1) = g - 1 \), \( h^0(K - p_1 - p_2) = g - 2 \), and repeating this, we get \( h^0(K - D) = \max\{0, g - d\} \), when we choose \( p_i \) that are as independent as possible (any section has f.m. zeros). Then by Riemann-Roch, \( l(D) = d - g + 1 + \max\{0, g - d\} = \max\{1, d - g + 1\} \). As every divisor of degree \( d \geq g \) is effective, this settles the \( d \geq g \) case.

If \( D \) is non-effective and \( d \leq g - 1 \), we need to show \( W^0_d \) is not dominant in \( \text{Pic}^d \). But \( J \) has dimension \( g \) by ?? and \( W^0_d \) has dimension at most \( d \), so this is true.

**Prop. (5.11.4.7).** Suppose \( D \) is a divisor of degree \( g + 3 \), then for \( D \) general, \( \varphi_D = \varphi_{|\mathcal{L}(D)|} \) is an embedding.

**Proof:** By (5.11.4.6), for a general \( D \), \( l(D) = 4 \). Thus \( \varphi_D \) being not an embedding is equivalent to the existence of a divisor \( D_0 = p + q \) that \( l(D - D_0) \geq 3 \). This means \( D - D_0 \in W^2_{g+1} = K - W^0_{g-3} \). So the divisor \( D = D_0 + (D - D_0) \in W^2_{g+1} + (K - W^0_{g-3}) \) which has dimension at most \( 2 + (g - 3) = g - 1 \). But a general divisor \( D \) doesn’t lie on this \( g - 1 \)-dimensional subvariety by (13.5.13.10), so a general \( D \) defines an embedding \( \varphi_D \).

**Def. (5.11.4.8) [Canonical Map].** For a smooth curve \( C \) of degree \( g \) over a field \( k \) of genus \( g \geq 1 \), the canonical divisor \( K_C \) is basepoint-free, and defines a canonical map to \( \mathbb{P}^{g-1}_k \).
5.11. CURVES

Proof: By (5.11.2.2)(5.5.3.3)(5.1.5.26), it suffices to prove for $\overline{\mathbb{C}}$, thus for any closed point $p$, $h^0(K_C-p) = 2g - 3 - g + 1 + h^0(O_C(p)) \leq g - 1 < h^0(K_C) = g$ by (5.11.2.23), so it is basepoint-free. □

Prop.(5.11.4.9)[Base-Free Pencil Trick]. Let $\mathcal{L}, \mathcal{M}$ be line bundles on $C$. Let $s_1, s_2$ be sections of $H^0(\mathcal{L})$ without common zero, then the kernel of the map

$$s_1 H^0(\mathcal{M}) \oplus s_2 H^0(\mathcal{M}) \to H^0(\mathcal{L} \otimes \mathcal{M})$$

is $H^0(\mathcal{M} \otimes \mathcal{L}^{-1})$.

Proof: Indeed, there is an exact sequence of sheaves:

$$\mathcal{M} \otimes \mathcal{L}^{-1} \to \mathcal{M} \oplus \mathcal{M} \xrightarrow{(s_1, s_2)} \mathcal{M} \otimes \mathcal{L} \to 0.$$ 

Where the first map maps a section $t$ to the pair $(ts_2, -ts_1)$. This is a Koszul regular sequence (on a common trivialization $U$ of $\mathcal{M}, \mathcal{L}$, $s_1, s_2 \in C(U)$, thus this is just $0 \to A \to A \oplus A \xrightarrow{s_1, s_2} A \to 0$). Taking the global section functor gives the desired result. □

Prop.(5.11.4.10)[Geometric Riemann-Roch]. Let $C$ be a non-hyperelliptic curve of genus $g \geq 2$. Then the canonical map $\varphi_K$ is an embedding, so we can assume $C \subset \mathbb{P}^{g-1}$. Then for a divisor $D = \sum p_i$,

$$r(D) = d - 1 - \dim \mathcal{D},$$

where $\mathcal{D}$ is the linear subspace generated by $p_i$. Thus $r(D)$ can be interpreted as the number of linear relations between $p_i$.

Proof: By the definition of the canonical embedding, $l(K-D)$ is just the dimension of hypersurfaces containing $p_i$, thus it is equal to $g-1-\dim \mathcal{D}$. Now by Riemann-Roch, $r(D) = d-g+l(K-D) = d-g+g-1-\dim \mathcal{D} = d-1-\dim \mathcal{D}$. □

Prop.(5.11.4.11).

Cor.(5.11.4.12)[Special Divisors]. Let $U^{(g)}$ be the open subscheme of $C^{(g)}$ corresponding to the set of non-special divisors of degree $g$.

Proof:

□

Prop.(5.11.4.13)[Clifford Theorem]. For a divisor $D$ of degree $0 \leq d \leq 2g-2$ on a curve of genus $g$,

$$r(D) \leq \frac{d}{2},$$

with equality iff one of the following holds:

- $r = d = 0, D = 0$.
- $d = 2g - 2, r = g - 1, D = K_C$.
- $C$ is hyperelliptic and $D = mg_2^1$.

Proof: Cf.[Algebraic Curves, Harris, P32]. □
5 Hyperelliptic Curves

Def. (5.11.5.1) [Hyperelliptic Curves]. A hyperelliptic curve over $k$ is a complete non-singular curve $C$ together with a finite degree 2 map $C \to \mathbb{P}^1_k$. Such a map is called a hyperelliptic map. For $g > 0$, this is equivalent to the existence of a $g^2$ on $C$ (such a linear series must be basepoint-free, by (5.11.2.24)).

Cor. (5.11.5.2) [Genus 2 Curves are Hyperelliptic]. Any complete nonsingular curve of genus 2 is hyperelliptic, because $K_C$ has degree 2 and $h^0(K_C) = 2(5.11.2.10)$.

Prop. (5.11.5.3) [Equation of Hyperelliptic Curves]. Any image of a hyperelliptic map from a hyperelliptic curve of genus $g$ over an alg.closed field $k$ of characteristic $k \neq 2$ is isomorphic to the projective curve that is the completion (5.11.1.18) of the affine curve in $\mathbb{A}^2$ defined in an affine chart by $y^2 = \prod_{i=0}^{2g+2}(x - \alpha_i)$ or $y^2 = \prod_{i=0}^{2g+1}(x - \alpha_i)$, depending on whether the $\infty$ is branched or not. And given 2g + 2 points in $\mathbb{P}^1_k$, there is exactly one degree 2 covering of $\mathbb{P}^1$ branched over these points.

Proof: Given any $r$ points of $\mathbb{P}^1_k$, we can use a transformation of $\mathbb{P}^1$ to assume that all branch points are finite, denoted by $\alpha_1, \ldots, \alpha_r$. Consider the curve $C'$ defined by $y^2 = \prod_{i=0}^{2g+2}(x - \alpha_i)$, then it is a smooth curve by Jacobian criterion. Now let $C$ be the smooth model of $C'$, and consider $\pi : C \to \mathbb{P}^1$ by projecting to the $x$-coordinates and extend to the whole $C$ by (5.11.1.15). This is finite separable of degree 2, and $\pi$ is simply branched at the points $\alpha_i$, and simply branched over $\infty$ if $r$ is odd, thus it has genus $\left\lfloor \frac{r-1}{2} \right\rfloor$ by Riemann-Hurwitz (5.11.1.32).

Conversely, by Riemann-Hurwitz (5.11.1.32), any degree 2 covering of $\mathbb{P}^1$ has 2g + 2 branch points, because the branch points must be simply branched. The map $k(x) \to k(C)$ is Galois of degree 2, take a $y \in k(C)$ that $\sigma(y) = -y$, then $y^2 = g \in k(x)$. We can modify $y$ s.t. $g$ is a monic polynomial with no repeated factors. Then it is of the form $g(x) = \prod_{i=1}^r(x - x_i)$. Then it is isomorphic to the curve constructed above, and branched over $x_1, \ldots, x_r$ and possibly $\infty$. In particular, it is determined by the set of branched points, so we get the desired assertion. □

Rem. (5.11.5.4). The completion of $C$ can be explicitly constructed, by gluing another affine chart defined by $(y^2) = \prod_{i=0}^{2g+2}(1 - \alpha_i \frac{1}{x})$ or $(y^2) = \frac{1}{x} \prod_{i=0}^{2g+1}(1 - \alpha_i \frac{1}{x})$.\n
Prop. (5.11.5.5). If $C$ is a nonsingular complete curve of genus $g \geq 2$ over $k$ and $\mathcal{L}$ is a line bundle that corresponds to a hyperelliptic map $C \to \mathbb{P}^1_k$, then $\mathcal{L}^{\otimes(g-1)} \cong K_C$.

In particular, the image of $C$ under the canonical map is the rational curve in $\mathbb{P}^{g-1}_k$.

Proof: Consider the composition of the hyperelliptic map and the Veronese map

$$C \xrightarrow{[\mathcal{L}]} \mathbb{P}^1_k \xrightarrow{\nu_{g-1}} \mathbb{P}^{g-1}_k,$$

which corresponds to the line bundle $|\mathcal{L}^{\otimes(g-1)}|$. This line bundle has degree $2g - 2$, and the map $H^0(\mathbb{P}^{g-1}, \mathcal{O}(1)) \to H^0(C, \mathcal{L}^{\otimes(g-1)})$ is injective, because the Veronese map is non-degenerate. Thus $h^0(\mathcal{L}^{\otimes(g-1)}) \geq g$, thus isomorphic to $K_C$, by (5.11.2.13). Hence this map is just the canonical map. □

Cor. (5.11.5.6). For a hyperelliptic curve, the smallest degree of an embedding $C \to \mathbb{P}^r$ is $g + r$. Note that hyperelliptic curves cannot be embedded into $\mathbb{P}^2$, i.e. smooth plane curves are non-hyperelliptic.
Proof: Firstly we show a special divisor cannot induce an embedding: A special divisor is a divisor that is contained in a hypersurface intersection of \( C \) under the canonical map, thus by geometric Riemann-Roch (5.11.4.10), \( r(D) \) is just the number of points of \( D \) mapped to the same point under the canonical map, because intersection with the rational normal curve are all linearly independent. Now this means \( D \) contains \( g_2^1 \), so \( \varphi_D \) factors through \( \pi \), thus not an embedding. \( \square \) Cf. [Algebraic Curves, Harris, P21].

Prop. (5.11.5.7) [Hyperelliptic and Canonical Map]. A complete smooth curve of genus \( g \geq 1 \) is hyperelliptic iff the canonical map (5.11.4.8) is not a closed embedding.

Proof: The canonical map is not an embedding iff there exists an effective divisor \( D \) of degree 2 that \( l(K - D) > l(K) - 2 \). Now \( l(K - D) = 2g - 4 - g + 1 + l(D) \), so this is equivalent to \( l(D) > 1 \), which is equivalent to a \( g_2^1 \), which is equivalent to hyperelliptic (5.11.5.1). \( \square \)

Prop. (5.11.5.8) [Uniqueness of Hyperelliptic Maps]. For a hyperelliptic curve of genus \( g \geq 2 \), up to automorphic of \( \mathbb{P}^1 \), there are at most one hyperelliptic map, or equivalently there is exactly one \( g_2^1 \) on \( C \).

But for (hyperelliptic) curve of genus 1, thus is not unique: any divisor of degree 2 is effective, but they are not unique, because Pic\(^2\)(\( C \)) \( \cong J(C)(13.5.13.10) \).

Proof: If \( \mathcal{L} \neq \mathcal{M} \) are two line bundles on \( C \) with \( h^0 = 2 \), then \( h^0(\mathcal{L} \otimes \mathcal{M}) \geq 4 \) by base-free pencil trick (5.11.4.9), and in fact \( h^0(\mathcal{L} \otimes \mathcal{M}) = 4 \) by (5.11.4.3). Now we can turn the same argument again to \( \mathcal{L} \) and \( \mathcal{L} \otimes \mathcal{M} \), to show that \( h^0(\mathcal{L}^2 \otimes \mathcal{M}) = 6 \). And inductively \( h^0(\mathcal{L}^n \otimes \mathcal{M}) = 2n + 2 \). But then for \( n \) large, Riemann-Roch shows \( 2n + 2 = 2n + 2 - g + 1 \), thus \( g = 1 \), contradiction. \( \square \)

Gonal Curves

Def. (5.11.5.9) [Gonal Curves]. A trignal curve is a complete non-singular curve \( C \) with a degree 3 map \( C \to \mathbb{P}^1 \). Similarly, a \( k \)-gonal curve is a complete non-singular curve \( C \) with a degree \( k \) map \( C \to \mathbb{P}^1 \). Being \( k \)-gonal is equivalent to having a basepoint-free \( g_1^k \).

Notice also for non-hyperelliptic curves, any \( g_1^3 \) must be basepoint-free.

Def. (5.11.5.10) [Hurewitz Spaces]. Let the Hurewitz space be

\[
\mathcal{H}_{d,g} = \{(C, f)| C \in \mathcal{M}_g, f : C \to \mathbb{P}^1 \text{ of degree } d \text{ with simple branching}\}.
\]

In particular, \( \mathcal{H}_{2,g} \) is just the space of hyperelliptic curves together with a hyperelliptic map.

Prop. (5.11.5.11) [Dimension of Hurewitz Spaces], \( \dim \mathcal{H}_{d,g} = 2d + 2g - 2 \).

Proof: Let \( b = 2d + 2g - 2 \), then the branch divisor will consist of an unordered \( b \)-tuple of distinct points. Then we obtain a map \( \mathcal{H}_{d,g} \to \mathbb{P}^b \setminus \Delta \), where we regard \( \mathbb{P}^b \) as the set of polynomials of degree \( b \) and \( \Delta \) the determinant, and the fiber is finite by cut-paste technique. \( \square \)

Cor. (5.11.5.12) [Dimension of Moduli Space of Curves]. \( \dim \mathcal{M}_g = 3g - 3 \).

Proof: There is a map \( \mathcal{H}_{d,g} \to \mathcal{M}_g \). When \( d \) is large, we can analyze the fiber of this map, that is, given a curve of genus \( g \), how many simply branched maps \( C \to \mathbb{P}^1 \) of degree \( d \) are there? Such a map is equivalent to a line bundle of degree \( d \) and a pair of base free sections \( \sigma_0, \sigma_1 \in H^0(L) \). The base-free condition is an open condition, thus the dimension of the fiber is \( g + 2(d - g - 1) - 1 = 2d + g - 1 \). Thus the dimension of \( \mathcal{M}_g = 2d + 2g - 2 - (2d - g + 1) = 3g - 3 \). \( \square \)
Cor. (5.11.5.13). The space of hyperelliptic curves has dimension $2g - 1$.

Proof: $H_{2g}$ has dimension $2g + 2$, and for any hyperelliptic curve, there is exactly one hyperelliptic map up to automorphism of $P^1$, by (5.11.5.8), thus the space of hyperelliptic curves has dimension $2g + 2 - 3 = 2g - 1$. □

Cor. (5.11.5.14). If $g \geq 3$, then not all curves of genus $g$ is hyperelliptic.

Proof: Because when $g \geq 3$, $2g - 1 < 3g - 3$. □

Lemma (5.11.5.15). For a line bundle of degree 3 on a curve of genus $g \geq 3$, $h^0(L) \leq 2$, by Clifford’s theorem (5.11.4.13). Thus a trinodal map must be associated to a complete linear series $g^3_3$.

Prop. (5.11.5.16) [Hyperelliptic are not Trigonal]. A curve of genus $g \geq 3$ cannot be both hyperelliptic and trigonal.

Proof: Suppose there are two basepoint-free line bundles $\mathcal{L}, \mathcal{M}$ of degree 2 and 3 on $C$ that $h^0(\mathcal{L}) = h^0(\mathcal{M}) = 2 (5.11.5.15)$, then the base-free pencil trick (5.11.4.13) implies that $h^0(\mathcal{M} \otimes \mathcal{L}) \geq 4$. If $g = 3$, then this contradicts Riemann-Roch. If $g \geq 4$, then this contradicts Clifford’s theorem (5.11.4.13). □

Prop. (5.11.5.17) [Genus 3 Curves are Hyperelliptic or Trigonal]. Any genus 3 non-hyperelliptic complete smooth curve $C$ with a rational point is trigonal.

Proof: If $C$ is non-hyperelliptic, then the canonical map realizes $C$ as a plane curve of degree 4 (5.11.8.6), thus the projection of $C$ along a point on $C$ induces a map $C \to P^1$. This map is finite of degree 3 because it is non-constant as $C$ is non-degenerate, and has degree 3, by (5.11.2.28). □

Prop. (5.11.5.18) [Uniqueness of Trigonal Divisors]. There exists at most one $g^1_3$ on a curve of genus $g \geq 5$.

Proof: If $\mathcal{L} \neq \mathcal{M}$ are two base free line bundles of degree 3 that $h^0 = 2$, then we can use base-free trick to show that $h^0(\mathcal{L} \otimes \mathcal{M}) = 4$. But this contradicts Clifford’s theorem (5.11.4.13). Notice the equality cannot hold, because the degree is too low to be the canonical bundle, and also $C$ cannot be both hyperelliptic and trigonal (5.11.5.16). □

6 Castelnuovo’s Theory

Lemma (5.11.6.1) [Castelnuovo’s Lemma]. Let $\Gamma \in P^n$ be a configuration of $d \geq 2n + 3$ points in linear general position, and if $h_\Gamma(2) = 2n + 1$, then $\Gamma$ lies in a rational normal curve.

7 Plucker Formulas

Def. (5.11.7.1) [Weierstrass Group]. Let $C$ be a smooth of genus $g \geq 2$, $p \in C$, then $S_p = \{-\text{ord}_p(f)|f \in H^0(\mathcal{O}_C(-p))\}$ is a semigroup, called the Weierstrass semigroup of $p \in C$. And the gap sequence is $\mathbb{N}\backslash S_p$, which is the set of orders of pole of $p$ that doesn’t occur.

Lemma (5.11.7.2). We have $|G_p| = g$.

Proof: Notice that

$G_p = \{m : h^0(mp) = h^0((m - 1)p)\}, \quad S_p = \{m : h^0(mp) = h^0((m - 1)p) + 1\}$

and we know by (5.11.2.12) that $h^p(mp) = m - g + 1$ for $m$ large, thus there are exactly $g$ jumps, which shows $|G_p| = g$. □
Def.(5.11.7.3)[Weierstrass Points]. A point \( p \in C \) is called \textbf{Weierstrass point} if the gap sequence is not \( \{1, 2, \ldots, g\} \). It is called a \textbf{hyperelliptic Weierstrass point} if \( G_p = \{1, 3, \ldots, 2g - 1\} \), and is called a \textbf{normal Weierstrass point} if \( G_p = \{1, 2, 3, \ldots, g - 1, g + 1\} \).

Define the \textbf{weight} of the \( p \in C \) to be the sum \( w(p) = \sum_{i \leq g} (a_i - i) \), where the gap sequence is numbered \( \{a_1, \ldots, a_g\} \).

Prop.(5.11.7.4). For any compact Riemann surface \( C \), \( \sum_{p \in C} w(p) = g(g - 1)(g + 1) \).

Proof: Cf.[G-H78], P274. \( \square \)

Cor.(5.11.7.5). For general \( p \in C \), \( G_p = \{1, 2, \ldots, g\} \).

Prop.(5.11.7.6) [Hyperelliptic Weierstrass Points]. If \( C \) is hyperelliptic defined by \( y^2 = \prod_{i=0}^{2g+1} (x - \alpha_i) \), then there are \( 2g + 2 \) branching point of \( x \), where \( S_p = \{0, 2, 4, \ldots, 2g, 2g + 1, \ldots\} \).

In this way, \( w(p) = g(g - 1)/2 \). Thus there are \( 2g + 2 \) Weierstrass points, and these are all of them.

If \( C \) is non-hyperelliptic, then by Clifford’s theorem(5.11.4.13),

\[
h^0(kp) < \frac{k}{2} + 1, \ k = 1, \ldots, g
\]

Thus \( h^0((a_i - 1)p) < \frac{a_i - 1}{2} + 1 \), and \( h^0((a_i - 1)p) = 1 + (a_i - 1) - (i - 1) \). Thus we get

\[
a_i \leq 2i - 2, \ i = 2, \ldots, g.
\]

Then \( w(p) \leq \sum_{i=2}^g (i - 2) = \frac{(g-1)(g-2)}{2} \). Thus there are at least

\[
\frac{2g(g - 1)(g + 1)}{(g - 1)(g - 2)} \geq 2g + 6
\]

Weierstrass points.

To sum up, there are no less than \( 2g + 2 \) Weierstrass points, and there are exactly \( 2g + 2 \) Weierstrass points iff \( C \) is hyperelliptic.

Prop.(5.11.7.7). A generic Riemann surface of genus \( g \geq 3 \) has no automorphisms.

8 Curves of Low Genus

In this subsection complete smooth curves of low genus are considered.

Prop.(5.11.8.1)[Genus 0 Curve]. All smooth complete curve \( C \) of genus 0 is isomorphic to a plane conic.

Proof: The curve has a degree 2 line bundle \( K_C \), thus by Riemann-Roch \( h^0(\mathcal{O}(p)) = 3 \) and by(5.11.2.26) it induces a closed embedding of \( C \) into \( \mathbb{P}^2 \) of degree 2, thus it is a plane conic. \( \square \)

Prop.(5.11.8.2). A nonsingular curve \( C \) of genus 0 with a \( k \)-rational point \( p \) is isomorphic to \( \mathbb{P}^1_k \).

Proof: By Riemann-Roch, \( h^0(\mathcal{O}(p)) = 2 \) and \( \deg \mathcal{O}(p) = 1 \), thus by(5.11.2.26), \( \mathcal{O}(p) \) defines a closed embedding of \( C \) into \( \mathbb{P}^1 \), which must be an isomorphism. \( \square \)
Prop. (5.11.8.3) [Genus 1 Curve]. By (5.11.2.26), an effective divisor of degree 3 induces an embedding of \( \mathbb{C} \) into \( \mathbb{P}^2 \). So it is a smooth plane cubic by genus formula (5.11.2.33). Conversely, any smooth plane cubic has genus 1.

Similarly, if we take an effective divisor of degree 4, then it gives an embedding \( C \rightarrow \mathbb{P}^3 \). We know that \( h^0(\mathcal{O}_{\mathbb{P}^3}(2)) = 10 \) and \( h^0(\mathcal{O}_C(2)) = 8 \), so \( C \) is contained in 2 quadrics. Then \( C \) is the intersection of these two quadrics, by Bezout’s theorem.

Prop. (5.11.8.4) [Genus 2 Curves and Degree 4 Divisors]. Let \( C \) be a curve of genus 2, and \( D \) a divisor of degree 4. Then \( l(D - K_C) = 1 + l(2K_C - D) \geq 1 \), thus \( D - K_C \) is effective. Let \( D - K_C = p + q \). Then \( \varphi_D \) maps \( p, q \) to the same point.

There are two situations, firstly if \( D \neq 2K_C \), then \( D - K_C \) can be written uniquely as \( p + q \). Then the image of \( \varphi_D \) is a degree 4 curve with a node (if \( p = q \)) or a cusp (if \( p = q \)). Counting genus, this has exactly arithmetic genus 2.

If \( D = 2K_C \). Then notice \( \varphi_{2K_C} \) is equal to \( \varphi_K \) followed by the normal curve map \( \mathbb{P}^1 \rightarrow \mathbb{P}^2 \).

This is because if \( \omega_1, \omega_2 \) are a basis of \( H^0(K_C) \), then \( \omega_1^2, \omega_1\omega_2, \omega_2^2 \) is a basis of \( H^0(K_C^2) \). So \( \varphi_D \) is a 2 to 1 map to a rational normal curve in \( \mathbb{P}^2 \).

Prop. (5.11.8.5) [Genus 2 Curve and degree 5 Divisors]. Let \( C \) be a curve of genus 2 and \( D \) a divisor of degree 5, then \( \varphi_D : C \rightarrow \mathbb{P}^3 \) embeds \( C \) as a degree 5 curve, by (5.11.2.26).

Notice \( h^0(\mathcal{O}_{\mathbb{P}^3}(2)) = 10 \) and \( h^0(\mathcal{O}_C(2)) = 10 - 2 + 1 = 9 \), thus \( C \) lies on at least one quadric \( Q \). And it can in fact lie on only one quadric, because if it lies on two quadrics, then \( C \) is the intersection, and can have degree at most 4.

Next, notice \( h^0(\mathcal{O}_{\mathbb{P}^3}(3)) = 20 \) and \( h^0(\mathcal{O}_C(3)) = 15 - 2 + 1 = 14 \), so \( C \) lies on at least 6 cubics. Without the 4 cubics containing the quadric, there are still at least 2 new cubics. Let \( S \) be such a cubic, then \( S \cap Q \) is a curve of degree 6, so \( S \cap Q = C \cup L \), where \( L \cong \mathbb{P}^1 \).

Prop. (5.11.8.6) [Genus 3 Non-Hyperelliptic Curve]. For any non-hyperelliptic smooth curve \( C \) of genus 3 over a field \( k \), the canonical map (5.11.4.8) embeds \( C \) as a smooth quartic curve in \( \mathbb{P}^2 \). This induces an isomorphism of smooth quartic plane curves up to automorphism of \( \mathbb{P}^2 \).

Proof: The canonical embedding is a closed embedding by (5.11.5.7). For the last assertion, any plane curve of degree 4 has genus 3 by (5.11.2.33), and the sheaf \( \mathcal{O}_C(1) \) has degree 4 and 3 sections, thus by (5.11.2.13), so this comes from a canonical embedding. In particular, any such curve can be embedded in \( \mathbb{P}^2 \) in a unique way.

Prop. (5.11.8.7). Any hyperelliptic smooth curve of genus 3 is a flat limit of non-hyperelliptic smooth curves of genus 3.

Proof: Cf. [Vak17]P520.

Prop. (5.11.8.8) [Genus 4 Non-Hyperelliptic Curves]. Any non-hyperelliptic smooth complete canonical curve \( C \) of genus 4 is a complete intersection of a quadric surface and a cubic surface. Conversely, any regular complete intersection of a quadric surface and a cubic surface is a canonically embedded non-hyperelliptic curve of genus 4.

Proof: Looking at the map \( H^0(\mathcal{O}_{\mathbb{P}^3}(2)) \rightarrow H^0(\mathcal{O}_C(2)) \), we see \( C \) lies on a unique quadric \( Q \) (uniqueness follows from Bezout’s theorem and (5.7.3.11), by the same reason as (5.11.8.5)).

Next looking at the map \( H^0(\mathcal{O}_{\mathbb{P}^3}(3)) \rightarrow H^0(\mathcal{O}_C(3)) \), then the kernel has dimension at least 5, thus there is a cubic containing \( C \) but not \( Q \). Then \( S \cap Q \) is a complete intersection of degree 6
containing $C$, also it has the same arithmetic genus as $C(5.7.3.8)$, thus the same Hilbert polynomial (linear function), so $C = S \cap Q$ by (5.7.3.11). Conversely, any smooth curve of the form $S \cap Q$ is a canonical curve of genus 4, by adjunction formula ($K_C = \mathcal{O}_C(1)$ has degree 6).

Conversely, for any smooth complete intersection of a quadric surface and a cubic surface has arithmetic genus 4 by (5.7.3.8), $\mathcal{O}_C(1)$ has degree 6 and $h^0(\mathcal{O}_C(1)) \geq 4$ because $C$ is non-degenerate: there are no smooth plane curve of genus 4.

Now if $Q$ is non-singular, then $C$ is of type $(3, 3)$ in $Q$, thus the two projections are two trigonal map from $C$ to $\mathbb{P}^1$, and if $Q$ is a cone, the projection from the vertex is a trigonal map from $C$ to $\mathbb{P}^1$. □

**Prop.(5.11.8.9)[Non-Hyperelliptic Curve of Genus $\geq 5$].** For a non-hyperelliptic curve $C$ of genus 5, we have a canonical map $\varphi : C \to \mathbb{P}^4$. Firstly we consider what quadrics $C$ lies on: $h^0(\mathcal{O}_{\mathbb{P}^4}(2)) = 15$ and $h^0(\mathcal{O}_C(2)) = 12$, so $C$ lies on at least 3 quadrics. There are two cases:

1. $C = \cap Q_i$ where $Q_i$ are the quadrics containing $C$.
2. $C$ is a strict subset of $\cap Q_i$, which corresponds to non-trigonal and trigonal curves.

*Proof:* The case 1 does occur, because by Bertini’s theorem (5.6.4.29), for general three quadrics $Q_i$, $\cap Q_i$ is a smooth curve, and thus $K_C = (K_{\mathbb{P}^4}(-5 + 2 + 2 + 2))|_C = \mathcal{O}_C(1)$. So $d = 8, g(C) = 5$.

In this case, $C$ is not trigonal, because if $C$ is trigonal, then $C$ has a $g_3$, which means $C$ has three colinear point. Then all the quadrics $Q_i$ must contain this line, contradiction.

The case 2: Cf. [Algebraic Curves, Harris, P24].? This case corresponds to trigonal curves. □

**Prop.(5.11.8.10)[Non-Hyperelliptic Curve of Genus 5 is Tetragonal].** Let $C$ be a canonical embedded curve which is not trigonal admits a map of degree 4 to $\mathbb{P}^1$.

*Proof:* Let $\mathbb{P}^2 = \{Q | C \subset Q\}$. We can ask there are singular quadrics in this set. Inside $\mathbb{P}^{14}$ which is the space of all quadrics in $\mathbb{P}^4$, there is a quintic hypersurface of singular quadrics. ? For the rest, Cf. [Algebraic Curves, Harris, P25]. □

**Prop.(5.11.8.11).** If $C \subset \mathbb{P}^{g-1}_k$ is a canonical smooth curve of genus $g \geq 6$, then $C$ is not a complete intersection.

*Proof:* □

**Correspondences**

**Complex Tori and Algebraic Varieties**

9 Castelnuovo Theory

10 Brill-Noether Theory

11 Complex Algebraic Curves

**Prop.(5.11.11.1)[compact Riemann Surfaces as Complex Algebraic Curves].** Any Riemann surface is a Hodge manifold by (11.8.9.7), and the category of compact Riemann surfaces is equivalent to the category of compact algebraic curves, by GAGA (11.7.6.17).

*Proof:* □
Prop.(5.11.11.2)[Genus].

Prop.(5.11.11.3). A compact Riemann surface $M$ is Kähler by definition, so by Hodge decomposition (11.8.4.1),
\[ H^1(M, \mathbb{C}) \cong H^0(M, \Omega_M) \oplus \overline{H^0(M, \Omega_M)}, \]
so the number of holomorphic 1-forms on $M$ is equal to $b_1(M)/2 = g$, the topological genus.

Prop.(5.11.11.4) [Riemann Existence Theorem]. Any compact Riemann Surface is a Hodge manifold, thus projective algebraic, by (11.8.9.6) and Chow’s lemma.

Proof: Because $H^{1,1}(X) = H^2(X, \mathbb{Z})$, so it clearly contains integral classes. And it is positive because there is a basis generated by any Hermitian metric on $X$. So the theorem follows from (11.8.9.6). \qed

Cor.(5.11.11.5). In fact the same argument shows that any Kähler manifold with $H^{0,2}(X) = 0$ is projective.

Prop.(5.11.11.6).
- For any meromorphic function $f$ on a compact Riemann surface, $(f) = (f)_0 - (f)_{\infty}$ has degree 0.
- Let $\omega$ be a differential form on a compact Riemann surface, then the sum of residues of $\omega$ at its poles is zero.

Proof: 2: Choose a triangularization of the Riemann surface, then use the fact for any simple region $\Omega$ be boundary $C$,
\[ \int_C \omega = 2\pi i \left( \sum_{\text{poles}} \text{res}_p \omega \right). \]
And the integrals cancel out.
1: This is a direct consequence of 2 applied to the differential form $\omega = df/f$. \qed

Abel’s Theorem and Reciprocity Law

Prop.(5.11.11.7) [Reciprocity Law I]. Cf.[Griffith/Harris P230].

Prop.(5.11.11.8)[Weil]. $f, g$ are meromorphic functions on a compact Riemann surface that $(f), (g)$ are disjoint, then
\[ \prod f(p)^{v_p(g)} = \prod g(p)^{v_p(f)}. \]
Proof: Cf.[Griffith/Harris, P242]. \qed

Prop.(5.11.11.9)[Differentials on Plane Curves].

12 Relative Curves

Def.(5.11.12.1) [Relative Curves]. Let $S \in \text{Sch}$, a smooth curve over $S$ is a smooth morphism $C \to S$ of relative dimension 1 that is separated and of f.p..

Prop.(5.11.12.2). Let $S \in \text{Sch}$ and $C$ a smooth curve over $S$, then
5.12 K3 Surfaces

References are [Lectures on K3 Surfaces Huybrechts].
6  |  Weil Cohomologies and Motives

6.1  Intersection Theory

Main references are [Sta]Chap43, 44 and [Ful98].

1  Setups

Def.(6.1.1.1) [Setups]. The setup is a universally catenary(hence locally Noetherian) scheme $S(5.4.1.31)$ endowed with a dimension function $\delta(3.8.3.36)$, which will be fixed.

Example(6.1.1.2). There are some examples of $(S,\delta)$ in(6.1.1.1):

- $k \in \text{Field}, S = \text{Spec} \ k$ and $\delta(\vert S\vert) = 0$.
- $A$ is a Noetherian domain of dimension $1$, $\delta(p) = 0$ if $p$ is a maximal ideal and $\delta(\eta) = 1$ for the generic point $\eta$.
- $S$ is a C.M. scheme and let $\delta(s) = -\dim(\mathcal{O}_{S,s})$.

Proof: These follow from(5.4.1.33). □

Prop.(6.1.1.3). Let $(S,\delta)$ be in(6.1.1.1), $S$ Jacobian and $\delta(s) = 0$ for any closed point $s \in S$. If $Z \subset S$ is an integral closed subscheme with generic point $\xi$, then

$$\delta(\xi) = \dim(Z) = \dim(\mathcal{O}_{Z,z})$$

where $z \in Z$ is a closed point.

Proof: Cf.[Sta]02QO. □

Prop.(6.1.1.4)[\delta-Dimension]. For $f : X \rightarrow S$ locally of f.t., the function

$$\delta(x) = \delta(f(x)) + \text{tr.deg}_{k(f(x))} k(x)$$

is a dimension function on $X$. In particular, this equation is satisfied for any morphisms between schemes of f.t. over $S$.

For a closed subscheme $Z$ of $X$, define $\dim_{\delta}(Z) = \sup \dim_{\delta}(\eta)$ where $\eta$ are generic pts of irreducible components of $Z$.

Proof: Cf.[Sta]02JW. □
2 Chow Homologies

Cycles

Def. (6.1.2.1) [Cycles]. An algebraic cycle on a scheme \( X \in \text{Sch}^{\text{loc.ft.}} / S \) is a formal sum of integral closed subschemes of \( X \) with integer coefficients that is locally finite. A \( k \)-cycle is a cycle that is a sum of integral closed subschemes of dimension \( k \) that is locally finite. The group of \( k \)-cycles over \( X \) is denoted by \( Z_k(X) \).

If \( \dim_\delta(X) = d \), then we also denote \( Z^d(X) = Z_{d-k}(X) \).

Prop. (6.1.2.2). Let \( X \) be a scheme locally of f.t. over \( S \), and \( X = X_1 \cup X_2 \) is a decomposition as closed subschemes, then there are exact sequences

\[
Z_k(X_1 \cap X_2) \to Z_k(X_1) \oplus Z_k(X_2) \to Z_k(X) \to 0
\]

Prop. (6.1.2.3) [Cycle associated to a Closed Subscheme]. For a closed subscheme \( Z \) of a scheme \( X \in \text{Sch}^{\text{loc.ft.}} / S \), if \( \dim_\delta(Z) \leq k \) and \( \eta \in Z \) has dimension \( k \), then \( \eta \) is a generic pt of an irreducible component \( Z' \) of \( Z \), and \( m_{Z,Z'} = \text{length}_{\mathcal{O}_{X,\eta}} \mathcal{O}_{Z,\eta} \) is finite.

So we may define the \( k \)-cycle associated to \( Z \) as:

\[
[Z]_k = \sum_{Z' \subset Z} m_{Z,Z'} [Z']
\]

where the sum is over all integral components of \( Z \) of \( \delta \)-dimension \( k \).

Proof: \( m_{Z,Z'} \) is finite because \( \text{length}_{\mathcal{O}_{Z,\eta}} \mathcal{O}_{Z,\eta} = \text{length}_{\mathcal{O}_{X,\eta}} \mathcal{O}_{Z,\eta} < \infty \) because it is Noetherian and have 0 dimension (4.1.3.4). The sum is locally finite by (5.4.1.23).

Prop. (6.1.2.4) [Cycle associated to a Coherent Sheaf]. For \( X \in \text{Sch}^{\text{loc.ft.}} / S \) and \( \mathcal{F} \in \text{Coh}(X) \), if \( \dim_\delta(\text{Supp}(\mathcal{F})) \leq k \) and \( \eta \in \text{Supp}(\mathcal{F}) \) has dimension \( k \), then \( \eta \) is a generic pt of an irreducible component \( Z' \) of \( Z \), and \( m_{Z,F} = \text{length}_{\mathcal{O}_{X,\eta}} \mathcal{F}_\eta \) is finite.

So we may define the \( k \)-cycle associated to \( \mathcal{F} \) as:

\[
[F]_k = \sum_{Z' \subset Z} m_{Z,F} [Z']
\]

where the sum is over all integral components of \( \text{Supp}(\mathcal{F}) \) of \( \delta \)-dimension \( k \).

Proof: \( \text{length}_{\mathcal{O}_{X,\eta}} \mathcal{F}_\xi \) is finite by (4.2.5.7).

Prop. (6.1.2.5). Let \( X \in \text{Sch}^{\text{loc.ft.}} / S \) and \( Z \subset X \) a closed subscheme with \( \dim_\delta(Z) \leq k \), then \( [Z]_k = [\mathcal{O}_Z]_k \).

Prop. (6.1.2.6). Let \( X \in \text{Sch}^{\text{loc.ft.}} / S \), the cycle map from \( \text{Coh}^{\leq k}(X) \) to \( Z_k(X) \) is additive.

Pushforward and Pullback

Lemma (6.1.2.7) [Degree of Maps]. Let \( f : X \to Y \) be a map between schemes integral and locally of f.t. over \( S \), if \( \dim_\delta X = \dim_\delta Y \), then either \( f(X) \) not dominant or the function field extension is finite. If \( f \) is dominant, the the degree of \( f(5.4.4.55) \) is a finite number.

Proof: Because \( X \) is irreducible, so does \( f(X) \) and \( f(\overline{X}) \). If \( f(X) \) is dominant, then \( f \) maps the generic point of \( X \) to that of \( Y \). Now \( \text{deg}_{K(Y)}(K(X)) = 0 \) and \( K(X)/K(Y) \) is f.g., thus it is a finite extension.

Lemma (6.1.2.8). Let \( f : X \to Y \) be a qc map between schemes integral and locally of f.t. over \( S \), and \( \{Z_i\} \) is a locally finite collection of closed subschemes of \( X \), then \( \{f(Z)\} \) is also a locally finite collection of closed subschemes of \( X \).
Proof: This is a simple topological proof and omitted. \qed

**Def. (6.1.2.9) [Proper Pushforward].** Let $f : X \to Y$ be a proper morphism in $\Sch_{\text{loc. ft}} / S$, we define a map

$$p_* : Z_k(X) \to \CH_k(X)$$

as follows: If $Z \subset X$ is an integral closed subscheme of $X$ that $\dim_{\delta}(Z) = k$, then we define

$$f_*[Z] = \begin{cases} 0 & \text{dim}_{\delta}(f(Z)) \leq k \\ \deg(Z/f(Z))[f(Z)](6.1.2.7) & \text{dim}_{\delta}(f(Z)) = k \end{cases}$$

where we regard $f(Z)$ as an integral closed subscheme of $Y$ using its scheme-theoretical image. In general

$$f_*(\sum n_Z[Z]) = \sum n_Zf_*([Z]).$$

The sum is locally finite by (6.1.2.8).

It can be easily verified that $f_* \circ g_* = (f \circ g)_*$. 

**Prop. (6.1.2.10) [Pushforward of Coherent Sheaves].** Let $f : X \to Y \in \Sch_{\text{loc. ft}} / S$, then

- If $Z \subset X$ is an integral closed subscheme of $X$ that $\dim_{\delta}(Z) \leq k$, then
  $$f_*[Z]_k = [\mathcal{O}_Z]_k.$$  

- If $\mathcal{F} \in \text{Coh}^{\leq k}(X)$, then
  $$f_*[\mathcal{F}]_k = [f_*\mathcal{F}]_k.$$ 

**Proof:** 1 follows from 2 and (6.1.2.5). To show 2, by restricting to $\text{Supp}(\mathcal{F})$ and taking the scheme-theoretic image, it suffices to show for both closed immersions and proper dominant maps. The closed immersions case are easy. For the proper dominant case, it suffices to show $f_*[\mathcal{F}]_k$ and $[f_*\mathcal{F}]_k$ have the same coefficients in each integral subscheme $Z \subset X$ of dimension $k$. By looking at the inverse image of the generic point of $Z$, we may assume that $f$ is finite by (5.4.4.53). Thus we can assume $f$ is finite. Then it reduces to the affine case, which follows from (4.1.2.7). \qed

**Lemma (6.1.2.11).** Let $f : X \to Y$ be a flat morphism of relative dimension $r$ in $\Sch_{\text{loc. ft}} / S$, then for any closed subscheme $Z \subset Y$, $\dim_{\delta}(f^{-1}(Z)) = \dim_{\delta}(Z) + r$ if $f^{-1}(Z) \neq \emptyset$. If $Z$ is irreducible and $Z' \subset f^{-1}(Z)$ is an irreducible component, then $Z'$ dominants $Z$ and $\dim_{\delta}(Z') = \dim_{\delta}(Z) + r$.

**Proof:** By passing to the integral components, we may assume $Z = Y$ is integral and $X \to Y$ is surjective, then notice $f$ is open, and use (6.1.1.4) and (5.6.3.7). \qed

**Def. (6.1.2.12) [Flat Pullbacks].** Let $f : X \to Y$ be a flat morphism of relative dimension $r$ in $\Sch_{\text{loc. ft}} / S$, for $Z \subset X$ an integral closed subscheme that $\dim_{\delta}(Z) \leq k$, define

$$f^* : Z_k(Y) \to Z_{k+r}(X) : f^*([Z]) = [f^{-1}(Z)]_{k+r}$$

which is definable by (6.1.2.11). In general, define $f^*(\sum n_Z[Z]) = \sum n_Zf^*([Z])$, which is locally finite.

**Prop. (6.1.2.13).** If $f : X \to Y, g : Y \to Z \in \Sch_{\text{loc. ft}} / S$ is flat of relative dimensions $r$ and $s$, then $f^* \circ g^* = (g \circ f)^*$. 

Proof: Firstly \( g \circ f \) is flat of relative dimension \( r + s \) by (5.6.3.18). And the assertion follows from (4.1.2.9).

Prop. (6.1.2.14). Let \( X \in \text{Sch}^{\text{loc.ft}} / S \) and \( i : Y \to X \) a reduced closed subscheme of \( X \), \( j : U = X \setminus Z \to X \), then for any \( k \in \mathbb{Z} \), there is an exact sequence

\[
Z_k(Y) \xrightarrow{i_*} Z_k(X) \xrightarrow{j^*} Z_k(U) \to 0.
\]

Prop. (6.1.2.15) [Pullback of Coherent Sheaves]. If \( f : X \to Y \in \text{Sch}^{\text{loc.ft}} / S \) is flat of relative dimensions \( r, \mathcal{F} \in \text{Coh}^{\leq k}(\mathcal{O}_Y) \), then \( f^* \mathcal{F} \in \text{Coh}^{\leq k+r}(\mathcal{O}_X) \), and

\[
f^* \mathcal{F} = [f^* \mathcal{F}]_{k+r}.
\]

In particular, for a closed subscheme \( Z \subset X \) with \( \dim_{\delta}(Z) \leq k \), \( f^*[Z]_k = [f^{-1}Z]_{k+r} \), by (4.1.2.8).

Proof: This follows from (4.1.2.9).

Prop. (6.1.2.16) [Push and Pull].

- Let

\[
\begin{array}{ccc}
X' & \xrightarrow{g'} & X \\
\downarrow{f'} & & \downarrow{f} \\
Y' & \xrightarrow{g} & Y
\end{array}
\]

be a diagram in \( \text{Sch}^{\text{loc.ft}} / S \) where \( f \) is proper and \( g \) is flat of relative dimension \( r \), then

\[
g^* f_* = (g')^* f'_* : Z_k(X) \to Z_{k+r}(Y').
\]

- Let \( f : X \to Y \in \text{Sch}^{\text{loc.ft}} / S \) be a finite locally free morphism of degree \( d \), then it it both proper and flat of relative dimension \( 0 \), and \( f_* f^* = [d] : Z_k(Y) \to Z_k(Y) \).

Proof: 1: It suffices to prove for a closed subscheme \( W \subset X \) of \( \delta \)-dimension \( k \). Then \([W] = [\mathcal{O}_W](6.1.2.5)\). Then by (6.1.2.10) and (6.1.2.15), the assertion follows from flat base change.

2: Similarly this follows from the fact \( f_* f^* \mathcal{O}_Z \) is a finite locally free \( \mathcal{O}_Z \)-sheaf of rank \( d \).

Rational Equivalences and Chow Groups

Def. (6.1.2.17) [Prime Weil Divisors]. Let \( X \in \text{Sch}^{\text{loc.ft,int}} / S \), then an integral closed scheme \( W \subset X \) of \( \delta \)-codimension 1 is called a prime Weil divisor.

Prop. (6.1.2.18) [Principal Weil Divisor]. Let \( X \in \text{Sch}^{\text{loc.ft,int}} / S \), \( f \in \mathcal{K} \), for any prime Weil divisor \( Z \) with generic pt \( \eta \), we can define \( \text{ord}_Z(f) = \text{ord}_{\mathcal{O}_{X,\eta}}(f)(4.1.2.10) \). It is multiplicative, and the closed integral subschemes \( Z \) that \( \text{ord}_Z(f) \neq 0 \) is locally finite.

So, we can define the principal Weil divisor \( \text{div}(f) = \sum_Z \text{ord}_Z(f)[Z] \).

Proof: There is an open subset \( U \) that \( f \in \Gamma(U, \mathcal{O}_X^*) \), so all \( Z \) are irreducible components of \( X - U \), which is locally finite because \( X \) is locally Noetherian and (5.4.1.23).

Def. (6.1.2.19) [Principal Divisors]. Let \( X \in \text{Sch}^{\text{loc.ft}} / S \) and \( f \in K(X)^* \), then the principal divisor associated to \( f \) is defined to be

\[
\text{div}(f) = \sum \text{ord}_Z(f)[Z] \in Z^1(X)
\]
as defined in (6.1.2.18). This is truly a \( k \)-cycle.
Def. (6.1.2.20) [Rational Equivalence]. Let $X \in \text{Sch}^{\text{loc} \text{.ft}} / S$ has $\delta$-dimension $k + 1$. Given any locally finite collection of integrally closed subschemes $W_i \subset X$ of $\delta$-dimension $k + 1$ and rational functions $f_i$ on $W_i$, we can consider the $k$-cycle $\sum(i_j)_{S}(\text{div}(f_i))$ on $X$. This is a cycle because $\coprod W_i \to X$ is proper. Two $k$-cycles are called rational equivalent if they differ by a $k$-cycle of the this form.

Define the Chow group of $k$-cycles $\text{CH}_k(X)$ to be $Z_k(X)$ modulo the rational equivalence relation. $\text{CH}_k(X)$ is also denoted by $\text{Cl}(X)$.

Lemma (6.1.2.21) [Push and Pull of Principle Divisors].

- If $f : X \to Y \in \text{Sch}^{\text{loc} \text{.ft}, \text{int}} / S$ is flat of relative dimension $r$, and $g \in K(Y)^*$, then $f^* \text{div}(f) = \text{div}(f)$.
- If $\varphi : X \to Y \in \text{Sch}^{\text{loc} \text{.ft}, \text{int}, \delta = d} / S$ is a dominant proper morphism, $f \in K(X)^*$, and $g = \text{Nm}_{K(X)/K(Y)}(f) \in K(Y)^*$, then $f^* \text{div}(f) = \text{div}(g)$.

Proof: 1: Cf.[Sta]0EPH?
2: Cf.[Sta]02RT?

Lemma (6.1.2.22). If $X \in \text{Sch}^{\text{loc} \text{.ft}, \text{int}, \delta = n} / S U \subset X$ be an open subscheme and $f \in \Gamma(U, \mathcal{O}_X)^* \subset K(X)^*$, let $Y$ be the graph of $f$ in $X \times_S \mathbb{P}^1_S$, then

- the projection $\text{pr}_1 : Y \to X$ is an isomorphism $\text{pr}^{-1}(U) \to U$, thus $\dim_\delta(Y) = n$.
- the closed subschemes $Y_0 = \text{pr}_2^{-1} \{0\}$ and $Y_\infty = \text{pr}_2^{-1} \{\infty\}$ of $Y$ are effective Cartier divisors.

In particular, they have $\delta$-dimension $n - 1$ by (6.1.5.2).

- $\text{div}_Y(f) = [Y_0] - [Y_\infty]$.
- $\text{div}_X(f) = \text{pr}_1^* \text{div}_Y(f) = [Y_0] - [Y_\infty]$.

Proof: 1 is clear.
2 follows from (5.8.1.7) as $\text{pr}_2 : Y \to \mathbb{P}^1$ is dominant.
3 is clear.
4 follows from item1 and (6.1.2.21).

Prop. (6.1.2.23) [Rational Equivalence via Rational Functions]. Let $X \in \text{Sch}^{\text{loc} \text{.ft}} / S$, then $\alpha \in Z_k(X)$ is rationally trivial iff

$$\alpha = \sum(([(W_i)_0]_k - [(W_i)_1]_k) = j_0^*(\sum[W_i]) - j_\infty^*(\sum[W_i])$$

where $\{W_i\}$ is a locally finite family of integral closed subschemes of $X \times_S \mathbb{P}^1_S$ of $\delta$-dimension $k$. $(j_0^*, j_\infty^*)$ are the Gysin maps, which will be defined in (6.1.4.2))

Proof: Firstly such a $\sum(([(W_i)_0]_k - [(W_i)_1]_k)$ is locally finite, and each $[(W_i)_0]_k - [(W_i)_1]_k$ is rationally trivial: Similar as in (6.1.2.22), $[(W_i)_0]_k - [(W_i)_\infty]_k$ is rationally trivial on $W_i$, and then it pushforward via $\text{pr}_1$ is also rationally trivial, by (6.1.2.21).

Conversely, if $\alpha = \sum(V_i \to X)_* \text{div}(f_i)$, where $\{V_i\}$ is a locally finite family of integral closed subschemes of $X$ of $\delta$-dimension $k + 1$ and $f_i \in K(V_i)^*$. Let $W_i \subset V_i \times X_i \subset X_i \times \mathbb{P}_k^1$ be the the graph of $f_i$, then $(V_i \to X)_* \text{div}(f_i)$ equals $[(W_i)_0]_k - [(W_i)_1]_k$ by (6.1.2.22) again.(We are secretly using the fact Gysin map commutes with pushforwards (6.1.6.9), but in this case it is trivial trough).

□

Prop. (6.1.2.24) [Push and Pull for Chow Groups].
• If $f : X \to Y \in \text{Sch}^{\text{loc}.\text{ft}} / S$ is flat of relative dimension $r$, then $f^*$ induces a map $\text{CH}_k(Y) \to \text{CH}_{k+r}(X)$ for each $k \in \mathbb{N}$.
• If $f : X \to Y \in \text{Sch}^{\text{loc}.\text{ft}} / S$ is proper, then $f_*$ induces a map $\text{CH}_k(X) \to \text{CH}_k(Y)$ for each $k \in \mathbb{N}$.

Proof: Cf. [Sta]02S2, 02S1.

Prop. (6.1.2.25) [Restriction of Divisors]. Let $X \in \text{Sch}^{\text{loc}.\text{ft}} / S$ and $i : Y \to X$ a reduced closed subscheme of $X$, $j : U = X \setminus \overline{Z} \to X$, then for any $k \in \mathbb{Z}$, there is an exact sequence

\[ \text{CH}_k(Y) \xrightarrow{i_*} \text{CH}_k(X) \xrightarrow{j^*} \text{CH}_k(U) \to 0. \]

Proof: Cf. [Sta]02RX.

Prop. (6.1.2.26) [Excision]. Let $X \in \text{Sch}^{\text{loc}.\text{ft}} / S$ and $X_1, X_2$ be closed subschemes of $X$ s.t. $X_1 \cup X_2 = X$ as sets, then for any $k \in \mathbb{Z}$, there is an exact sequence

\[ \text{CH}_k(X_1 \cap X_2) \to \text{CH}_k(X_1) \oplus \text{CH}_k(X_2) \to \text{CH}_k(X) \to 0. \]

Proof: Cf. [Sta]0F94.

Def. (6.1.2.27) [Degree of 0-Cycles]. Let $X$ be a proper scheme over a field $k$, the degree of a zero cycle is given by the proper pushforward

\[ p_* : \text{CH}_0(X) \to \text{CH}_0(\text{Spec } k) \cong \mathbb{Z}. \]

Equivalently, if $\alpha = \sum n_i[Z_i] \in \text{Z}_0(X)$, $\deg(\alpha) = \sum n_i \deg(Z_i)$. $\deg$ is also denoted by $f_X$.

Def. (6.1.2.28) [Stratification by Dimension]. Let $X \in \text{Sch}^{\text{loc}.\text{ft}} / S$, then the following are equivalent:

• There exists a decomposition $X = \bigsqcup_n X_n$ where $X_n$ is pure of $\delta$-dimension $n$.
• For any $x \in X$, there exist s nbhd $x \in U$ s.t. $U$ is pure of $\delta$-dimension $n$.
• For an $x \in X$, the irreducible components of $X$ containing $x$ are all of the same $\delta$-dimension.

These conditions are satisfied if $X$ is normal or Cohen-Macaulay.

Proof: $1 \to 2 \to 3$ is trivial. $3 \to 1$ follows from the fact $x \mapsto n_x$ is continuous.

If $X$ is normal, it is a disjoint union of integral schemes by (5.4.2.3). For $X$ Cohen-Macaulay, Cf. [Sta]0FE3.

Def. (6.1.2.29) [Cohomological Chow Groups]. If $X$ satisfies (6.1.2.28), we define

\[ Z^p(X) = \prod_n Z_{n-p}(X_n), \quad Z^*(X) = \bigoplus_p Z^p(X) \]

and the Chow group of codimension $p$ cycle

\[ \text{CH}^p(X) = \prod_n \text{CH}_{n-p}(X_n), \quad \text{CH}^*(X) = \bigoplus_p \text{CH}^p(X). \]

Def. (6.1.2.30) [Fundamental Class]. If $X$ satisfies (6.1.2.28), define

\[ [X] = \prod_n [X_n]_n \in \text{CH}^0(X) \]

to be the fundamental class of $X$. 
3 Chow Groups and K-Groups
Cf.[Sta]42.22, 42.56 and42.68.

4 Gysin Maps
Def.(6.1.4.1)[Gysin Maps for Virtual Divisors]. Let \( X \in \text{Sch}^{\text{loc.ft}} / S, L \in \text{Pic}(X), s \in H^0(X, L) \), denote \( D = Z(s) \), and \( i : D \to X \) the closed immersion. Then for any \( k \in \mathbb{Z} \), there is a Gysin homomorphism
\[
i^* : Z_{k+1}(X) \to \text{CH}_k(D)
\]
that for an integral closed subscheme \( Z \subset X \) with \( \text{dim}_{\mathbb{Z}}(Z) = k + 1 \),
\[
i^*([Z]) = \begin{cases} [D \cap Z]_k, & Z \not\subset D \\ i^*_{\alpha}([\mathcal{L}|_Z \cap [Z])], & Z \subset D \text{ via } i' : Z \to D \end{cases}
\]
and extends linearly to \( Z_{k+1}(X) \), which is also locally finite.

We will see this is map \( i^* \) in fact factor through rational equivalence relations in(6.1.6.9).

Proof: To show this is well defined, Cf.[Sta]02TO.

Remark(6.1.4.2). If \( \mathcal{L}|_D \cong \mathcal{O}_D \), the \( c_1(\mathcal{L}|_Z) \) term is trivial, so the Gysin homomorphism factors through \( Z_k(D) \to \text{CH}_k(D) \).

Cor.(6.1.4.3). Let \( X \in \text{Sch}^{\text{loc.ft}} / S, (\mathcal{L}, s : D \to X) \) as in(6.1.4.1), then for any \( \alpha \in \text{CH}_s(X) \),
\[
i_* i^* \alpha = c_1(\mathcal{L}) \cap \alpha
\]

Def.(6.1.4.4)[Intersection with Cartier Divisors]. If \( X \in \text{Sch}^{\text{loc.ft}} / S, D \in \text{Cart}^{\text{eff}}(X) \), denote
\[
D \cap \alpha = c_1(\mathcal{O}_X(D)) \cap \alpha \text{ for } \alpha \in Z_s(X).
\]

Def.(6.1.4.5)[Gysin Map for Local Complete Intersection Maps]. Let \( f : X \to Y \in \text{Sch}^{\text{loc.ft}} / S \) be a local complete intersection map s.t. \( f = g \circ i \) where \( g \) is smooth and \( i \) is a regular immersion, then we define the Gysin map for \( f \) to be \( f^! = i^! \circ g^* \in A^*(X \to Y) \). This is independent of the decomposition \( f = g \circ i \) chosen. In this case, we say the Gysin map for \( f \) exists.

Proof: Cf.[Sta]0FF2.

Prop.(6.1.4.6)[\( f^! \text{ and } f^* \)]. Let \( f : X \to Y \in \text{Sch}^{\text{loc.ft}} / S \) be a local complete intersection map, then if the Gysin map \( f^! \) exists and \( f \) is flat, then \( f^* \) can be defined and \( f^! = f^* \in A^*(X \to Y) \).

Proof: Cf.[Sta]0FF4.

5 Weil Divisors
Prop.(6.1.5.1)[Weil-Cartier]. For \( X \in \text{Sch}^{\text{loc.ft}} / S \), there is a map from Cartier divisors on \( X \) to Weil divisors mapping \( (D, s_D) \) to \( [Z(s_D)]_k \). Notice this is defined because a Cartier divisor is locally defined by a regular element and Krull’s principal ideal theorem.

Moreover, if \( X \) is locally factorial, this map is an isomorphism \( \text{CaCl}(X) \to \text{Cl}(X) \) by(5.8.1.4), and (effective)Cartier divisors correspond (effective)Weil divisors.

This in particular applies to non-singular varieties over a field, by(4.3.5.19).
Prop. (6.1.5.2). Let \( X \in \text{Sch}^{\text{loc.ft}} / S \) and \( Z \subset X \) be an integral closed subscheme, then \( Z \) is a Weil divisor iff \( \dim(Z) = \dim_s(X) - 1 \). In particular, this holds for any irreducible component of a Cartier divisor by (6.1.5.1).

Def. (6.1.5.3) [Q-Cartier Divisors]. A Q-Cartier divisor on a locally Noetherian integral scheme is a Weil divisor that some multiply of it is the image of a Cartier divisor.

Example (6.1.5.4) [Non-Q-Cartier Divisors]. It is easy to show some Weil divisor is not a Q-Cartier divisor (on a singular variety), by showing its complement is not affine (5.8.1.1). For example, on \( X = \text{Spec} k[x, y, z, w]/(xy - zw) \), the Weil divisor cut out by \( (z, w) \) is not Q-Cartier, as the closed subscheme \( y = w = 0 \) of its complement is isomorphic to \( A^2_k \setminus \{(0, 0)\} \), which is not affine by calculating Čech cohomology.

In particular, \( k[x, y, z, w]/(xy - zw) \) is normal but not a UFD.

Prop. (6.1.5.5) [Rational Functions and Poles]. If \( X \) is an integral locally Noetherian normal scheme and \( f \in K(X) \) has no poles, then \( f \in \Gamma(X) \), by (4.3.5.11).

Prop. (6.1.5.6) [UFD and Class Groups]. For \( A \) a Noetherian normal domain, it is a UFD iff \( \text{Cl}(\text{Spec} A) = 0 \).

Proof: It suffices to show minimal primes of \( A \) is principal iff minimal primes of \( A \) are principal divisors. This is done by (4.3.5.11) and (2.2.3.6).

Prop. (6.1.5.7) [Picard Group of Projective Spaces]. Let \( R \) be a UFD, then \( \text{Cl}(\mathbb{P}^n_R) = \mathbb{Z} \), and it is generated by \([H]\) where \( H \) is any hyperplane of \( \mathbb{P}^n_R \). And a hypersurface \( Y \) of degree \( d \) is mapped to \( d[H] \) by direct verification.

Cor. (6.1.5.8). If \( Y \subset \mathbb{P}^n_k \) is a hypersurface of degree \( d \), then \( \text{Cl}(\mathbb{P}^2 \setminus Y) = \mathbb{Z}/d\mathbb{Z} \).

Proof: This follows from (6.1.7.10) and (6.1.5.6). The last assertion follows from the fact \([Y] \sim d[H]\) by direct verification.

Cor. (6.1.5.9). If \( k \in \text{Field} \), \( \text{Cl}(\mathbb{P}^1_k \times \mathbb{P}^1_k) = \mathbb{Z} \oplus \mathbb{Z} \), by (6.1.7.10).

Prop. (6.1.5.10). If \( X \) is a non-singular cubic surface in \( \mathbb{P}^3_k \), then \( \text{Cl}(X) \cong \mathbb{Z}^7 \).

Proof: Cf. [Har77] Chap 5.4.8.

6 Bivariant Classes

Def. (6.1.6.1) [Bivariant Classes]. Let \( f : X \to Y \in \text{Sch}^{\text{loc.ft}} / S \) and \( p \in \mathbb{Z} \), a bivariant class \( c \) of degree \( p \) for \( f \) is a class of maps

\[ c \cap - : \text{CH}_k(Y') \to \text{CH}_{k-p}(Y' \times_Y X) \]

for any \( Y' \in \text{Sch}^{\text{loc.ft}} / Y \) and \( k \in \mathbb{Z}_+ \) that satisfies

- If \( Y'' \to Y' \in \text{Sch}^{\text{loc.ft}} / Y \) is proper, \( c \cap - \) commutes with proper pushforwards.

- If \( Y'' \to Y' \in \text{Sch}^{\text{loc.ft}} / Y \) is flat of relative dimension \( r \in \mathbb{Z} \), \( c \cap - \) commutes with flat pullbacks.
• Let \((L, s, i : D \to Y')\) be a triple on \(Y'\) as in (6.1.4.1), then \(c \cap -\) commutes with Gysin homomorphisms \(i^*\).

The set of bivariant classes of degree \(p\) for \(f\) is denoted by \(A^p(X \to Y)\). And denote \(A^*(X \to Y) = \bigoplus_{p \in \mathbb{Z}} A^p(X \to Y)\).

**Prop. (6.1.6.2).** For any \(f : X \to Y, g : Y \to X \in \text{Sch}^{\text{loc.ft}}/S, p, q \in \mathbb{Z}, A^p(X \to Y)\) is an Abelian group, and the composition defines a bilinear map

\[
A^q(Y \to Z) \times A^p(X \to Y) \to A^{p+q}(X \to Z)
\]

that is associative w.r.t. compositions in \(\text{Sch}^{\text{loc.ft}}/S\).

**Def. (6.1.6.3) [Chow Cohomologies].** Let \(X \in \text{Sch}^{\text{loc.ft}}/S\), denote \(A^p(X) = A^p(\text{id}_X)\), and \(A^*(X) = \bigoplus_{p \in \mathbb{Z}} A^p(X)\) the graded ring, called the **Chow cohomology group** of \(X\).

**Prop. (6.1.6.4) [Restriction of Classes].** Let \(X \to Y, f : Y' \to Y \in \text{Sch}^{\text{loc.ft}}/S\) and \(X' = X \times_Y Y'\), then obviously there is a map \(f^* : A^p(X \to Y) \to A^p(X' \to Y')\). In particular, if \(Z \subset X\) is a closed subscheme, then \(f^*(c)\cap \alpha = c\cap f_\ast(\alpha)\) for \(c \in A^p(Z \to X), \alpha \in A^p(Z)\) by proper pushforward (6.1.6.1).

**Cor. (6.1.6.5) [Product of Classes].** Let \(X \to Y, X' \to Y' \in \text{Sch}^{\text{loc.ft}}/S, c \in A^p(X \to Y), c' \in A^q(X' \to Y')\), then the product \(c \circ c'\) is defined to be the element in \(A^{p+q}(X \times_S X' \to Y \times_S Y')\) defined by the map

\[
\text{CH}_*(Y \times_S Y') \xrightarrow{c \cap -} \text{CH}_*+q(Y \times_S X') \xrightarrow{\alpha \cap -} \text{CH}_{*+p+q}(X \times_S X')
\]

and all base change variants of this.

Notice \(c' \circ c\) is also in \(A^{p+q}(X \times_S X' \to Y \times_S Y')\), so it makes sense to talk about when two classes commute. Maybe \(c' \circ c\) can be defined on smaller base changes, but to say \(c, c'\) commute always means \(c \circ c' = c' \circ c \in A^{p+q}(X \times_S X' \to Y \times_S Y')\).

**Lemma (6.1.6.6) [Gysin Factors Through Rational Equivalences].** Let \(X \in \text{Sch}^{\text{loc.ft}}/S\), Gysin homomorphism for a triple \((L, s, j : D \to X)\) on \(X\) that are base change of \((\mathcal{O}(1), x, j : S \times(0) \to P_S^1)\) factors through rational equivalences.

**Proof:** This follows from the characterization of rational equivalences in (6.1.2.23) and the fact in this case Gysin maps are easy to describe: They are just \(k\)-parts of the inverse images. \(\square\)

**Prop. (6.1.6.7) [Weakening Bivariant Conditions].** Let \(f : X \to Y \in \text{Sch}^{\text{loc.ft}}/S\) and \(c\) is a class of maps

\[
c \cap - : Z_k(Y') \to \text{CH}_{k-p}(Y' \times_Y X)
\]

for any \(Y' \in \text{Sch}^{\text{loc.ft}}/Y\) that is compatible with Gysin homomorphism for triples \((L, s, j : D \to Y')\) that are base change of \((\mathcal{O}(1), x, j : S \times(0) \to P_S^1)\), then \(c\) factors through rational equivalences.

And if moreover \(c\) commutes with proper pushforwards and flat pullbacks (up to rational homotopy), then it induces a bivariant class \(c \in A^p(X \to Y)\).

**Proof:** For the first assertion: As \(L|_D = \mathcal{O}_D\), the Gysin homomorphism is defined on the level of cycles by (6.1.4.2) and pass to \(\text{CH}_*(6.1.6.6)\), so compositions with Gysin homomorphisms are well-defined. Then \(c\) factors through rational equivalence by the characterization of rational equivalences in (6.1.2.23).

For the last assertion, Cf. [Ful98] P321 or [Sta]0F9A. \(\square\)
Prop. (6.1.6.8). Let \( f : X \to Y \in \mathcal{S}_{\text{loc.ft}} / S \) and \( X = \bigsqcup_i X_i, Y = \bigsqcup_j Y_j \) be clopen subschemes and \( \alpha : I \to J \) is a map of sets s.t. \( f(X_i) \subset Y_{\alpha(i)} \), then for any \( p \in \mathbb{Z}_+ \),

\[
A^p(X \to Y) = \prod_i A^p(X_i \to Y_{\alpha(i)}).
\]

Proof: Cf. [Sta]0FDZ.

Prop. (6.1.6.9) [Gysin Homomorphisms are Bivariant]. Let \( X \in \mathcal{S}_{\text{loc.ft}} / S \) and \( (\mathcal{L}, s, i : D \to X) \) be a triple on \( X \) as in (6.1.4.1), then the Gysin homomorphism \((i^!)^*\) associated to the base changes of \( i \) form a bivariant class in \( A^1(D \to X) \).

Proof: Cf. [Sta]02TA, 0B71, 0B73 and (6.1.6.7).

Let \( f : X' \to X \in \mathcal{S}_{\text{loc.ft}} / S \) and \( (\mathcal{L}, s, i : D \to X) \) be a triple on \( X \) as in (6.1.4.1), we can define the pullback triple \( f^* (\mathcal{L}, s, i) = (\mathcal{L}', s', i' : D' \to X') \), and then

- If \( f \) is proper, then Gysin maps commute with proper pushforwards.
- If \( f \) is flat of relative dimension \( r \), then the Gysin maps commute with flat pullbacks.
- If \((\mathcal{M}, t, f : X' \to X)\) is a triple on \( X \) as in (6.1.4.1), then the different Gysin maps are compatible.

Prop. (6.1.6.10) [Flat Pullbacks are Bivariant]. Let \( f : X \to Y \in \mathcal{S}_{\text{loc.ft}} / S \) be flat of relative dimension \( r \), then the flat pullbacks along base changes of \( f \) form a bivariant class of degree \(-r\).

Proof: This follows from (6.1.2.13)(6.1.2.16)(6.1.6.9) and (6.1.6.7).

Prop. (6.1.6.11) [Proper Pushforwards are Bivariant]. Let \( f : X \to Y, g : Y \to Z \in \mathcal{S}_{\text{loc.ft}} / S \), \( f \) is proper, and \( c \in A^p(X \to Z) \), then the base change of \( f_* \circ c \) form a bivariant class in \( A^p(Y \to Z) \).

Proof: This reduces to the fact proper pushforwards commutes with flat pullbacks, proper pushforwards and Gysin maps, by (6.1.6.10)(6.1.6.9)(6.1.2.9) and (6.1.6.7).

7 Chern Classes

Invertible Sheaves

Prop. (6.1.7.1) [First Chern Classes]. Let \( X \in \mathcal{S}_{\text{loc.ft}} / S \) and \( \mathcal{L} \in \text{Pic}(X) \), then for any \( k \in \mathbb{Z} \), there is a map

\[
c_1(\mathcal{L}) \cap - : Z_{k+1}(X) \to CH_k(X)
\]

called intersection with the first Chern class of \( \mathcal{L} \) (the name will be made clear from (6.1.7.5)), defined as follows: If \( i : Z \to X \) is an integral subscheme of \( X \) with \( \dim_i(Z) = k+1 \), then \( c_1(\mathcal{L}) \cap [Z] \) is the the pushforward of the image of \( i^* \mathcal{L} \) under the map \( \text{Pic}(Z) \to \text{Cl}(Z) \cong CH_k(Z)(5.5.3.14) \), i.e.

\[
c_1(\mathcal{L}) \cap [Z] = i_*(c_1(i^* \mathcal{L}) \cap [W]).
\]

In general, define \( c_1(\mathcal{L}) \cap (\sum n_Z[Z]) = \sum n_Z c_1(\mathcal{L}) \cap [Z] \). We will see the first Chern class factors through rational equivalence relations in (6.1.7.5).
Lemma (6.1.7.2) [The first Chern Class is Multiplicative]. Let $X \in \text{Sch}^{\text{loc.ft}}/S$ and $\mathcal{L}, \mathcal{N} \in \text{Pic}(X)$, then
\[
c_1(\mathcal{L}) + c_1(\mathcal{N}) = c_1(\mathcal{L} \otimes \mathcal{N}) : \text{CH}_*(X) \to \text{CH}_*(X).
\]
In particular, $c_1(\mathcal{L}) = -c_1(\mathcal{L}^{-1})$, and $c_1(\mathcal{O}_X) = 0$.

Prop. (6.1.7.3) [Chern Classes and Zero Cycles]. Let $X \in \text{Sch}^{\text{loc.ft}}/S$ and $\mathcal{L} \in \text{Pic}(X)$, $Y \subset X$ a closed subscheme. If $s \in \Gamma(Y, \mathcal{L}|_Y)$ satisfies
\begin{itemize}
  \item $\dim s(Y) \leq k + 1$.
  \item $\dim s(Z(s)) \leq k$.
  \item For any generic point $\xi$ of irreducible components of $Z(s)$ of $\delta$-dimension $k$, multiplying by $s$ induces an injection $\mathcal{O}_{Y, \xi} \to (\mathcal{L}|_Y)_\xi$.
\end{itemize}
Then $c_1(\mathcal{L}) \cap [Y]_{k+1} = [Z(s)]_k$.

Proof: Cf. [Sta]02SQ.

Prop. (6.1.7.4) [First Chern Classes Factor Through CH_k(X)]. Situation in (6.1.7.1), then the map $c_1(\mathcal{L}) \cap - : Z_{k+1}(X) \to \text{CH}_k(X)$ factors through $Z_{k+1}(X) \to \text{CH}_{k+1}(X)$.

Proof: Cf. [Sta]02TI.

Prop. (6.1.7.5) [First Chern Classes Form Bivariant Classes]. Let $X \in \text{Sch}^{\text{loc.ft}}/X$ and $\mathcal{L} \in \text{Pic}(X)$, then the maps $c_1(f^*\mathcal{L}) \cap - : Z_{k}(X') \to \text{CH}_{k-1}(X')$ factor through rational equivalences for each $f : X' \to X \in \text{Sch}^{\text{loc.ft}}/X$, and form a bivariant class in $A^1(X)$, called the first Chern class $c_1(\mathcal{L})$.

Proof: Cf. [Sta]02SU, 02SS, 0B72, and (6.1.6.7).

To show it commutes with pullbacks,

Prop. (6.1.7.6) [First Chern Classes Commute with Bivariant Classes]. Let $f : X' \to X \in \text{Sch}^{\text{loc.ft}}/S$ and $\mathcal{L} \in \text{Pic}(X)$, then $c_1(\mathcal{L})$ commutes with every element of $A^*(X' \to X)$.

In particular, $c_1(\mathcal{L})$ is in the center of $A^*(X)$.

Proof: Cf. [Sta]0B7B.

Prop. (6.1.7.7). Let $X \in \text{Sch}^{\text{loc.ft}}/S$ and $\mathcal{L} \in \text{Pic}(X)$ be an ample invertible sheaf. Assume $d = \dim(X) < \infty$, then for any $\mathcal{L}_1, \ldots, \mathcal{L}_{d+1} \in \text{Pic}(X)$, $c_1(\mathcal{L}_1) \circ \ldots c_1(\mathcal{L}_{d+1}) = 0 \in A^{d+1}(X)$.

Proof: Use induction on $d$: $d = 0$ case is trivial as $X$ is discrete thus any invertible sheaf is trivial. In general, by (5.8.1.8) and (6.1.7.2), it suffices to prove for $\mathcal{L}_i = \mathcal{O}_X(D_i)$ be Cartier divisors. If $i : D_{d+1} \to X$, then $c_1(\mathcal{L}_{d+1}) = i_* \circ i^*$ by (6.1.4.3), and $c_1(\mathcal{L}_i)$ commutes with both $i_*$ and $i^*$, so we can replace $X$ by $D$ and then use induction hypothesis.

Lemma (6.1.7.8). If $X \in \text{Sch}^{\text{loc.ft}}/S$ and $0 \to \mathcal{L}_1 \to \mathcal{E} \to \mathcal{L}_2 \to 0$ is an exact sequence with $\mathcal{L}_1, \mathcal{L}_2 \in \text{Pic}(X)$, and there is a non-vanishing section $s$ of $\mathcal{E}$, then $c_1(\mathcal{L}_1) \cap c_1(\mathcal{L}_2) = 0 \in A^2(X)$.

Proof: Consider the image $\bar{s}$ of $s$ in $\Gamma(X, \mathcal{L}_2)$, then we can consider the Gysin map associated to $(\mathcal{L}_2, \bar{s}, j)$. Then
\[
c_1(\mathcal{L}_1) \cap c_1(\mathcal{L}_2) \cap \alpha = j_*(c_1(j^*\mathcal{L}_1) \cap j^*\alpha).
\]
\(j^*\mathcal{L}_1\) is trivialized by $s$ now, so this one is vanishes.
Lemma (6.1.7.9). If \( X \in \text{Sch}^{\text{loc.flt}} / S, r \in \mathbb{Z}_+, \mathcal{L} \in \text{Vect}^r(X) \), let \( \pi : P(\mathcal{E}) \to X \) be the projective space of \( \mathcal{E} \), then for any \( k \in \mathbb{Z} \) and \( \alpha \in \text{CH}_k(X) \),

\[
\pi_* (c_1(\mathcal{O}_{P(\mathcal{E})}(1))^s \cap \pi^* \alpha) = \begin{cases} 
0, & s < r - 1 \\
\alpha, & s = r - 1
\end{cases} \in \text{CH}_{k+r-1-s}(X).
\]

Proof: Cf. [Sta]02TW.

Prop. (6.1.7.10) [Projective Bundles Formula]. If \( X \in \text{Sch}^{\text{loc.flt}} / S, r \in \mathbb{Z}_+, \mathcal{L} \in \text{Vect}^r(X) \), let \( \pi : P(\mathcal{E}) \to X \) be the projective space of \( \mathcal{E} \), then for any \( k \in \mathbb{Z} \), the map

\[
\text{CH}_{k+r-1}(P(\mathcal{E})) = \bigoplus_{i=0}^{r} c_i(\mathcal{O}_{P(\mathcal{E})}(1))^i \cap \pi^* \text{CH}_{k+i}(X).
\]

is an isomorphism.

In particular, if \( X \) is integral, then

\[
\text{Cl}(P(\mathcal{E})) = \pi^*(\text{Cl}(X)) \oplus [c_1(\mathcal{O}_{P(\mathcal{E})}(1))].
\]

Proof: Cf. [Sta]02TX.

Prop. (6.1.7.11) [Vector Bundles]. If \( X \in \text{Sch}^{\text{loc.flt}} / S, r \in \mathbb{Z}_+, \mathcal{L} \in \text{Vect}^r(X) \), let \( \pi : E = \text{Spec}(\text{Sym}(\mathcal{E})) \to X \) be the vector bundle of \( \mathcal{E} \), then for any \( k \in \mathbb{Z} \), \( p^* : \text{CH}_k(X) \to \text{CH}_{k+r}(X) \) is an isomorphism.

Proof: Cf. [Sta]02TY.

Vector Bundles

Prop. (6.1.7.12) [Splitting Principle]. Let \( X \in \text{Sch}^{\text{loc.flt}} / S, \mathcal{E}_i \subset \text{Vect}(X) \) be a finite set of finite locally free sheaves, there exists a projective flat morphism \( \pi : P \to X \) of relative dimension \( d \) s.t.

- For any \( Y \in \text{Sch}^{\text{loc.flt}} / X \), the map \( \pi_*^Y : \text{CH}^*(Y) \to \text{CH}^*(Y \times_X P) \) is injective.
- Each \( \pi^* \mathcal{E}_i \) has a filtration with invertible quotient sheaves.

This is useful in the way that when proving functorial properties of Chern classes of vector bundles, we can reduce to invertible sheaves.

Proof: Cf. [Sta]02UL.

Prop. (6.1.7.13) [Chern Classes of Vector Bundles]. Let \( X \in \text{Sch}^{\text{loc.flt}} / S, r \in \mathbb{Z}_+, \mathcal{E} \subset \text{Vect}^r(X) \) with projective bundle \( \pi : P(\mathcal{E}) \to X \), then for any \( k, p \in \mathbb{N} \), there is a map

\[
c_p(\mathcal{E}) \cap - : \text{CH}_k(X) \to \text{CH}_{k-p}(X)
\]

called intersection with Chern classes as follows (the name will be made clear in (6.1.7.14)): Let \( \alpha \in \text{CH}_k(X) \), by (6.1.7.10) there are unique elements \( c_p \in \text{CH}_{k-p}(X) \) s.t. \( c_0 = \alpha \) and

\[
\sum_{p=0}^{r} (-1)^p c_1(\mathcal{O}_{P(\mathcal{E})})^p \cap \pi^* c_{r-p} = 0 \in \text{CH}_{k-1}(P(i^* \mathcal{E}))).
\]

Then define \( c_p(\mathcal{E}) \cap \alpha = c_p \).

In particular, if \( \mathcal{E} \) is an invertible sheaf, \( c_1(\mathcal{E}) \cap \) is just the intersection with the first Chern class \( c_1(\mathcal{E}) \cap \alpha \).
Prop.(6.1.7.14) [Chern Classes Form Bivariant Classes]. Let $X \in \text{Sch}^{\text{loc.ft}}/X, r \in \mathbb{Z}_+, \mathcal{E} \in \text{Vect}^r(X)$, then the maps $c_p(f^* \mathcal{E}) \cap - : \text{CH}_k(X') \to \text{CH}_{k-p}(X')$ for each $f : X' \to X \in \text{Sch}^{\text{loc.ft}}/X, k \in \mathbb{Z}_+$, form a bivariant class in $A^p(X)$, called the Chern classes $c_p(\mathcal{E})$. By convention, set $c_p(\mathcal{E}) = 0$ for $p > r$.

And $c(\mathcal{E}) = \sum_{i=0}^r c_i(\mathcal{E}) \in A^r(X)$ are called the total Chern class of $\mathcal{E}$.

Proof: For commuting with proper pushforward, use the definition(6.1.7.13) and (6.1.2.24)(6.1.7.5), and push and pull(6.1.2.16).

For commuting with flat pullback, use the definition(6.1.7.13) and (6.1.2.24)(6.1.7.5) and properties of flat pullbacks(6.1.2.13).

For commuting with Gysin map, use the definition(6.1.7.13) and (6.1.2.24)(6.1.7.5) and properties of Gysin maps(6.1.6.9). □

Prop.(6.1.7.15) [Chern Classes Commute with Bivariant Classes]. Let $f : X' \to X \in \text{Sch}^{\text{loc.ft}}/S$ and $\mathcal{E} \in \text{Vect}^r(X)$, then for any $p \in \mathbb{Z}_+$, $c_p(\mathcal{E})$ commutes with every element of $A^r(X' \to X)$.

In particular, $c_p(\mathcal{E})$ are in the center of $A^*(X)$, and for $\mathcal{E} \in \text{Vect}^r(X), F \in \text{Vect}^s(X), p, q \in \mathbb{Z}_+$, $c_p(\mathcal{E}), c_q(F)$ commute.

Proof: Reduce to $c_1$ and (6.1.7.6) as we did in (6.1.7.14). □

Prop.(6.1.7.16) [Chern Classes for Arbitrary Vector Bundles]. Let $X \in \text{Sch}^{\text{loc.ft}}/X, \mathcal{E} \in \text{Vect}^r(X)$, then constancy of $r$ induces a clopen partition of $X = \bigsqcup_{i=0}^\infty X_i$, where $X_i$ are the clopen subscheme s.t. $\delta = i$. Then by (6.1.6.8), $A^p(X) = \bigsqcup_{i=0}^\infty A^p(X_i)$, so we can define the Chern class $c_p(\mathcal{E})$ to be the product of $c_p(\mathcal{E}|_{X_i})$. Also we can define a rank class $r(\mathcal{E}) \in A^0(X) = \bigsqcup_{i=0}^\infty A^0(X_i)$ that is product of $[\mathcal{E}] \in A^0(X_i)$.

Prop.(6.1.7.17) [Additivity]. Let $X \in \text{Sch}^{\text{loc.ft}}/S$ and $0 \to \mathcal{E}_1 \to \mathcal{E} \to \mathcal{E}_2 \to 0 \in \text{Vect}(X)$, then

$$c(\mathcal{E}) = c(\mathcal{E}_1)c(\mathcal{E}_2).$$

Proof: It suffices to check this by their action on $[X]$ where $X \in \text{Sch}^{\text{loc.ft.int}}/S$. Using splitting principle(6.1.7.12), we can easily reduce to the case $\mathcal{E}_1, \mathcal{E}_2 \in \text{Pic}(X)$ by induction on $\text{rank}(\mathcal{E}_1)$ and $\text{rank}(\mathcal{E}_2)$. In this case, let $P$ be the projective bundle of $\mathcal{E}$ with $\mathcal{O}(1) = \mathcal{O}_P(1)$. By tag02U6, it suffices to show that

$$c_1(\mathcal{O}(1))^2 \cap \pi^* \alpha - c_1(\mathcal{O}(1)) \cap \pi^*(c_1(\mathcal{E}_1) \cap \alpha + c_1(\mathcal{E}_2) \cap \alpha) + \pi^*(c_1(\mathcal{E}_1) \cap c_1(\mathcal{E}_2) \cap \alpha).$$

for which it suffices to show that

$$(c_1(\mathcal{O}(1)) - c_1(\pi^* \mathcal{E}_1)) \cap (c_1(\mathcal{O}(1)) - c_1(\pi^* \mathcal{E}_2)) = c_1(\pi^* \mathcal{E}_1^\vee(1)) \cap c_1(\pi^* \mathcal{E}_2^\vee(1)) = 0$$

There is a surjection $\mathcal{E} \to \mathcal{O}(1)$, which corresponds to a non-zero section of $\mathcal{E}^\vee(1)$. Notice there is an exact sequence

$$0 \to \mathcal{E}_2^\vee \to \mathcal{E}^\vee(1) \to \mathcal{E}_1^\vee \to 0,$$

so the assertion follows from (6.1.7.8). □

Prop.(6.1.7.18). Let $X \in \text{Sch}^{\text{loc.ft}}/S$ and $\mathcal{E} \in \text{Vect}^r(X)$, then $c_1(\wedge \mathcal{E}) = c_1(\mathcal{E})$, and

$$\prod_{p=0}^r c(\wedge^p \mathcal{E})(-1)^n = 1 - (r - 1)!c_r(\mathcal{E}) + \ldots.$$
Proof: Use splitting principle and Cf.[Sta]0FEE. □

Prop.(6.1.7.19) [Degrees and First Chern Classes]. Let $X$ be a proper scheme over a field $k$, then

- Let $\mathcal{L}_1, \ldots, \mathcal{L}_d$ be invertible sheaves on $X$ and $Z \subset X$ a closed subscheme of dimension $d$, then

$$(\mathcal{L}_1 \cdot \ldots \cdot \mathcal{L}_d; Z) = \deg(c_1(\mathcal{L}_1) \cap \ldots \cap c_1(\mathcal{L}_d) \cap [Z]_d).$$

In particular, if $\mathcal{L}$ is an ample invertible sheaf,

$$\deg(\mathcal{L})(Z) = \deg(c_1(\mathcal{L})^d \cdot [Z]_d).$$

- If $\dim X \leq 1$, for $\mathcal{E} \in \mathcal{Coh}^{\text{free}}(X)$,

$$\deg(\mathcal{E}) = \deg(c_1(\mathcal{E}) \cdot [X]_1).$$

Proof: Cf.[Sta]0AZ3, 0BFI.? □

Prop.(6.1.7.20) [Chern Characters]. Let $X \in \text{Sch}^{\text{loc,ft}}/S$, $r$ a locally constant $\mathbb{Z}$-valued functions on $X$ and $\mathcal{E} \in \mathcal{V}ect^r(X)$, define the Chern character of $\mathcal{E}$ to be

$$\text{ch}(\mathcal{E}) = \text{rank}(\mathcal{E}) + \sum_{p \geq 0} \frac{P_p(c_1(\mathcal{E}), \ldots, c_n(\mathcal{E}))}{p!} \in \prod_{i \geq 0} A^i(X)_{\mathbb{Q}}$$

$$= \text{rank}(\mathcal{E}) + c_1(\mathcal{E}) + \frac{1}{2}(c_1(\mathcal{E})^2 - 2c_2(\mathcal{E})) + \frac{1}{6}(c_1(\mathcal{E})^3 - 3c_1(\mathcal{E})c_2(\mathcal{E}) + 3c_3(\mathcal{E}))$$

$$+ \frac{1}{24}(c_1(\mathcal{E})^4 - 4c_1(\mathcal{E})^2c_2(\mathcal{E}) + 4c_1(\mathcal{E})c_3(\mathcal{E}) + 2c_2(\mathcal{E})^2 - 4c_4(\mathcal{E})) + \ldots$$

where $P_p$ are Chern polynomials(2.2.2.17).

Prop.(6.1.7.21) [Tensor Products]. If $X \in \text{Sch}^{\text{loc,ft}}/S$, $r, s, t$ are locally constant $\mathbb{Z}$-valued functions on $X$ and $\mathcal{E} \in \mathcal{V}ect(X)$, $\mathcal{F} \in \mathcal{V}ect(X)$, $\mathcal{G} \in \mathcal{V}ect(X)$, then

- If there is an exact sequence $0 \to \mathcal{E} \to \mathcal{G} \to \mathcal{F} \to 0$, then $\text{ch}(\mathcal{E}) + \text{ch}(\mathcal{F}) = \text{ch}(\mathcal{G})$.

- $\text{ch}(\mathcal{E} \otimes_{\mathcal{O}_X} \mathcal{F}) = \text{ch}(\mathcal{E}) \text{ch}(\mathcal{F})$.

- $\text{ch}_i(\mathcal{E}^r) = (-1)^i \text{ch}_i(\mathcal{E})$.

In particular, ch defines a ring homomorphism $\text{ch} : K_0(\mathcal{V}ect(X)) \to \prod_{i \geq 0} A^i(X)_{\mathbb{Q}}$.

Proof: It suffices to prove for $X$ connected, and then by(6.1.7.12), we can assume $\mathcal{E}, \mathcal{F}$ have filtrations with invertible quotient sheaves $\mathcal{E}_1, \ldots, \mathcal{E}_r$ and $\mathcal{F}_1, \ldots, \mathcal{F}_s$ with first Chern characters $a_1, \ldots, a_r$ and $b_1, \ldots, b_s$, then by additivity(6.1.7.17) and the definition of Chern polynomials(2.2.2.17), we see

$$\text{ch}(\mathcal{E}) = \sum_{i=1}^{r} \exp(a_i), \quad \text{ch}(\mathcal{F}) = \sum_{j=1}^{s} \exp(b_j),$$

and $\mathcal{E} \otimes \mathcal{F}$ has a filtration with quotient sheaves $\mathcal{E}_i \otimes \mathcal{F}_j$ with first Chern characters $a_i + b_j$ by(6.1.7.2), so the assertions are now clear. □
Cor. (6.1.7.22) [Chern Classes of Tensor Products]. If $X \in \mathbb{S}ch_{\text{loc.ft}}/S$, $r, s$ are locally constant \mathbb{Z}-valued functions on $X$ and $\mathcal{E} \in \mathbb{V}ect^r(X), \mathcal{F} \in \mathbb{V}ect^s(X)$, then

$$c_1(\mathcal{E}^r) = (-1)^ic_i(\mathcal{E}) \in A^i(X),$$

$$c_1(\mathcal{E} \otimes \mathcal{F}) = r c_1(\mathcal{E}) + sc_1(\mathcal{F}) \in A^1(X),$$

$$c_2(\mathcal{E} \otimes \mathcal{F}) = r c_2(\mathcal{F}) + sc_2(\mathcal{E}) + \left(\frac{r}{2}\right)c_1(\mathcal{F})^2 + (rs - 1)c_1(\mathcal{E})c_1(\mathcal{F}) + \left(\frac{s}{2}\right)c_1(\mathcal{E})^2 \in A^2(X),$$

$$c_2(\text{Hom}(\mathcal{E}, \mathcal{E})) = 2rc_2(\mathcal{E}) - (r - 1)c_1(\mathcal{E})^2 \in A^2(X).$$

Prop. (6.1.7.23) [Todd Classes]. Let $X \in \mathbb{S}ch_{\text{loc.ft}}/S$ and $\mathcal{E} \in \mathbb{V}ect(X)$, define the Todd class $\text{Todd}(\mathcal{E})$ of $\mathcal{E}$ to be

$$\text{Todd}(\mathcal{E}) = \text{Todd}(c_1(\mathcal{E}), c_2(\mathcal{E}), \ldots)(2.2.2.18) = 1 + \frac{1}{2}c_1(\mathcal{E}) + \frac{1}{12}(c_1(\mathcal{E})^2 + c_2(\mathcal{E}))$$

$$+ \frac{1}{24}c_1(\mathcal{E})c_2(\mathcal{E}) + \frac{1}{720}(-c_1^4(\mathcal{E}) + 4c_1^2(\mathcal{E})c_2(\mathcal{E}) + 3c_2^2(\mathcal{E}) + c_1(\mathcal{E})c_3(\mathcal{E}) - c_4(\mathcal{E})) + \ldots .$$

Then if $0 \rightarrow \mathcal{E}' \rightarrow \mathcal{E} \rightarrow \mathcal{E}'' \rightarrow 0 \in \mathbb{V}ect(X)$ be an exact sequence, then $\text{Todd}(\mathcal{E})\text{Todd}(\mathcal{E}'') = \text{Todd}(\mathcal{E})$.

Proof: The proof is the same as that of (6.1.7.21). □

Prop. (6.1.7.24) [Borel-Serre]. Let $X \in \mathbb{S}ch_{\text{loc.ft}}/S$ and $\mathcal{E} \in \mathbb{V}ect^r(X)$, then

$$\sum_{p=0}^{r} (-1)^p \text{ch}(\wedge^p \mathcal{E}^r) = c_r(\mathcal{E})\text{Todd}(\mathcal{E})^{-1}.$$ 

Proof: ? □

Prop. (6.1.7.25) [Chern Classes of K-Groups]. $X \in \mathbb{S}ch_{\text{loc.ft}}/S$, by additivity and multiplicativity(6.1.7.17)(6.1.7.21), we can extend Chern classes and Chern characters to the K-group $K_0(\mathbb{V}ect(X))$:

$$c : K_0(\mathbb{V}ect(X)) \rightarrow \prod_{p \geq 0} A^p(X), \quad \text{ch} : K_0(\mathbb{V}ect(X)) \rightarrow \prod_{p \geq 0} A^p(X)_\mathbb{Q}$$

where $c$ is a group homomorphism and $\text{ch}$ is a ring homomorphism.

Prop. (6.1.7.26) [Adam Operators and Chern Characters]. $X \in \mathbb{S}ch_{\text{loc.ft}}/S$ and $\alpha \in K_0(\mathbb{V}ect(X))$, then $c_i(\psi^k(\alpha)) = 2^{ki}c_i(\alpha)$ and $\text{ch}_i(\psi^k(\alpha)) = 2^{ki}\text{ch}_i(\alpha)$.

Proof: It suffices to prove for $\alpha = [\mathcal{E}]$ where $\mathcal{E} \in \mathbb{V}ect(X)$, then by splitting principle it suffices to prove for line bundles, and this is clear from (6.1.7.22) and the definition (6.1.7.20)t. □
Perfect Complexes

**Lemma (6.1.7.27).** Let \( X \in \text{Sch}^{\text{loc.\,ft}} / S \), then for each perfect complex \( \mathcal{E} \) in \( D(\mathcal{O}_X) \), we can define the Chern classes, Chern characters and ranks of \( \mathcal{E} \). But we only define for a subset of \( E \) here? Cf.[Sta]0F9E: If \( \mathcal{E} \) is represented by a finite complex \( \mathcal{E}^\bullet \) of vector bundles on \( X \), define

\[
c(\mathcal{E}) = \prod_i c(\mathcal{E}^i)^{(-1)^i} \in \prod_i A^i(X), \quad ch(\mathcal{E}) = \sum_i (-1)^i ch(\mathcal{E}^i) \in \prod_i A^i(X)_Q, \quad r(\mathcal{E}) = \sum_i (-1)^i r(\mathcal{E}^i).
\]

**Proof:** To show this is well defined.

**Prop. (6.1.7.28) [Chern Classes via Envelopes].** Let \( Y \rightarrow X \in \text{Sch}^{\text{loc.\,ft}} / S \) be an envelope, \( \mathcal{E} \) perfect in \( D(\mathcal{O}_X) \) s.t. \( Lf^* \mathcal{E} \) is representable by a finite complex of vector bundles on \( Y \), then there are unique bivariant classes \( c(\mathcal{E}) \in \prod_i A^i(X), ch(\mathcal{E}) \in \prod_i A^i(X)_Q, \quad r(\mathcal{E}) \) s.t. their restrictions to \( Y \) are of the form defined in (6.1.7.27).

Moreover, these bivariant classes are invariant of the envelope chosen. In this case, we say the Chern classes of \( \mathcal{E} \) are defined.

**Proof:** Cf.[Sta]0GUD.

**Prop. (6.1.7.29).** If \( X \in \text{Sch}^{\text{loc.\,ft}} / S \) and each irreducible components of \( X \) are qc, then \( X \) has an envelope. In particular, this applies to \( X \) qc.

**Proof:** Cf.[Sta]0GUE?

**Prop. (6.1.7.30) [Additivity].** If \( X \in \text{Sch}^{\text{loc.\,ft}} / S \) and \( \mathcal{E}_1 \rightarrow \mathcal{E}_2 \rightarrow \mathcal{E}_3 \rightarrow \mathcal{E}_1[1] \) is a distinguished triangle of perfect complexes in \( D(\mathcal{O}_X) \), and one of the following holds:

- There exists an envelope \( f : Y \rightarrow X \) s.t. \( Lf^* \mathcal{E}_1 \rightarrow Lf^* \mathcal{E}_2 \) is representable by a map of finite complexes of vector bundles on \( Y \).

- Each irreducible components of \( X \) is irreducible.

Then Chern classes of \( \mathcal{E}_i \) are defined, and

\[
c(\mathcal{E}_2) = c(\mathcal{E}_1)c(\mathcal{E}_3), \quad ch(\mathcal{E}_2) = ch(\mathcal{E}_1) + ch(\mathcal{E}_3).
\]

**Proof:** Cf.[Sta]0F9F?.

**Prop. (6.1.7.31).** If \( X \in \text{Sch}^{\text{loc.\,ft}} / S \) and \( \mathcal{E} \) be a perfect object in \( D(\mathcal{O}_X) \) whose Chern classes are defined, then

- Let \( f : X' \rightarrow X \in \text{Sch}^{\text{loc.\,ft}} / S, p \in \mathbb{Z}_+ \), then \( c_p(\mathcal{E}) \) commutes with every element of \( A^*(X' \rightarrow X) \), i.e. \( c \cdot c_p(\mathcal{E}) = c_p(Lf^* \mathcal{E}) \cdot c \).

In particular, \( c_p(\mathcal{E}) \) are in the center of \( A^*(X) \), and for \( \mathcal{E}, \mathcal{F} \) perfect in \( D(\mathcal{O}_X) \) whose Chern classes are defined, \( p, q \in \mathbb{Z}_+, c_p(\mathcal{E}), c_q(\mathcal{F}) \) commute.

- \( \log(c(\mathcal{E})) = \sum_{p \geq 0} P_p(c_1(\mathcal{E}), \ldots, c_n(\mathcal{E})) \) also holds, where \( P_p \) are Chern polynomials (2.2.2.17). Similarly for Chern character \( ch(\mathcal{E}) \).

- \( c_i(\mathcal{E}^\vee) = (-1)^i c_i(\mathcal{E}), ch_i(\mathcal{E}^\vee) = (-1)^i ch_i(\mathcal{E}) \).

**Proof:** These follow from the splitting principle and the definition (6.1.7.28).
Prop. (6.1.7.32) [Tensor Products]. If \( X \in \text{Sch}_{\text{loc.ft}}^{\text{ft}} / S \) and \( E, F \) perfect in \( D(O_X) \) whose Chern classes are defined, then
\[
\text{ch}(E \otimes_{O_X}^L F) = \text{ch}(E) \text{ch}(F),
\]
in particular, formulas in (6.1.7.22) hold.

Proof: This follows from the splitting principle and the definition (6.1.7.28).

\[\Box\]

8 Non-Singular Intersection Theory

Lemma (6.1.8.1). If \( X \in \text{Sch}_{\text{reg}, \text{qc}}^{\text{ft,sep}} / S \) with bounded \( \delta \)-dimension, then the composition
\[
K_0(\text{Vect}(X)) \otimes \mathbb{Q} \xrightarrow{\text{ch}} \prod_{p \geq 0} A^p(X) \xrightarrow{-\cap [X]} \text{CH}^*(X) \otimes \mathbb{Q}
\]
is an isomorphism.

Proof: Firstly \( K_0(X) = K_0^r(X) = K_0(\text{Vect}(X)) \) by (5.8.5.33) and (5.8.5.36).
The rest follows from [Sta]0FEY.

Prop. (6.1.8.2) [Q-Intersection Products on Regular Schemes]. If \( X \in \text{Sch}_{\text{reg}, \text{qc}}^{\text{ft,sep}} / S \) with bounded \( \delta \)-dimension, then the isomorphism \( K_0(\text{Vect}(X)) \otimes \mathbb{Q} \cong \text{CH}^*(X) \otimes \mathbb{Q} \) endows \( \text{CH}^*(X)_{\mathbb{Q}} \) with a commutative associative ring structure: If \( \alpha = \text{ch}(\alpha^r) \cap [X], \beta = \text{ch}(\beta^i) \cap [X] \), then
\[
\alpha \cdot \beta = \text{ch}(\alpha) \cap \text{ch}(\beta) \cap [X] = \text{ch}(\alpha^r) \cap \beta = \text{ch}(\beta^i) \cap \alpha.
\]
And this ring structure preserves the gradation on \( \text{CH}^*(X)_{\mathbb{Q}} \). Also it is preserved under morphism in \( \text{Sch}_{\text{reg}, \text{qc}}^{\text{ft,sep}} \) flat of relative dimension \( r \).

Proof: To prove it preserves gradation, suppose \( \alpha \in \text{CH}^i(X), \beta \in \text{CH}^j(X) \), then \( \alpha^r \) and \( 2^{-i} \psi^2(\alpha^i)(6.1.7.26) \) are both inverse images of \( \alpha \), so they are equal. Then \( \text{ch}(\alpha^r) = \text{ch}(2^{-i} \psi^2(\alpha)) \), which means \( \text{ch}(\alpha^r) \in A^i(X)_{\mathbb{Q}} \), and then \( \text{ch}(\alpha^r) \cap \beta \in \text{CH}^{i+j}(X)_{\mathbb{Q}} \).

\[\Box\]

Smooth over Dedekind Schemes Case

Smooth over Fields Case

Prop. (6.1.8.3) [Exterior Products]. If \( k \in \text{Field}, S = \text{Spec} \, k, X, Y \in \text{Sch}_{\text{loc.ft}}^{\text{ft}} / k \), there is an exterior product map
\[
\text{CH}_n(X) \otimes \text{CH}_m(Y) \to \text{CH}_{n+m}(X \times_S Y)
\]
defined by sending \( [X'] \otimes [Y'] \) to \( [X' \times_S Y']_{n+m} \), where \( X' \subset X, Y' \subset Y \) are integral closed subschemes of dimension \( n \) and \( m \) resp.

Proof: To show this is well defined, consider \( i : X' \to X, c : X \to \text{Spec} \, k \), then by (6.1.6.11), \( c_a \circ (c \circ i)^* \in A^{-n}(X \to \text{Spec} \, k) \), which sends \( [Y'] \) to \( [X' \times_k Y']_{n+m} \), so this map factors through rational equivalences on \( Y \), and similarly it factors through rational equivalences on \( X \).

\[\Box\]

Prop. (6.1.8.4). If \( k \in \text{Field}, S = \text{Spec} \, k \) and \( X \in \text{Sch}_{\text{loc.ft}}^{\text{ft}} / k \), there is a natural isomorphism
\[
A^p(X \to \text{Spec} \, k) \cong \text{CH}_{-p}(X)
\]
for any \( p \in \mathbb{Z} \).
Proof: The map $A^p(X \to \text{Spec } k) \to \text{CH}_{-p}(X)$ is given by $c \mapsto c \cap [\text{Spec } k]$. Conversely, for any $\alpha \in \text{CH}_{-p}(X)$, we can define for any $X' \in \text{Sch}^{\text{loc. ft.}} / k$ a map

$$\text{CH}_n(X') \to \text{CH}_{n-p}(X \times_k X') : \beta \mapsto \alpha \times \beta \tag{6.1.8.3}. $$

Then this is a bivariant class in $A^p(X \to \text{Spec } k)$: Let $\alpha = \sum n_i [X_i]$, and let $g : \coprod_i X_i \to X$, $f : \coprod_i X_i \to \text{Spec } k$. Denote $\nu^* \in A^0(\coprod_i X_i)$ the bivariant class that multiplies by $n_i$ at each component $X_i$, then $g_* \circ \nu \circ f^* \in A^p(X \to \text{Spec } k)$ by (6.1.6.10)(6.1.6.11), and this is just the map we defined above.

To show these two maps are inverse to each other, one direction is clear. To show $c(\beta) = (c \cap [\text{Spec } k]) \times \beta$, it suffices to show for $\beta = [X']$ is integral, then $\beta = (X' \to \text{Spec } k)^*[\text{Spec } k]$, then it is easy to see they are equal because $c$ commutes with flat pullbacks $(X' \to \text{Spec } k)^*$. \hfill \Box

Cor. (6.1.8.5) [Commutativity and Associativity]. If $k \in \text{Field}$, $S = \text{Spec } k$ and $X \in \text{Sch}^{\text{loc. ft.}} / k$, then $c \in A^p(X \to \text{Spec } (k))$ commutes with any $c' \in A^q(Y \to Z)$ for any $f : Y \to Z \in \text{Sch}^{\text{loc. ft.}} / k$. In other words, for any $\alpha \in \text{CH}_*(X), \beta \in \text{CH}_*(Z)$ and $c \in A^*(Y \to Z)$,

$$\alpha \times (c \cap \beta) = c \cap (\alpha \times \beta) \in \text{CH}_*(X \times_k Y).$$

In particular, if $\gamma \in \text{CH}_*(Y)$, then

$$(\alpha \times \beta) \times \gamma = \alpha \times (\beta \times \gamma) \in \text{CH}_*(X \times_k Y \times_k Z).$$

Proof: This is because $c = g_* \circ \nu \circ f^*$ as in the proof of (6.1.8.4). \hfill \Box

Prop. (6.1.8.6) [Perturbation and Chow Rings]. Any two algebraic cycles $\gamma_1, \gamma_2 \in \text{Z}_*(X)$ are rationally equivalent to cycles $\gamma_1', \gamma_2'$ s.t. $\gamma_1', \gamma_2'$ intersect properly. And the rational class of resulting intersection cycle is well-defined. So there is an intersection on $\text{CH}^*(X)$ making it a commutative ring, called the **Chow ring of $X$**.

Proof: \hfill \Box

Prop. (6.1.8.7) [Bezout]. The Chow ring of $\mathbb{P}_k^n$ is isomorphic to $\mathbb{Z}[x]/(x^{n+1})$. The degree of an irreducible closed variety corresponds to the coefficient of it.

Proof: \hfill \Box

Def. (6.1.8.8) [Euler Characteristic]. If $X$ is a smooth scheme over a field $k$ of dimension $d$ with tangent bundle $T_{X/k}$, the **Euler characteristic** of $X$ is defined to be $\text{deg}(c_d(T_{X/k}) \cap [X])$, and the **Todd characteristic** of $X$ is defined to be $\text{deg}(\text{Todd}_d(T_{X/k}) \cap [X])$.

Prop. (6.1.8.9). If $X$ is a smooth scheme over a field $k$ and $i : Y \to X$ is a regular closed immersion and $Y$ is equidimensional of dimension $e$, then

$$[Y]_e \cdot \alpha = i_* (i^!(\alpha)).$$

Proof: Cf. [Sta]0FFE?. \hfill \Box
Serre’s Approach

Prop. (6.1.8.10). If $X$ is an integral scheme smooth over a field $k$, and $W,V$ be two integral closed subschemes of $X$, then $	ext{codim}(W \cap V) \leq \text{codim}(W) + \text{codim}(V)$.

Proof: Cf. [Sta]0AZP.

Def. (6.1.8.11) [Proper Intersections]. Let $X$ be an integral scheme smooth over a field $k$, then two cycles $\alpha = \sum n_i [W_i]$ and $\beta = \sum m_j [V_j]$ are said to intersect properly iff

$$\text{codim}(W_i \cap V_j) \geq \text{codim}(W_i) + \text{codim}(V_j).$$

And in fact equality holds, by (6.1.8.10).

Lemma (6.1.8.12) [Tor Sheaves]. Let $X$ be an integral scheme smooth over a field $k$ and $F,G \in \text{Coh}(X)$, then $\text{Tor}_p^{O_X}(F,G) \in \text{Coh}(X)$, with stalk at $x \in X$ being $\text{Tor}_p^{O_{X,x}}(F_x,G_x)$, and is supported on $\text{Supp}(F) \cap \text{Supp}(G)$, and nonzero only for $0 \leq p \leq \dim X$.

Proof: Cf. [Sta]0AZT.

Def. (6.1.8.13) [Intersection via Tor]. Let $X$ be a regular scheme and $W,V \subset X$ be integral closed subschemes intersecting properly, by (6.1.8.12) we can define the intersection product

$$W \cdot V = \sum [\text{Tor}_i^{O_X}(O_W,O_V)]_{r+s-\dim X},$$

and for any irreducible component $Z$ of $W \cap V$ the intersection multiplicities

$$e(X,W \cdot V,Z) = \sum (-1)^i \text{length}_{O_{X,Z}} \text{Tor}_i^{O_{X,Z}}(O_W,Z,O_V,Z).$$

Proof: Why is this compatible with the definition given before? Why the multiplicity is given by this form?

Remark (6.1.8.14) [Serre Conjecture]. Serre conjectured that in (6.1.8.13), even if $W,V$ doesn’t intersect properly, for an irreducible component $Z \subset W \cap V$ of dimension $\geq \dim W + \dim V - \dim X$, we have $e(X,W \cdot V,P) = 0$.

Prop. (6.1.8.15) [Discrete Case]. Let $X$ be an integral scheme smooth over $k$ and $W,V \subset X$ be closed subvarieties that intersect properly. Let $Z$ be an irreducible component of $V \cap W$ with generic point $\xi$ and $O_{W,\xi}, O_{V,\xi}$ are both C.M., then

$$e(X,W \cdot V,Z) = \text{length}_{O_{X,\xi}}(O_{V \cap W,\xi}).$$

Proof: Cf. [Sta]0B02.

Prop. (6.1.8.16) [Exterior Product of Subvarieties]. Let $X,Y$ be integral schemes smooth over $k$ and $W \subset X, V \subset Y$ be subvarieties, then $[W] \times [V] = ([W] \times [Y]) \cdot ([X] \times [V]) \in Z_*(X \times Y)$.

Proof: As $W \times V$ is a variety with generic point $\xi$, and $X$ is smooth over $k$, $X \times V$ is smooth over $V$, thus $O_{X \times V,\xi}$ is regular, hence C.M., and similarly is $O_{W \times Y,\xi}$, thus (6.1.8.15) applies to show that $([W] \times [Y]) \cdot ([X] \times [V]) = [W] \times [V]$. 

□
Prop. (6.1.8.17) [Serre]. If $X$ is a integral scheme smooth over a field $k$, $F \in \text{Coh}_{r}(X)$, $G \in \text{Coh}_{s}(X)$, and $\dim(\text{Supp}(F) \cap \text{Supp}(G)) \leq r + s - \dim X$. Then $[F]_r$ and $[G]_s$ intersect properly, and

$$[F]_r \cdot [G]_s = \sum_{p} (-1)^p [\text{Tor}_p^O(X, G)]_{r+s-\dim X}$$

Proof: Cf. [Sta]0B0W. □

Cor. (6.1.8.18). If $X$ is a smooth integral scheme over a field $k$, the intersection product on $\text{CH}^*(X)$ makes it a commutative graded (associative, unital) ring.

Proof: To show the intersection is associative, let $U, V, W$ be closed subvarieties of $X$ s.t. $\text{codim}(U \cap V \cap W, X) = \text{codim}(U, X) + \text{codim}(V, X) + \text{codim}(W, X) = p$, then it suffices to show that

$$\sum_{i}(-1)^i \text{Tor}_i(\text{O}_U, \text{Tor}_j(\text{O}_V, \text{O}_W))_{\dim X - p} = \sum_{i}(-1)^i \text{Tor}_i(\text{Tor}_j(\text{O}_U, \text{O}_V), \text{O}_W)_{\dim X - p}.$$

This is true because they are both equal to

$$\sum_k (-1)^k \text{H}^k(\text{O}_U \otimes L \text{O}_V \otimes L \text{O}_W)_{\dim X - p}$$

which is because there is an spectral sequence convergence

$$E_2^{p,q} = \text{Tor}_p^O(\text{O}_U, \text{Tor}_q^O(\text{O}_V, \text{O}_W)) \Rightarrow \text{H}^{p+q}(\text{O}_U \otimes L \text{O}_V \otimes L \text{O}_W)$$

and use the fact length functions are additive. □

9 Numerical Geometry

Let $k \in \text{Field}$ and $k = \bar{k}$.


Prop. (6.1.9.1) [Schubert Cycles of the Grassmannian].

Prop. (6.1.9.2). Given 4 curves $C_1, \ldots, C_4$ in $\mathbb{P}^3_k$ of degree $d_1, \ldots, d_4$, there are $2d_1d_2d_3d_4$ lines intersecting all of them.

Proof: □

Prop. (6.1.9.3). Use the projective bundle formula to show that given 9 lines $L_1, \ldots, L_8 \in \mathbb{P}^2_k$ in general position, there are 92 conics meeting all $L_i$.

Proof: □

Prop. (6.1.9.4). Show that given two general twisted cubic curves $C, C' \in \mathbb{P}^3_k$, they have 10 common chords.

Proof: □
6.1. INTERSECTION THEORY

**Prop.** (6.1.9.5). Show that given a general quintic surface \( S \in \mathbb{P}^3_k \), there are 575 lines meeting \( S \) at only one point.

*Proof:*

**Prop.** (6.1.9.6). Show that given 5 general conics \( S_1, \ldots, S_r \) in \( \mathbb{P}^3_k \), there are 3264 conics tangent to all \( S_i \).

*Proof:*

10 Riemann-Roch

Main references are [Ful98] Chap15, 18.

**Prop.** (6.1.10.1) [Grothendieck-Riemann-Roch]. Let \( f : X, Y \in \text{Sch}^{\text{loc-ft}} / S \) be proper smooth, and \( \mathcal{E} \in \text{Coh}^{\text{free}}(X) \), \( T_{X/Y} \) the locally free relative tangent bundle, then

\[
 f_*(\text{Todd}(T_{X/Y}) \cdot \text{ch}(\mathcal{E})) = \sum_i (-1)^i \text{ch}(R^if_*\mathcal{E}).
\]

**Remark** (6.1.10.2). This theorem also has an Arithmetic version.

*Proof:*

**Cor.** (6.1.10.3) [Hirzebruch-Riemann-Roch]. If \( X \) is a smooth complete variety over a field \( k \), \( \mathcal{E} \in \text{Coh}^{\text{free}}(X) \), then

\[
 \chi(X, \mathcal{E}) = \int_X \text{Todd}(T_{X/k}) \cdot \text{ch}(\mathcal{E})
\]

**Cor.** (6.1.10.4). If \( X \) is a smooth complete variety over a field \( k \), then

\[
 \chi(X, \mathcal{O}_X) = \int_X \text{Todd}(T_{X/k}).
\]

Singular Case

11 Numerical Equivalences

**Def.** (6.1.11.1) [Numerical Equivalences]. Two cycles \( \gamma, \gamma' \in \text{CH}^k(X) \) are called **numerically equivalent** if for any \( \delta \in \text{Z}_k(X), \gamma \cdot \delta = \gamma' \cdot \delta \). And we can define \( GH_k(X) \) the **Grothendieck group of \( k \)-cycles** to be \( \text{Z}_k(X) \) modulo the numerical equivalence relation.

**Prop.** (6.1.11.2) [Grothendieck Rings]. There is a group homomorphism \( \text{CH}^*(X) \to GH^*(X) \) and the ring structure on \( \text{CH}^*(X) \) descends to \( GH^*(X) \), making it a ring, called the **Grothendieck ring of \( X \)**.

12 Intersection for Line Bundles

Main references are [FGA, Appendix B].
Algebraic Equivalence

Def. (6.1.12.1) [Algebraically Equivalent Line Bundles]. Let $X$ be a scheme over a field $k$, then $\mathcal{L}_1, \mathcal{L}_2 \in \text{Pic}(X)$ are called algebraically equivalent if they are equivalent in the equivalence relation $\mathcal{M} \sim \mathcal{N}$ iff there is a connected scheme $T$ and a line bundle $\mathcal{L} \in \text{Pic}_{X/k}(T)$ s.t. $\mathcal{N}_{k(t_1)} = \mathcal{L}_{t_1}$ and $\mathcal{M}_{k(t_2)} = \mathcal{L}_{t_2}$ where $t_1, t_2 \in T$.

Cor. (6.1.12.2) [Pic$^0(X)$]. The elements in Pic$(X)$ algebraically equivalent to 0 is a subgroup of Pic$(X)$, denoted by Pic$^0(X)$. In (6.1.12.4), we will see when $X$ has a rational point and Pic$_{X/k}$ is representable, this is just Pic$^0_{X/k}(k)$, by (7.7.3.7).

Prop. (6.1.12.3) [Algebraically Equivalent Divisors]. If $X$ is a regular $K$-prevariety, then Pic$(X) \cong \text{CH}^1(X)(5.5.3.15)$. We call two divisors $D_1, D_2$ on $X$ algebraically equivalent if $\mathcal{O}(D_1)$ and $\mathcal{O}(D_2)$ are algebraically equivalent.

Proof: Cf. [Diophantine Geometry, P563].

Prop. (6.1.12.4) [Moduli Characterization]. If $X$ is a scheme over a field $k$ s.t. Pic$_{X/k}$ is representable, then two line bundles are algebraically equivalent iff they correspond to points of Pic$_{X/k}$ in the same connected component.

Proof: By (7.7.3.20), Pic$_{X/k}$ is a locally algebraic group scheme over $k$, so by (7.1.4.13), every connected components of it is irreducible. Clearly two algebraically equivalent line bundles are in the same connected component of Pic$_{X/k}$. Conversely, the inclusion of their common connected component $P$ corresponds to a line bundle on some fppf covering $T \to P$. Then use the fact fppf covering is open map, and the fact $P$ is irreducible to get an algebraic equivalence chain.

Prop. (6.1.12.5) [Algebraic Equivalence for Curves]. If $C$ is a smooth complete curve over a field $k$, then two line bundles $\mathcal{L}_1, \mathcal{L}_2 \in \text{Pic}(C)$ are algebraically equivalent iff they have the same degree.

Proof: It suffices to show after base change to $\overline{k}$. Then it suffices to show for any two closed points $x_1, x_2 \in C$, $\mathcal{L}(x_1) \sim \mathcal{L}(x_2)$. Consider the diagonal of $C \times C$ is a Cartier divisor, and its restriction to $C \times \{x_i\}$ is $\mathcal{L}(x_i)$.

Numerical Intersections

Def. (6.1.12.6). Let $X$ be a proper scheme and $\mathcal{F}$ be a coherent sheaf with $\dim \text{Supp} \mathcal{F} \leq n$, and $\mathcal{L}_1, \ldots, \mathcal{L}_n$ are invertible sheaves on $X$, then we define $(\mathcal{L}_1 \cdot \ldots \cdot \mathcal{L}_n; \mathcal{F})$ to be

$$\sum_{\{i_1, \ldots, i_m\} \subset \{1, \ldots, n\}} (-1)^m \chi(X, \mathcal{L}_{i_1}^\vee \otimes \ldots \otimes \mathcal{L}_{i_m}^\vee \otimes \mathcal{F}).$$

When $\mathcal{F}$ is the structure sheaf of a closed subscheme $Y$, then denote $(\mathcal{L}_1 \cdot \ldots \cdot \mathcal{L}_n; \mathcal{F})$ by $(\mathcal{L}_1 \cdot \ldots \cdot \mathcal{L}_n; \mathcal{Y})$. This intersection is stable under base change of fields.

Prop. (6.1.12.7). If $X$ is a complete curve and $\mathcal{L}$ an invertible sheaf on $X$, then $(\mathcal{L}; X) = \deg(\mathcal{L})$.

Proof:

Prop. (6.1.12.8). If $k$ is an infinite field and $X = \mathbb{P}_k^n$, and $Y$ is a dimension $n$ subvariety of $X$. If $H_1, \ldots, H_n$ are generic chosen hypersurfaces of degree $d_1, \ldots, d_n$ resp., then

$$(\mathcal{O}_X(H_1) \cdot \ldots \cdot \mathcal{O}_X(H_n); Y) = d_1 \ldots d_n \deg(Y).$$
Proof:

Prop. (6.1.12.9). If \(D\) is an effective Cartier divisor on \(X\) that doesn’t contain any associated point of \(\mathcal{F}\), then
\[
(\mathcal{L}_1 \cdots \mathcal{L}_n \cdot \mathcal{O}(D); \mathcal{F}) = (\mathcal{L}_1|_D \cdots \mathcal{L}_n|_D; \mathcal{F}|_D)
\]

Proof:

Prop. (6.1.12.10). For a fixed \(\mathcal{F}\), \((\mathcal{L}_1 \cdots \mathcal{L}_n; \mathcal{F})\) is a symmetric multilinear function of \(\mathcal{L}_1, \cdots, \mathcal{L}_n\), where the addition is tensor production. Moreover, if \(\mathcal{F}\) is a coherent sheaf with support dimension \(n\), then \((\mathcal{L}_1 \cdots \mathcal{L}_{n+1}; \mathcal{F}) = 0\).

Proof: Cf. [Rising Sea, P544].

Prop. (6.1.12.11). The numerical intersection \((\mathcal{L}_1 \cdots \mathcal{L}_n; \mathcal{F})\) only depends on the numerical classes of \(\mathcal{L}_i\).

Prop. (6.1.12.12)[Projection Formula]. Let \(\pi : X_1 \to X_2\) be a proper morphism of proper schemes, then
\[
(\pi^* \mathcal{L}_1 \cdots \pi^* \mathcal{L}_n; \pi^* \mathcal{F}) = (\mathcal{L}_1 \cdots \mathcal{L}_n; \pi_* \mathcal{F}).
\]
In particular, when \(X_1, X_2\) are integral with the same dimensions and \(\pi\) is a finite map,
\[
(\pi^* \mathcal{L}_1 \cdots \pi^* \mathcal{L}_n) = \deg(\pi)(\mathcal{L}_1 \cdots \mathcal{L}_n).
\]

Proof: For the last assertion, notice \(\pi_* \mathcal{O}_{X_1} = \deg(\pi) \mathcal{O}_{X_2} + \) coherent sheaves with smaller supper dimensions.

Prop. (6.1.12.13). Let \(k\) be a field and \(X\) a proper scheme over \(k\), and \(Z \subset X\) a closed subscheme of dimension \(d\). If \(\mathcal{L}_1, \ldots, \mathcal{L}_d\) are ample invertible sheaves on \(X\), then \((\mathcal{L}_1 \cdots \mathcal{L}_d; Z)\) is positive.

Proof:

Prop. (6.1.12.14). Let \(X\) be a complex projective scheme, then \((\mathcal{L}_1 \cdots \mathcal{L}_n; Z)\) equals
\[
(c_1((\mathcal{L}_1)_\text{an}) \cup \cdots c_1((\mathcal{L}_n)_\text{an}), Z)
\]
where \(c_1\) is the complex Chern class.

Proof: Cf. [Rising Sea, P547].

Def. (6.1.12.15)[First Chern Class]. Let \(X\) be a proper scheme and \(K\) be the Grothendieck group of \(\text{Coh}(X)\). For \(\mathcal{L} \in \text{Pic}(X)\), define \(c_1(\mathcal{L})\) to be the endomorphism of \(K\) defined by
\[
c_1(\mathcal{L}) \mathcal{F} = \mathcal{F} - \mathcal{L}^{-1} \otimes \mathcal{F}.
\]

Prop. (6.1.12.16). If \(\mathcal{L}, \mathcal{M} \in \text{Pic}(X)\), then
- \(c_1(\mathcal{L})c_1(\mathcal{M}) = c_1(\mathcal{L}) + c_1(\mathcal{M}) - c_1(\mathcal{L} \otimes \mathcal{M})\).
- \(c_1(\mathcal{O}_X) = 0\).
- \(c_1(\mathcal{L})c_1(\mathcal{L}^{-1}) = c_1(\mathcal{L}) + c_1(\mathcal{L}^{-1})\).
In particular, $c_1(L)$ and $c_2(M)$ commutes.

**Prop. (6.1.12.17).** If $X$ is a proper scheme over a field $k$ and let $K^d$ be the subgroup generated by coherent sheaves over $X$ with support dimension $\leq d$, then if $F \in K^d$, then $c_1(L)F \in K^{d-1}$.

*Proof:* 

**Prop. (6.1.12.18).** If $Y \subset X$ is a closed subscheme, and $L \in \text{Pic}(X)$ satisfy $L_Y$ is an effective Cartier divisor $D$, then $c_1(L)[Y] = [D]$.

*Proof:* There is an exact sequence $0 \rightarrow O_Y(-D) \rightarrow O_Y \rightarrow O_D$, and $O_Y(-D) \cong L^{-1} \otimes O_Y$. 

---

### τ-Equivalences

**Def. (6.1.12.19)**[τ-Equivalence]. Let $X$ be a scheme over a field $k$, then two line bundles $L_1, L_2$ are called **τ-equivalent** if there are some $m \in \mathbb{Z}_+$ s.t. $L_1^{\otimes m} \sim L_2^{\otimes m}$.

**Prop. (6.1.12.20)**[Moduli Characterization]. Let $X$ be a scheme over a field $k$ and $\text{Pic}^r X\chi k$ is representable, then $L \in \text{Pic}(X)$ is τ-equivalent to $O_X$ iff its corresponding point $\lambda \in \text{Pic}^r X\chi k$ is in $\text{Pic}^\tau X\chi k$.

*Proof:* Clear from the definition of $\text{Pic}^\tau X\chi k$. 

**Def. (6.1.12.21)**[Numerically Equivalence]. Two line bundles $L_1, L_2$ on a complete prevariety over a field $K$ is called **numerically equivalent** if $c_1(L_1) \cdot \alpha = c_1(L_2) \cdot \alpha$ for any complete precurve $C \subset X$. Two divisors on $X$ is called **numerically equivalent** if their corresponding line bundle do.

Numerically trivial line bundles form a group, and are stable under proper pullbacks, by(5.11.2.7)(5.11.2.5).

**Prop. (6.1.12.22)**[Algebraic and Numerical Equivalences]. Let $L_1, L_2$ be algebraically equivalent line bundles on a proper scheme $X/k$, then $\deg_{L_1}(X) = \deg_{L_2}(X)$. In particular, algebraically equivalent divisors are numerically equivalent.

*Proof:* This is because in this case $L_1, L_2$ are in the same connected component of $\text{Pic}^\tau X\chi k$. 

**Cor. (6.1.12.23).** Let $X$ be a complete prevariety over $K$ and $L_i$ be line bundles and $Z \in Z_r(X)$, then $\deg(c_1(L_1) \cdot c_1(L_2) \cdots c_r(L_r), Z)$ only depends on algebraic equivalence classes of $L_i$.

*Proof:* Cf.[Diophantine Geometry, P562].

**Def. (6.1.12.24)**[Bounded Set of Line Bundles]. Let $X$ be a scheme over $S$, then a set $\Lambda \subset \text{Pic}(X_k)$ where $\text{Spec} k \rightarrow S$ are points are called **bounded** if there is a $T \in \text{Sch}^\text{ft} / S$ and a line bundle $M$ on $X_T$ s.t. for any $L \in \Lambda$, there is some schematic point $\text{Spec} k \rightarrow T$ s.t. $L \cong M_k$.

**Prop. (6.1.12.25)**[Numerical and τ-Equivalence]. If $X$ is proper over an alg.closed field $k$ and $L \in \text{Pic}(X)$, then the following are equivalent:

- $L$ is τ-equivalent to $O_X$.
- $L$ is numerically equivalent to $O_X$.
- The family $\{L^{\otimes p}| p \in \mathbb{Z}\}$ is bounded.
For any $F \in \text{Coh}(X)$, $\chi(F \otimes L) = \chi(F)$.

For any $p \in \mathbb{Z}$, $\mathcal{L}^p(1)$ is ample.

Proof: Cf.[Kle05]P52, 57. is this true for $k$ separably closed? □

Prop.(6.1.12.26). If $X$ is projective over an alg.closed field $k$, then the set of line bundles numerically equivalent to $\mathcal{O}_X$ is bounded.

Proof: See the proof of [Kle05]P52. □

Prop.(6.1.12.27). If $X$ is projective over an alg.closed field $k$, then there exists an $m \in \mathbb{Z}$ s.t. for any $\mathcal{L} \in \text{Pic}(X)$ numerically equivalent to $\mathcal{O}_X$, $\mathcal{L}$ is $m$-regular and $\chi(\mathcal{L}(n)) = \chi(\mathcal{O}_X(n))$ for any $n \in \mathbb{Z}$.

Proof: Cf.[Kle05]P55. □

Nef Line Bundles

Def.(6.1.12.28)[Nef Line Bundles]. A nef line bundle or numerically effective line bundle on a complete prevariety over a field $k$ is a line bundle $\mathcal{L}$ s.t. $c_1(\mathcal{L}).C \geq 0$ for any complete precurve $C \subset X$.

Nef line bundles form a semigroup, and are stable under proper pullbacks, by(5.11.2.7)(5.11.2.5).

Prop.(6.1.12.29). Ample line bundles are nef, by(5.11.2.20).

Surface Case

Def.(6.1.12.30)[(-1)-Curves]. Let $X$ be a complete curve over a field $k$, then a $(-1)$-curve on $X$ is a curve $C$ consisting of smooth points, $C \cong \mathbb{P}^1_k$ and $C \cdot C = -1$.

Prop.(6.1.12.31)[Hodge Index Theorem]. Let $X$ be a smooth surface over a field $k$ and $\mathcal{L}, \mathcal{H} \in \text{Pic}(X)$ with $\mathcal{H} \cdot \mathcal{H} > 0$ and $\mathcal{L} \cdot \mathcal{H} = 0$, then $\mathcal{L} \cdot \mathcal{L} = 0$, and the equality holds iff $\mathcal{L}$ is numerically trivial.

Proof: Cf.[Rising Sea, P552]. □

Prop.(6.1.12.32)[$\mathbb{P}^1 \times \mathbb{P}^1$]. Let $X = \mathbb{P}^1 \times \mathbb{P}^1$, $l = \mathbb{P}^1 \times \{0\}$ and $m = \{0\} \times \mathbb{P}^1$, then $l \cdot l = m \cdot m = 0$, and $l \cdot m = 1$. 

6.2 Algebraic de Rham Cohomology

1 de Rham Complexes

Def. (6.2.1.1) [Absolute de Rham Complex]. Let $B$ be a ring, let $\Omega_B = \Omega_{B/\mathbb{Z}}$, and $\Omega^i_B = \wedge^i \Omega_B$, then there is a total de Rham complex of $B$:

$$B \to \Omega^1_B \to \Omega^2_B \to \ldots$$

as $B$-modules, which is a complex, where $d(b_0 db_1 \wedge \ldots \wedge db_p) = db_0 \wedge db_1 \ldots db_p$.

Proof: $d$ is well-defined on $\Omega^1_B$ because it vanishes on the element $d(a + b) - da - db$ and $d(ab) - ad(b) - bd(a)$ by Leibniz rule, and the we get a map

$$\bigotimes_1^p \Omega_B \to \Omega^{p+1}_B : \omega_1 \otimes \ldots \otimes \omega_p \mapsto \sum (-1)^{i+1} \omega_1 \wedge \ldots \wedge d(\omega_i) \wedge \ldots \wedge \omega_p.$$ 

We want to descend this to a map on $\Omega^i_B$ using (4.1.1.20): it is clearly alternating, and it suffices to show it is $f$-linear, and this is clear by direct calculation.

Finally $d^2 = 0$. \qed

Prop. (6.2.1.2) [Quotient of de Rham Complexes]. Let $B$ be a ring and $\pi : \Omega_B \to \Omega$ be a surjective map of $B$-modules. Denote $d : B \to \Omega^1_B \to \Omega^2_B$, and $\Omega^i = \wedge^i \Omega$. Assume that the kernel of $\pi$ is generated as a $B$-module by elements $\omega$ that $\wedge^2(\pi)(d_B(\omega)) = 0$ in $\Omega^2$, then there is a de Rham complex

$$B \to \Omega^1 \to \Omega^2 \to \ldots$$

whose differential is defined by the rules similar to that of (6.2.1.1).

Proof: Because $\pi$ is surjective, so do $\wedge^i \pi$, and it suffices to show $\wedge \pi$ gives a connecting morphism between $\Omega^i_B$ and $\Omega^i$, then the well-definedness of $d$ is automatic. Cf. [[Sta]07HY]. \qed

Cor. (6.2.1.3) [Relative de Rham Complex]. If $B$ is an $A$-algebra, the surjection $\Omega_B \to \Omega_{B/A}$ satisfies the condition of (6.2.1.2) thus we can define the relative de Rham complex $\Omega^i_{B/A}$.

Proof: The verification of the condition is routine. \qed

Prop. (6.2.1.4) [Universality of de Rham Complexes]. Let $C$ be a $B$-algebra and $(E^\bullet, d)$ a non-negatively graded commutative $B$-dga and we are given a $B$-algebra map $\eta : C \to E^0$ that for every $x \in C$, the element $d(\eta(x)) \in E^1$ satisfies $d^2 = 0$, then the map $C \to E^0$ extends uniquely to a map $\Omega^\bullet_{C/B} \to E^\bullet$ of $B$-dga.

Proof: One direction is trivial as $\Omega^\bullet_{C/B}$ is strict by construction. Conversely, the composite map $C \to E^0 \to E^1$ is a $B$-derivation thus extends to a map $\eta^1 : \Omega^1_{C/B} \to E^1$, then the universal property of the exterior product (4.1.1.20) gives maps $\eta^i : \Omega^i_{C/B} \to E^i$, and this gives the desired extension. \qed

Def. (6.2.1.5) [Connection]. Let $B$ be a ring and $\Omega_B \to \Omega$ be a quotient satisfying the condition of (6.2.1.2), then a connection on $M$ is an additive map

$$\nabla : M \to M \otimes_B \Omega : \quad \nabla(b \otimes m) = b \nabla(m) + m \otimes db$$
Given a connection on $M$, we can define maps

\[ \nabla : M \otimes_B \Omega^i \to M \otimes_B \Omega^{i+1}, \quad \nabla(b \otimes \omega) = \nabla(b) \wedge \omega + m \wedge d\omega \]

This is well defined because it commutes with $B$-action. The connection is called integrable if $\nabla^2 = 0$.

**Prop.(6.2.1.6)** [Algebraic de Rham Cohomology]. Let $X \to S$ be a morphism of rings, then we define the algebraic de Rham cohomology of $X$ over $S$ as the image of the de Rham complex $\Omega^\bullet_{X/S}$ in $D(\text{Mod}(\mathcal{O}_S))$.

**Prop.(6.2.1.7).** There is a similar construction of connections on a f.g. projective $R$-module $M$ and Weil-Chern theory parallel to that of 9 and 3.

But in this case, the trace map is defined only when $M$ is f.g. projective, which is called the Hattori-Stallings trace: If $A$ is f.g. projective, the natural map $\text{Hom}_R(A, R) \otimes_R A \to \text{End}_A(P)$ is an isomorphism (Because locally it is an isomorphism??), and the inverse composed with $\text{Hom}_R(A, R) \otimes_R A \to A$, we get the desired map.

Also, when $M$ is f.g. projective, there is a Levi-Cevita connection induced by the $A \to \Omega^1_{A/R}$ because $M$ is a direct summand of some $A^n$. This is verified to be independent of $n$, or one can more algeoly use the fact that projective module is locally free.

The Chern character is important, it defines a ring map from $K_0(R)$ to $H^{ev}_{dR}(A)$. In fact, this can be lifted to a morphism $K_0(A) \to HC^{\text{perf}}_0(A) \to H^{ev}_{dR}(A)$, Cf.[阳恩林 循环同调 Dennis trace].

## 2 De Rham Cohomologies

### 3 Cup Products

**Def.(6.2.3.1)** [Hodge Cohomologies]. For a morphism $f : X \to S$, define the Hodge cohomology to be the graded $H^0(S, \mathcal{O}_S)$-algebra

\[ H^n_{\text{Hodge}}(X/S) = \bigoplus_{n \geq 0} H^n_{\text{Hodge}}(X/S) = \bigoplus_{n \geq 0} \bigoplus_{p+q=n} H^p(X, \Omega^q_{X/S}) \]

with cup product given by $\cup$. It is associative and graded commutative. And $S \mapsto H^n_{\text{Hodge}}(X/S)$ is compatible with base change.

**Proof:** Cf.[Sta]0FM5. \hfill $\square$

## 4 Poincaré Duality

**Def.(6.2.4.1)** [Situation]. Let $S$ be a qcqs scheme and $f : X \to S$ is a proper smooth morphism of schemes whose fiber are all equidimensional of dimension $d$.

**Prop.(6.2.4.2)** [Relative Poincaré duality]. In situation(6.2.4.1) there is a canonical $\mathcal{O}_S$-module map

\[ t : Rf_* \Omega^d_{X/S}[d] \to \mathcal{O}_S \]

s.t. for any $p$, the pairing

\[ Rf_* \Omega^p_{X/S} \otimes_{\mathcal{O}_S} Rf_* \Omega^{n-p}_{X/S} \to \mathcal{O}_S \]
induced from relative cup product and $t$ is a perfect pairing of perfect complexes in $D(\mathcal{O}_S)$ that is compatible perfect under base change. And it also induces a perfect $\mathcal{O}_S$-bilinear pairing

$$f_*\mathcal{O}_X \otimes R^d f_*\Omega^d_{X/S} \to \mathcal{O}_S$$

compatible with base change.

Proof: Cf.[Sta]0G8I. □

**Cor. (6.2.4.3).** If $S$ is Noetherian and $X$ is a proper smooth variety over $S$, then there is an isomorphism $R^d f_*\Omega^d_{X/S} \cong \mathcal{O}_S$ that is compatible with base change.
6.3 Étale Fundamental Groups

References are [K-M85].

1 Étale Connected Components

Def. (6.3.1.1) [Étale Connected Components]. Let $X$ be a scheme over a field $k$, let $\pi_0(X) = \text{Spec}(\pi(X))$, where $\pi(X)$ is the largest étale subalgebra of $\Gamma(X,\mathcal{O}_X)$ (4.4.7.23).

Prop. (6.3.1.2). Let $X$ be a locally algebraic scheme over a field $k$, then
- for any field extension $k'/k$, $\pi_0(X_{k'}) = \pi_0(X)_{k'}$.
- Let $Y$ be a scheme over a field $k$, then $\pi_0(X \times Y) = \pi_0(X) \times \pi_0(Y)$.

2: There is a map $\pi(X) \times_k \pi(Y) \to \pi(X \times Y)$. Because $\pi$ commutes with base change, we can base change to separable closure. In this case, it suffices to show if $X, Y$ is connected then $X \times Y$ is connected, but this follows from (5.4.3.12). \[\square\]

Prop. (6.3.1.3). Let $X$ be a locally algebraic scheme over a field $k$, then
- The mapping $\varphi : X \to \pi_0(X)$ induces a 1 to 1 correspondence of points of $\pi_0(X)$ and connected components of $X$.
- For all $x \in \pi_0(X)$, the fiber $\varphi^{-1}(x)$ is geo.connected over $k(x)$.
- $X \to \pi_0(X)$ is faithfully flat.

Proof: $\pi_0(X)$ is discrete, so the inverse image of each point is a sum of connected components of $X$. But this must be connected, because $\pi_0(X_{k(x)}) = \pi_0(X)_{k(x)} = k(x)$. Also, this implies for the alg.closure $\overline{k}$ of $k(x)$, $\pi_0(X_{\overline{k}}) = \pi_0(X_{k(x)})_{\overline{k}} = \overline{k}$, thus $X_{\overline{k}(x)}$ is geo.connected. \[\square\]

2 Étale Fundamental Groups

Main references are [Sta]Chap53 and [Fu11]Chap3.

Lemma (6.3.2.1) [Rigidity Lemma]. If $f, g : S' \to S''$ are two $S$-morphisms where $S''$ is a separated étale $S$-scheme and $(S', \overline{s})$ is a pointed scheme that $f(\overline{s}) = g(\overline{s})$, then $f = g$.

Proof: The diagonal $S'' \to S'' \otimes_S S''$ is a closed immersion and also étale hence open (5.6.6.3), so the diagonal is an clopen subset. And now $f \times g : S' \to S'' \otimes_S S''$ intersects the diagonal, and $S'$ is connected, so $f, g$ are identical on the diagonal. \[\square\]

Def. (6.3.2.2) [Galois Cover]. If $(S, \overline{s})$ is a pointed connected scheme, $S' \to S$ is a finite étale cover of degree $n$, then there are at most $n$ point over $\overline{s}$, so by (6.3.2.1), $|\text{Aut}(S'/S)| \leq n$. If the equality holds, then we call $S'/S$ a Galois cover and define $\text{Gal}(S'/S) = \text{Aut}(S'/S)^{op}$.

Prop. (6.3.2.3). If $S' \to S$ is a connected finite étale cover, then there is a finite étale cover $S'' \to S'$ that $S'' \to S$ is Galois.

Proof: Cf. [SGA1, Exp.V, §2 – §4]. \[\square\]
**Def. (6.3.2.4) [Étale Fundamental Group].** For any two finite Galois étale cover $S'/S, S''/S$, if there is a $S$-morphism $S'' \to S'$, then it induces a morphism of Galois groups because the Galois group of $S'$ acts transitively on the fiber over a closed point. And it is surjective by the same reason for $S''$.

Then we define the *étale cohomology group* 

$$\pi_1(S, x) = \lim_{\leftarrow} \text{Gal}(S'/S)$$

**Prop. (6.3.2.5) [Fundamental Group and Covers].** For $X$ connected smooth scheme and $\overline{x} \to X$ a geometric point, there is a profinite group $\pi_1(X, \overline{x})$ that there is a correspondence:

$$\{\text{finite étale covers } Y \to X\} \leftrightarrow \{\text{Finite sets with a continuous action of } \pi_1(X, x)\}$$

Such a group $\pi_1(X, \overline{x})$ is called the *étale fundamental group* of $X$ w.r.t $\overline{x}$.

**Proof:**

□

**Prop. (6.3.2.6).** Let $(S, s)$ be a connected scheme, then the functor $S' \mapsto S' \times_s S$ induces an equivalence of categories between the finite étale covers $S' \to S$ with the category of finite discrete $\pi_1(X, x)$-sets.

**Proof:** We may assume $S'$ is connected, then use (6.3.2.3) to find a Galois cover $S'' \to S'$ that $S''/S$ is Galois, then clearly there is a bijection

$$\text{Gal}(S''/S)/\text{Gal}(S''/S') \cong S'(s')$$

And any transitive discrete $\pi_1(X, x)$-sets arise this way.

To prove the essentially surjectivity and fully faithfulness, ?

□

**Cor. (6.3.2.7).** The étale fundamental group is independent of the base point $\overline{x}$ chosen.

**Proof:** This is because for two profinite groups, if the categories of their finite sets are equivalent, then they are isomorphic ?.

□

**Cor. (6.3.2.8) [Locally Constant Sheaves and Fundamental Group].** By (6.4.2.18), if $X$ is a connected scheme and $\overline{x}$ be a geometric point of $X$, then there is an equivalence of categories between finite locally constant Abelian sheaves on $X$ and finite $\pi_1(X, x)$-modules.

**Prop. (6.3.2.9).** For $k$ alg.closed, $\pi_1(\mathbb{P}^1_k) = 0$.

**Proof:**

□

**Prop. (6.3.2.10) [Arithmetic Geometric Exact Sequence].** If $X_0$ is a variety over $\mathbb{F}_q$, then there is an exact sequence

$$1 \to \pi_1(X, \overline{x}) \to \pi_1(X_0, \overline{x}) \to G(\mathbb{F}/k) \to 1.$$

### 3 Galois Inverse Problem

**$p$-adic Case**

**Prop. (6.3.3.1) [Abhyankar’s conjecture, Raynaud].** A finite group $\Gamma$ is the Galois group of an unramified Galois covering of $\mathbb{A}^1_{\mathbb{F}_p}$ iff it is generated by its $p$-Sylow subgroups.

**Proof:**

□
6.4 Étale Cohomology Theory

Basic references are [Fu11], [Sta], [Étale Cohomology, Tamme], [Mil13b] and [Notes on étale cohomology of number fields, Ann. Sci. Éc. Norm. Super. (4) 6, 521–552 (1973), Mazur].

Notations (6.4.0.1).
• Use notations defined in Cohomology of Ringed Sites 5.3.

1 Basics

Remark (6.4.1.1). For $X \in \text{Sch}$, the étale site $X_{\text{ét}}$ is a ringed site, $\text{Sh}(X_{\text{ét}})$ is a Grothendieck Abelian category, and we can define right derived functors of any left exact functor, by (5.3.1.2).

Étale Topoi

Prop. (6.4.1.2) [Zariski-Étale Comparison]. For $X \in \text{Sch}$, the inclusion $X_{\text{Zar}} \to X_{\text{ét}}$ of topologies which is a morphism of sites $\varepsilon : X_{\text{ét}} \to X_{\text{Zar}}$, for any $F \in \text{Sh}(X_{\text{ét}})$, there is a Leray spectral sequence (5.3.1.9)

$$E_2^{pq} = H^p_{\text{Zar}}(X, R^q\varepsilon_*(F)) \Rightarrow H^{p+q}_{\text{ét}}(X, F).$$

Def. (6.4.1.3) [Pushforward & Pullback]. For a morphism of schemes $X \to Y$, there is a continuous functor between sites $f_{\text{ét}} : Y_{\text{ét}} \to X_{\text{ét}}$, which preserves final objects and finite fiber products, so by (5.1.2.14), it induces a morphism of topoi (5.1.1.5)

$$f_{\text{ét}} : \text{Sh}(X_{\text{ét}}) \to \text{Sh}(Y_{\text{ét}}).$$

$f_{\text{ét}}$ is called the inverse image, it is exact. By definition (5.1.2.11), for $F \in \text{Sh}(Y_{\text{ét}})$ and $X \in X_{\text{ét}}$, $f^*F(X')$ equals the colimit over all pairs $(Y', \varphi)$ where $Y' \in Y_{\text{ét}}$ and $\varphi : X' \to Y' \times_Y X$, equivalently, all $X' \to Y'$ over $Y$.

Cor. (6.4.1.4) [Localizations]. By (5.1.2.24), an object $i : X' \to X \in X_{\text{ét}}$ induce a morphism $(\_\_\_i^* i^*)$ of topoi $X'_i \to X_i$.

Denote $i^*F = F/X'$, then for $Z' \in X'_i$, by (5.3.1.5) and (5.1.2.24)

$$F/X'(Z') = F(Z'), \quad H^q(X_{\text{ét}}; Z', F) \cong H^q(X'_i; Z', F/X').$$

In particular,

$$H^q(X_{\text{ét}}; X'_i, F) = H^q(X'_i; X', F|_{X'}).$$

thus we will omit the ambient sites and the restriction of sheaves, which should cause no confusion.

Prop. (6.4.1.5). If $Z$ is étale over $X$, then the canonical morphism

$$f^* \text{Hom}_X(-, Z) \to \text{Hom}_Y(-, Z \times_X Y)$$

is an isomorphism.

Proof: By definition, $f^* \text{Hom}_X(-, Z)$ is the sheaf associated to the presheaf $f_*\text{Hom}_X(-, Z)$ (5.1.2.11), which is identical to the presheaf $\text{Hom}_Y(-, Z)$ on $Y_{\text{ét}}$, but it is already a sheaf (5.1.4.34).
Prop. (6.4.1.6)[Relative Leray Spectral Sequence]. If \( f : X \to Y, g : Y \to Z \in \text{Sch} \), then for any \( \mathcal{F} \in \text{Sh}(X_{\text{et}}) \), there is a relative Leray spectral sequence (5.3.1.9)

\[
E_2^{pq} = R^p g_*(R^q f_*(\mathcal{F})) \Rightarrow R^{p+q}(gf)_*(\mathcal{F}).
\]

Cor. (6.4.1.7)[Leray Spectral Sequence]. For a morphism of schemes \( f : X \to Y \) and \( \mathcal{F} \in \text{Sh}(X_{\text{et}}) \), \( Y' \in Y_{\text{et}} \), there is a Leray spectral sequence?

\[
E_2^{pq} = H^p(Y', R^q f_*(\mathcal{F})) \Rightarrow H^{p+q}(Y' \times_Y X, \mathcal{F})
\]

Prop. (6.4.1.8)[Commutes with Colimits]. For \( X \in \text{Sch}^{qcqs} \), by (5.1.4.17)(5.1.4.20) and (5.3.1.15), \( H^q_{\text{et}}(X, -) \) commutes with filtered colimits.

Prop. (6.4.1.9). Let \( X, Y \in \text{Aff} \), then for any morphism of ringed sites \( (g, g^\sharp) : (X_{\text{et}}, O_X) \to (Y_{\text{et}}, O_Y) \), there exists a unique morphism of schemes \( f : X \to Y \in \text{Sch} \) s.t. \( (g, g^\sharp) \) is 2-isomorphic to \( (f, f^\sharp) \).

Proof: Cf. [Sta]04I6. \( \square \)

Field Case

Prop. (6.4.1.10)[Étale Site over Fields]. The functor \( f : X' \to X'(k_s) \) is an equivalence of topologies from the small étale site \((\text{Spec}(k))_{\text{ét}}\) to the canonical topology \( T_G \) on the category of \( G \)-sets, where \( G = G(k_s/k) \).

In particular, any Abelian sheaf on \( \text{Spec}(k)_{\text{ét}} \) is representable by \?.

Proof: First \( f \) maps a family of morphisms of schemes to a covering iff this family is a covering itself. This is because both are defined by set-theoretical surjectivity, and this is by (5.6.6.13).

Next we need to show this is an equivalence of categories. \( f \) has a left adjoint \( g \) because \( X' \to \text{Hom}_G(U, X'(k_s)) \) is representable for any \( G \)-set \( U \), because any \( G \)-set is equivalent to disjoint sums of \( G/H \), and both category has arbitrary sums, so it suffice to prove for \( G/H \), but this is represented by \( \text{Spec} k' \), where \( k' \) is the fixed field of \( H \).

To prove \( fg \cong \text{id} \) and \( gf \cong \text{id} \), they commute with direct sums, so the first one is true because \( G/H \to fg(G/H) = \text{Spec}(k_s)(k) \) is an isomorphism, and the second follows from (5.6.6.6) as all étale schemes over field \( k \) is a disjoint union of spectra of finite separable field extensions of \( k \). \( \square \)

Cor. (6.4.1.11)[Étale and Galois Cohomologies]. By (10.1.2.1),

\[
\text{Sh}((\text{Spec}(k)_{\text{ét}}) \to \text{Mod}_{G}^{\text{conts}} : \mathcal{F} \to \varinjlim_{k \subseteq k' \subseteq k^s} \mathcal{F}(\text{Spec} k')
\]

is an equivalence of categories, so

\[
H^q_{\text{ét}}(\text{Spec} k, \mathcal{F}) \cong H^q(G, \varprojlim_{k \subseteq k' \subseteq k^s} \mathcal{F}(\text{Spec} k_s)).
\]

In particular, if \( k = k^s \), then \( (\text{Spec} k)_{\text{ét}} \) is equivalent to \( \text{Ab} \), and \( H^p(\text{Spec}(k), \mathcal{F}) = 0 \) for \( p > 0 \).
Stalks

Def. (6.4.1.12) [Stalk]. By (6.4.1.10), for any scheme $X$ and a geometric point $P$, the section functor $F \to F(P)$ is an equivalence of categories from $(\text{Spec } k)_{\text{ét}}$ to $\text{Ab}$, thus for any $F \in X_{\text{ét}}$, we can define the stalk $F_P = u^*F(P)$.

Prop. (6.4.1.13). For any geometric point $P$ of $X$,
- the stalk map is exact and commutes with colimits.
- For any morphism $u : P' \to P$ of geometric points over $X$, $F_P \cong F_{P'}$.
- If $X \to Y$ is a morphism, then $(f^*F)_P \cong F_P$.

Proof: 1: taking stalk is a composition of $f^*$ and taking section over $P$ (which is an equivalence), so it is exact and commutes with colimits (6.4.1.3).
2, 3: Trivial. □

Prop. (6.4.1.14) [Stalk is Defined Naturally]. By the definition of $f^*(5.1.2.11)$, if $X'$ be an étale nbhd of $P$ in $X$, i.e. $P \to X' \to X$, then

$$(f_{\text{ét}})_P(F(P)) = \lim_{X' \to X} F(X')$$

and $F_P = f^*F(P)$, thus there is a natural map $\lim_{X' \to X} F(X') \to F_P$.

Then we have:

$$\lim_{X' \to X} G(X') \to (G^\sharp)_P$$

for any presheaf $G$ on $X_{\text{ét}}$.

Proof: Firstly $(f^\sharp)^*(G) \cong (f^*G)^\sharp$ by (5.1.2.12). Then it suffices to prove that $G(P) \to G^\sharp(P)$ is an isomorphism for any presheaf $G$ on $P_{\text{ét}}$. But this is because $P_{\text{ét}}$ is just $\text{Ab}(6.4.1.10)$, and $P \xrightarrow{id} P$ is cofinal in the category of coverings of $P$. □

Cor. (6.4.1.15). For a morphism of schemes $X \to Y$ and $P$ a geometric point of $Y$, then

$$R^p f_*(F)_P \cong \lim_{F_P \in Y'} H^p(X \times_Y Y', F).$$

Cor. (6.4.1.16). For $X = \text{Spec } k$, the equivalence (6.4.1.10) of $X_{\text{ét}}$ with continuous $G$-modules are just induced by taking the stalk at $\text{Spec } k_s$.

Prop. (6.4.1.17) [Exactness and Stalks]. The exactness, injectivity and surjectivity of maps of sheaves $F' \to F$ on $X_{\text{ét}}$ can be checked on stalks.

Proof: It suffices to prove the isomorphism case, because taking stalks are exact (6.4.1.13) and other maps can be characterized by isomorphisms.

Monomorphism: Suppose not, if $s \in F'(X')$ is mapped to 0, by taking base change, we can assume $X' = X$, and then $0 = (v(s))_?= v(s_?)$, thus $s_? = 0$ by assumption. Now by (6.4.1.14), for any $x$ there is an étale nbhd of $x$ that $s$ vanishes on it. So we find an étale covering of $X$ that $s$ vanishes, thus $s = 0$ because $F'$ is a sheaf.

Epimorphism: Similarly, for any $v \in F(X')$, we can pass to the base change and assume $X' = X$, then find for each $x$ a nbhd that comes from some $v(s_x)$, and they glue together to be a global section of $F'(X)$.

□

Prop. (6.4.1.18) [Finite Morphism is Exact]. For a finite morphism $f$, $f_*$ are exact on étale topos.

Proof: Check on stalks, □
Properties of Étale Cohomologies

Prop.(6.4.1.19) [Restriction to Small Sites]. If \( F \in \mathcal{S}h_{\text{ét}}/S \), then the cohomology groups of \( F \) on \( S \) agrees with the cohomology of its restriction on \( \mathcal{S}h(S_{\text{ét}}) \), by (5.3.1.5).

Prop.(6.4.1.20) [Čech Comparison, Arin]. If \( X \in \mathcal{S}ch \) is compact and any finite subset of \( X \) is contained in an open affine (e.g. \( X \) is quasi-projective), then for any covering \( U \in \text{Cov}(\mathcal{S}ch_{\text{ét}}/X) \) of \( X \), \( \check{H}(U, -) \) is exact.

In particular, by (5.3.2.16), in this case, we can use Čech cohomology to calculate the étale cohomologies.

Proof: Cf. [Milne, Étale Cohomologies, Prop 3.2.17]. \( \square \)

Prop.(6.4.1.21) [Inverse Limits]. Let \((X_i)_I\) be a projective system in \( \mathcal{S}ch_{\text{qc}} \) with affine morphisms, \( X_\infty = \varprojlim_{i \in I} X_i \). For any projective system of sheaves \((F_i)_I, F_i \in \mathcal{S}h((X_i)_{\text{ét}})\), let \( F_\infty = \varprojlim_{i \in I} F_i \), then there are isomorphisms

\[
\varprojlim_{i \in I} H^p_{\text{ét}}(X_i, F_i) \cong H^p_{\text{ét}}(X_\infty, F_\infty).
\]

Proof: Cf. SGA4, Prop 7.5.8, or Artin 1962, Chap 3.3. \( \square \)

Prop.(6.4.1.22) [Étale-Zariski Comparison for Qco Sheaves]. Recall by (5.1.4.36) if \( M \in \mathcal{Q}Coh(X) \) then \( \tilde{M} \) is a fpqc sheaf on \( X \), in particular an étale sheaf on \( X \). Now the edge map of the Zariski-étale comparison for \( \tilde{M} \) is an isomorphism:

\[
H^p_{\text{Zar}}(X, M) \cong H^p_{\text{ét}}(X, \tilde{M}).
\]

In particular, \( H^p_{\text{ét}}(X, G_a) \cong H^p(X, \mathcal{O}_X) \), and the étale cohomology for Qco sheaves vanishes on affine schemes.

Proof: Cf. [Sta].

We show that \( R^p \varepsilon^*(\tilde{M}) = 0 \) for \( p > 0 \), Cf. [Tamme P109]. Not hard. \( \square \)

Prop.(6.4.1.23) [Galois Covering and Group Cohomology]. If \( U = \{ Y \to X \} \) is a single Galois covering with Galois group \( G \), \( P \) is a presheaf on \( \mathcal{S}ch/X \) s.t. \( \check{H}^r(U, P) = H^r(G, P(Y)) \).

In particular, we may not use alternating complex to calculate the étale cohomologies.

Proof: \( \square \)

Prop.(6.4.1.24) [Hochschild-Serre Spectral Sequences]. Let \( X \in \mathcal{S}ch \) and \( Y \in X_{\text{ét}} \) be a Galois covering with Galois group \( \Gamma \), then for any \( F \in \mathcal{S}h(X_{\text{ét}}) \), there is a spectral sequence

Prop.(6.4.1.25) [Mayer-Vietoris Sequences]. Let \( X \in \mathcal{S}ch \) and \( f : Y \to X \in X_{\text{ét}}, U \subset X \) s.t. \( f(Y) \cup U = X \), then for any \( F \in \mathcal{S}h(X_{\text{ét}}) \), there is a long exact sequence

\[
0 \to H^0_{\text{ét}}(X, F) \to H^0_{\text{ét}}(U, F) \oplus H^0_{\text{ét}}(Y, F) \to H^0_{\text{ét}}(f^{-1}(U), F) \to H^1_{\text{ét}}(X, F) \to \ldots
\]

that is functorial in \( F \), by (5.3.1.12).
6.4. ÉTALE COHOMOLOGY THEORY 725

Def. (6.4.1.26) [Restricted Cohomologies]. Let $X \in \text{Sch}$, $Z \subset X$ be a closed subscheme, $U = X \setminus Z$, then there is a functor

$$\Gamma_Z(X, -) : \text{Sh}(X_{\text{ét}}) \to \text{Ab} : F \mapsto \ker(\Gamma(X, F) \to \Gamma(U, F)),$$

which is left exact as both $\Gamma(X, -)$ and $\Gamma(U, -)$ are.

The right derived cohomology of $H^r_Z(X, -)$, called the cohomology of $F$ with supports in $Z$.

Prop. (6.4.1.27) [Long Exact Sequences]. Situation as in (6.4.1.26), for any $F \in \text{Sh}(X_{\text{ét}})$, there is a functorial long exact sequence

$$\cdots \to H^r_Z(X, F) \to H^r_{\text{ét}}(X, F) \to H^r_{\text{ét}}(U, F) \to H^{r+1}_Z(X, F) \to \cdots.$$

Proof: Choose a functorial injective resolution (3.4.3.9), and this follows from the fact an injective sheaf is flabby (5.3.4.9).

Prop. (6.4.1.28) [Excisions]. Let $X \in \text{Sch}$, $f : X' \to X \in X_{\text{ét}}$, $Z \subset X$ be a closed subset s.t. $Z' = f^{-1}(Z) \to Z$ is an isomorphism, and $f^{-1}(X\setminus Z, F) \to X\setminus Z$ is an open immersion, then for $F \in \text{Sh}(X_{\text{ét}})$, the canonical maps

$$H^r_Z(X, F) \to H^r_{Z'}(X', F)$$

are isomorphisms.

Proof: As $f^*$ is exact and preserves injectives by (5.3.4.2), it suffices to prove for $r = 0$. Let $U = X\setminus Z, U' = X'\setminus Z'$. If $s \in \Gamma_Z(X, F)$ restricts to $0 \in \Gamma_{Z'}(X', F)$, then $s$ restricts to $0$ in both $X'$ and $U$. But $\{X', U\}$ is an étale covering of $X$, so $s = 0$.

Conversely, if $s' \in \Gamma_{Z'}(X', F)$, to show it comes from some $s \in \Gamma_Z(X, F)$, it suffices to show $s'$ and $0 \in \Gamma(U, F)$ defines a cocycle in the Čech complex $\check{C}((X', U), F)$: They both restrict to $0 \in X'\setminus U = U'$, and for $X' \times_X X'$, we can check on stalks: $s'$ restrict to $0$ on $U' \times_X U'$ from both sides, and on $Z' \times_X Z' \cong Z'$, the maps $Z' \times_X Z' \to Z$ are equal isomorphisms.

Cor. (6.4.1.29) [Restricted Cohomology at a point]. Let $x \in X$ be a closed point, then for any $F \in \text{Sh}(X_{\text{ét}})$, there is an isomorphism

$$H^r_x(X, F) \cong H^r_{\text{ét}}(\text{Spec } \mathcal{O}^h_{X, x}, j^*F).$$

Proof: Take limits over the affine étale nbhds of $x \in X$ and use (6.4.1.21).

Artin-Schreier Theory and Kummer Theory

Prop. (6.4.1.30) [Artin-Schreier Sequence]. Let $X$ be a scheme that has char $p$, let $F : (\mathbb{G}_a)_X \to (\mathbb{G}_a)_X$ be the Frobenius map, and let $P = \text{id} - F$, then there is an Artin-Schreier exact sequence

$$0 \to (\mathbb{Z}/(p))_X \to (\mathbb{G}_a)_X \xrightarrow{P} (\mathbb{G}_a)_X \to 0$$

Proof: If $s \in \mathcal{O}_{X'}$ is in the kernel, then $s = s^p$, so it is locally constant and comes from the map $\mathbb{Z}/p\mathbb{Z} \to \mathcal{O}_{X'}$. Conversely, for any $s \in \mathcal{O}_{X'}$, it suffices to find an étale cover that $s$ is a $p$-th power in $\mathcal{O}_{X'}$. For this, it suffices to notice that for any $p$-ring $A$, $A[t]/(t^p - t - s)$ is free of rank $p$ and étale over $A$. □
Cor. (6.4.1.31). If \( X \) has char \( p \), then by the long exact sequence and (6.4.1.22), there is an exact sequence
\[
0 \to H^0(X, \mathcal{O}_X)/P(H^0(X, \mathcal{O}_X)) \to H^1(X, (\mathbb{Z}/p\mathbb{Z})) \to H^1(X, \mathcal{O}_X)^F \to 0
\]
where the last one is the fixed elements.

Cor. (6.4.1.32). If \( X = \text{Spec } A \) and \( pA = 0 \), then \( H^q(X, (\mathbb{Z}/p\mathbb{Z})_X) = A/\pi A \) for \( p = 0 \) and vanish for \( p > 0 \).

Cor. (6.4.1.33). If \( k \) is separably closed field of char \( p \) and \( X \) is a reduced proper \( k \)-scheme, then \( H^1(X, (\mathbb{Z}/p\mathbb{Z})_X) = (H^1(X, \mathcal{O}_X))^F \).

Prop. (6.4.1.34) [Kummer Sequence]. If \( n \) is invertible on \( X \), then there is an exact sequence in \( \text{Sh}(X_{\acute{e}t}) \) :
\[
0 \to \mu_{n,X} \to G_{m,X} \xrightarrow{\pi} G_{m,X} \to 0
\]

Proof: The proof is similar to that of Artin-Schreier sequence (6.4.1.30), noticing that \( A \to A[T]/(T^n - s) \) is an étale map. \( \square \)

Cor. (6.4.1.35). If \( n \) is invertible on \( X \), then by (5.7.1.13), there is an exact sequence
\[
0 \to H^0(X, \mathcal{O}_X^\times)/nH^0(X, \mathcal{O}_X^\times) \to H^1(X, \mu_n) \to \text{Pic}(X)[n] \to 0
\]

Cor. (6.4.1.36). If \( X = \text{Spec } A \) where \( A \) is a local ring and \( n \) is invertible in \( A \), then \( H^1(X, \mu_n) \cong A^*/(A^*)^n \).

Proof: Cf. [Tamme, P110]. \( \square \)

Cor. (6.4.1.37). If \( k \in \text{Field}, k = k^s, X \in \text{Sch}/k \) is reduced and proper, and \( n \in \mathbb{Z} \cap k^\times \), then \( H^1(X, \mu_n) \cong \text{Pic}(X)[n] \), by (5.10.1.12).

**Strict Henselization**

Def. (6.4.1.38).

## 2 Constructible Sheaves

### Torsion Sheaves

Def. (6.4.2.1) [Torsion Sheaf]. An Abelian sheaf \( F \) on a topology is called a **torsion sheaf** if it is associated to a presheaf of torsion Abelian groups. Equivalently, the canonical morphism \( \lim_{n \to} nF \to F \) is an isomorphism.

Proof: If \( F = P^\sharp \), then consider \( 0 \to nP \to P \xrightarrow{\pi} P \to 0 \). Because \( \pi \) is exact, \( nF = (nP)^\sharp \).

Because \( \sharp \) commutes with inductive limits and \( P = \lim_{n \to} nP, F = \lim_{n \to} nF \).

Conversely, if \( F = \lim_{n \to} nF \), then \( F = \lim_{n \to} (nP)^\sharp = (\lim_{n \to} nP)^\sharp \) which is presheaf of torsion Abelian groups. \( \square \)

Remark (6.4.2.2). For a torsion sheaf, \( F(U) \) need not be torsion Abelian, but this is the case if \( U \) is quasi-compact, Cf. [Tamme P146].
Proposition (6.4.2.3) \textbf{[Being Torsion is Local].} If \(F \in \Sh(X_{\text{ét}})\) is a torsion sheaf iff all stalks \(F_x\) are torsion.

\textit{Proof: } Use the definition of torsion sheaf \(F = \lim_n F[n]\) and the fact isomorphisms are checked on stalks(6.4.1.17) and stalk maps are exact(6.4.1.13). \(\square\)

Proposition (6.4.2.4).

- If \(X \to Y\) is a morphism of schemes and \(F\) is a torsion sheaf on \(Y\), then \(f^*F\) is torsion sheaf on \(X\).
- If \(X \to Y\) is a qcqs morphism of schemes and \(F\) is a torsion sheaf on \(X\), then \(R^qf_*F\) are torsion sheaves on \(Y\).
- In particular, if \(X\) is qcqs and \(F\) is a torsion sheaf on \(X\), then \(H^q_{\text{ét}}(X,F)\) are torsion for all \(q\).

\textit{Proof: } 1: This follows immediately from(6.4.2.3) and (6.4.1.13).

2: For any \(y \in Y\), \((R^qf_*F)_y \cong H^q(X,F)\), where \(X = X \otimes_Y Y\) and \(Y\) is the strict localization of \(Y\) in \(\mathcal{Y}\). Now \(F\) is torsion sheaf by item1, and \(X \to Y\) is also qcqs with \(Y\) being affine, so \(H^q(X,F)\) is torsion by item3, so \(R^qf_*F\) is torsion by (6.4.2.3).

3: By(6.4.1.8), in this case, \(H^p_{\text{ét}}(X,-)\) commutes with filtered colimits, so we can replace \(F\) by \(nF\). Then multiplying by \(n\) is zero on \(F\), so also it is zero on \(H^p_{\text{ét}}(X,F)\), so \(H^p_{\text{ét}}(X,F)\) is torsion. \(\square\)

Proposition (6.4.2.5). If \(X\) is Noetherian scheme and \(x\) is a point of \(X\), let \(i : \Spec(k(x)) \to X\) be the structure map, then

- for any Abelian sheaf \(F\) on \(\Spec(k(x))_{\text{ét}}\), the sheaves \(R^pi_*F\) are torsion sheaf for \(p > 0\).
- \(H^p_{\text{ét}}(X,i_*F)\) are torsion for all \(p > 0\).

\textit{Proof: } 1: Cf.[Tamme P148]. Uses strict Henselization.

2: Consider the Leray spectral sequence \(H^p_{\text{ét}}(X,R^qi_*F) \Rightarrow H^{p+q}_{\text{ét}}(\Spec(k(x)),F)\), the left term vanishes for \(p \geq 0, q > 0\) by item1 and (6.4.2.4), and the right hand side vanish for \(p + q > 0\) by (6.4.2.4), then it can be checked that \(H^p_{\text{ét}}(X,i_*F)\) are torsion for \(p > 0\). \(\square\)

Proposition (6.4.2.6). For a closed subscheme \(i : Y \subset X\), \(R^pi^!\) preserves torsion sheaves.

\textit{Proof: } Cf.[Tamme P148]. \(\square\)

Proposition (6.4.2.7). For a regular Noetherian scheme \(X\), \(H^q_{\text{ét}}(X,(G_m)_X)\) are torsion for \(q \geq 2\).

\textit{Proof: } Cf.[Tamme P149]. \(\square\)

Proposition (6.4.2.8). For a torsion sheaf \(F\), define \(F(\ell) = \lim_n F[n]\), so it is an \(\ell\)-torsion sheaf, and in fact

\[\bigoplus_{\ell \in \mathbb{P}} F(\ell) = F\]

this is because this is true at the stalks, because stalks is exact and commutes with colimits(6.4.1.13).

So if \(X\) is qcqs, then \(H^p(X,F) \cong H^p(X,F(i))\), which is the primary decomposition of \(H^p(X,F)\).

\textit{Proof: } \(\square\)

Definition (6.4.2.9) \textbf{[Cohomological Dimension].} If \(X \in \Sch_{\text{qcqs}}/k\), \(\ell \in \mathbb{P}\), define the \(\ell\)-adic cohomological dimension of \(X\) as the smallest number \(\text{cd}_\ell(X) = n\) that \(H^p(X,F)_\ell = 0\) for all \(p > n\) and \(F \in \Sh^\text{for}(X_{\text{ét}})\), and define the cohomological dimension \(\text{cd}(X)\) of \(X\) as the smallest number \(n\) that \(H^p(X,F) = 0\) for all \(p > n\) and \(F \in \Sh^\text{for}(X_{\text{ét}})\). Equivalently, \(\text{cd}(X) = \sup_{\ell \in \mathbb{P}} \{\text{cd}_\ell(X)\}\).
Prop. (6.4.2.10). If $X$ is an algebraic scheme over a field $k$, then
\[ \operatorname{cd}(X) \leq \begin{cases} 2 \dim X + \operatorname{cd}(k) & \ell \neq \operatorname{char} k \\ \dim X + 1 & \ell = \operatorname{char} k \end{cases} \]

**Proof:** □

Cor. (6.4.2.11). If $k \in \text{Field}, k = k^s$, then $\operatorname{cd}(X) \leq 2 \dim X$.

**Proof:** □

Thm. (6.4.2.12) [Artin Vanishing]. If $X$ is an affine algebraic scheme over a separably closed field $k$, then $\operatorname{cd}(X) \leq \dim X$.

**Proof:** Cf. [Mil13b] P105. □

Prop. (6.4.2.13) [Arc Descent for Étale Cohomology]. Let $R$ be a ring and $G \in \text{Sh}_{\text{ét}}^\text{qcqs}(\text{Spec } R)$, and $\mathcal{F} : (\text{Sch}_{R}^{\text{qcqs}})_{\text{op}} \to D(\Lambda)_{\geq 0}$ be the functor $(f : X \to \text{Spec } R) \mapsto R\Gamma(X_{\text{ét}}, f^{*}G)$, then $\mathcal{F}$ satisfies arc-descent.

**Proof:** Cf. [Arc Topology, Bhatt, 5.4.] □

**Constructible Sheaves**

References are [Conrad notes, L3].

Prop. (6.4.2.14). $\mu_{n,X}$ is étale over $X$ iff $n$ is prime to the characteristic of all local residue fields of $X$. (Only unramifiedness is concerned, and it is fiberwise (4.4.6.6)). And we can compute the Kahler differential of $k[T]/(T^n - 1)$ vanish iff $n \neq 0$ in $k$.

In this case, $\mu_n$ is locally isomorphic to $(\mathbb{Z}/n\mathbb{Z})_{X}$, because for any affine open $U = \text{Spec } A$, $U' = \text{Spec } A[t]/(t^n - 1) \to U$ is étale and surjective (4.4.1.22) and $U'$ has all $n$-th roots of unity, so $(\mu_n)_{\text{Spec } U'} \cong (\mathbb{Z}/n\mathbb{Z})_{\text{Spec } U'}$.

Prop. (6.4.2.15). If $G$ is a commutative, finite and étale group scheme on $X$, the sheaf $G_X$ represented by $G$ is locally finite on $X_{\text{ét}}$.

Conversely, any locally constant sheaf on $X_{\text{ét}}$ is represented by a unique commutative étale group scheme over $X$, and it is finite if $F$ has finite stalks.

**Proof:** Cf. [Tamme P152]. □

Def. (6.4.2.16) [Finite étale Sheaves]. For $X \in \text{Sch}$, a finite étale sheaf is a sheaf $\mathcal{F} \in \text{Sh}(X_{\text{ét}})$ s.t. all its stalks are finite.

Def. (6.4.2.17) [Constructible Sheaves]. For $X \in \text{Sch}$, a constructible étale sheaf is a sheaf $\mathcal{F} \in \text{Sh}(X_{\text{ét}})$ s.t. there is a stratification $\{S_i\}$ of $X$ that $F/S_i$ are locally constant and finite (i.e. stalks are finite) for each $i$.

Prop. (6.4.2.18) [Properties of Constructible Sheaves].

- If $F$ is an Abelian sheaf on $X_{\text{ét}}$ that $X$ has a finite decomposition into constructible reduced subschemes $X_i$ that $F/X_i$ are locally constant, then $F$ is constructible. The converse is also true if $X$ is qcqs.
• Constructible is a local property.
• Constructibility is stable under pullback, pushout and finite direct limits.
• Constructibility is stable $j_!$ for a qc étale map.
• Subsheaves of a constructible sheaf is constructible.

Proof: Cf.[Tamme P155]. [Conrad L3 P2], [Étale Cohomology and Weil Conjecture P42].

Prop.(6.4.2.19)[lcc Sheaves and Finite Étale Schemes]. The functor $X \mapsto \text{Hom}_S(-, X)$ defines an equivalence of categories between the category of finite étale $S$-schemes to the category of locally constant finite sheaves.

Proof: The Yoneda functor is fully faithful, thus we need to show the essentially surjectivity. Notice first $\text{Hom}_S(-, X)$ is locally constant finite: we can restrict to an open subset of $S$ that the fiber are of fixed order $n$, and $X \to X \times_S X$ is étale and a closed immersion, thus $X \times_S X = X \coprod Y$, and $Y$ is finite étale over $X$ through $\pi_1$. Now by induction on the order of the fiber, $Y = X \otimes \Sigma'$ locally. So $X = S \times \Sigma$ locally, which means $X$ represents the constant sheaf $\Sigma$ locally.

To show that every locally constant finite étale sheaf is represented by a finite étale scheme, Cf.[Conrad, P19].

Prop.(6.4.2.20). If $G$ is a commutative étale group scheme over $X$, then the sheaf $G_X$ represented by $G$ is constructible iff $G$ is f.p. over $X$.

Proof:

Prop.(6.4.2.21)[Locally Constancy and Stalks]. If $\mathcal{F}$ is a constructible sheaf over a Noetherian scheme $S$, then $\mathcal{F}$ is locally constant iff all the specialization maps for geometric points $\mathcal{F}_s \to \mathcal{F}_{\eta}$ are bijective.

Proof: If $\mathcal{F}$ is locally constant, because the conclusion is local, we may assume $\mathcal{F}$ is constant, then $\mathcal{F}_s \to \mathcal{F}_{\eta}$ are all identities.

Conversely, for any geometric point $s$, $\Sigma = \mathcal{F}_s$ is finite by definition, thus there is an étale nbhd $U$ of $s$ that the map $\\Sigma \to \mathcal{F}$ induces an isomorphism on $s$-stalks, so this is an isomorphism for any geometric point linked to $s$ by specialization, in particular the generic point of the irreducible component containing $s$ and all the points in this irreducible component, thus $\mathcal{F}$ is constant on an open nbhd of $s$ (because $X$ is Noetherian thus has f.m. irreducible components), so $\mathcal{F}$ is locally constant because $X$ is Noetherian.

Prop.(6.4.2.22)[Constructible Sheaves are Noetherian]. The constructible sheaves of Abelian groups are exactly the Noetherian objects in the category of torsion sheaves.

Frobenius Actions

Cor.(6.4.2.23) [Frobenius action on Étale Sheaves]. Let $k \in \text{Field}^p$, $k \cong F_p^r$ and $X \in \text{Sch sep, ft}/k$, $\mathcal{F} \in \text{Sch}(X_\text{ét})$, we have an isomorphism $\mathcal{F} \cong (\varphi_{r,X})_*\mathcal{F}$ which is the inverse of the isomorphisms

$$(\varphi_{r,X})_*(\mathcal{F})(U) = \mathcal{F}(\varphi_{r,X}^{-1}(U)) \xrightarrow{F_{U/X}^*} \mathcal{F}(U),$$

and its adjoint $\varphi_{r,X}^*\mathcal{F} \to \mathcal{F}$ is denoted by $\varphi_\mathcal{F}$.

Then $\varphi_\mathcal{F}$ commutes with tensor product and it is an isomorphism.
The adjoint is an isomorphism because $\varphi$ induces equivalence of categories of étale site of $X_{\text{ét}}$ with itself by \((5.1.4.22)\). \hfill \square

\textbf{Prop. (6.4.2.24)} [Compatibility of $\varphi_F$ with Pullbacks]. Let $k \in \text{Field}^p, k \cong \mathbb{F}_p$, and $f : Y \to X \in \text{Sch}_{\text{sep}, \text{ft}/k}$ be separated, $\mathcal{F} \in \text{Sch}(X_{\text{ét}})$, then the morphism $\varphi_f^*f^*\mathcal{F} \cong f^*\varphi_{r,X}\mathcal{F}$ is just $\varphi_f^*\mathcal{F}$.

\textbf{Proof:} Cf. [Fu11] P586. \hfill \square

\textbf{Prop. (6.4.2.25)} [Compatibility of $\varphi$ with Higher Direct Image]. Let $k \in \text{Field}^p, k \cong \mathbb{F}_p$, and $f : X \to Y \in \text{Sch}_{\text{sep}, \text{ft}/k}$ be separated, $\mathcal{F} \in \text{Sch}(X_{\text{ét}})$, so we have a Cartesian diagram about $\varphi_{r,X}$ and $\varphi_Y$. Then the composition

$$\varphi^*_S R^if_*\mathcal{F} \to R^if_*\varphi^*_{r,X}\mathcal{F} \xrightarrow{R^if_*(\varphi_F)} R^if_*\mathcal{F}$$

is just $\varphi_{R^if_*\mathcal{F}}$.

\textbf{Proof:} Choose a compactification, the $j_i$ doesn’t matter, so we finish by \((6.4.2.25)\). \hfill \square

\textbf{Def. (6.4.2.27)} [Frobenius Action on Compact Cohomology]. Let $k \in \text{Field}^p, k \cong \mathbb{F}_p, X_0 \in \text{Sch}_{\text{sep}, \text{ft}/k}, \mathcal{F}_0 \in \text{Sh}(\mathcal{X}_{\text{ét}}), X = X_0 \times_k \bar{k}, \mathcal{F} = \mathcal{F}_0 \times_k \bar{k},$

- As $\text{Fr}_X$ is finite, by \((6.4.5.4)\) it induces a map $H^1_{\text{ét},c}(X, \mathcal{F}) \to H^1_{\text{ét},c}(X, \text{Fr}_X^*\mathcal{F})$, which by composing with the natural isomorphism $\text{Fr}_F^*\mathcal{F} \cong \mathcal{F}$ gives an endomorphism $\text{Fr}_F^* : H^1_{\text{ét},c}(X, \mathcal{F}) \to H^1_{\text{ét},c}(X, \mathcal{F})$, called the \textbf{geometric Frobenius action on the étale cohomology}.

- Similarly, there are natural isomorphisms $F^* \mathcal{F} = F^*X(X \to X_0)^*\mathcal{F}_0 \cong ((X \to X_0) \circ F_X)^*\mathcal{F}_0 = \pi^*\mathcal{F}_0$, so we can define the action of $F_X$ on $H^1_{\text{ét},c}(X, \mathcal{G})$, called the \textbf{arithmetic Frobenius action on the étale cohomology}.

- Similarly, there are natural isomorphisms $\varphi^*_{r,X}\mathcal{F} = F^*X(X \to X_0)^*\mathcal{F}_0 \cong ((X \to X_0) \circ F_X)^*\mathcal{F}_0 = \pi^*\mathcal{F}_0$, so we can define the action of $\varphi_{r,X}$ on $H^1_{\text{ét},c}(X, \mathcal{F})$, called the \textbf{absolute Frobenius action on the étale cohomology}.

\textbf{Lemma (6.4.2.28)}. Situation as in \((6.4.2.27)\), $\text{Fr}_X^*\mathcal{F} = \varphi^*_r\varphi^*_X F^*_X \mathcal{F} \cong \varphi^*_r\mathcal{F} \xrightarrow{\varphi_F^*} \mathcal{F}$ is just $\text{Fr}_F^*$, by \((5.2.10.2)\) and \((6.4.2.27)\).

\textbf{Prop. (6.4.2.29)}. Situation as in \((6.4.2.27)\), $\varphi^* = \text{id}$ on $H^1_{\text{ét},c}(X, \mathcal{F})$.

In particular, \((6.4.2.28)\) shows $\varphi^*_X = \varphi^*_X \circ \varphi^*_X : H^1_{\text{ét},c}(X, \mathcal{G})$, so $\varphi^*_X$ agrees with $\text{Fr}_X^*$ on $H^1_{\text{ét},c}(X, \mathcal{F})$, which is $\bar{k}$-linear. We can calculate with either one of them, and denote it by $F^*_X$, called the \textbf{Frobenius action on compact étale cohomologies}.

\textbf{Proof:} Choose an injective resolution $\mathcal{F} \to \mathcal{T}^\bullet$, it suffices to show that

$$\Gamma(X, \mathcal{T}^\bullet) \to \Gamma(X, \varphi_* \varphi^* \mathcal{T}^\bullet) \xrightarrow{\varphi_F^*} \Gamma(X, \varphi_* \mathcal{T}^\bullet)$$

is the identity. But notice by definition $\mathcal{T}^\bullet \to \varphi_* \varphi^* \mathcal{T}^\bullet \xrightarrow{\varphi_F^*} \varphi_* \mathcal{T}^\bullet$ is the inverse of the isomorphism in \((6.4.2.23)\). \hfill \square
3 Base Changes

Prop.(6.4.3.1)[Proper Base Change]. If there is a Cartesian diagram
\[
\begin{array}{ccc}
X' & \xrightarrow{g'} & Y' \\
\downarrow{f'} & & \downarrow{f} \\
X & \xrightarrow{g} & Y
\end{array}
\]
that \( f \) is proper, then for any torsion sheaf \( \mathcal{F} \) on \( Y' \), the base change maps (5.3.3.18)
\[ g^* R^q f_* \mathcal{F} \to R^q f'_*(g^* \mathcal{F}) \]
are isomorphisms.

Proof: Cf.[Conrad L6]. \qed

Prop.(6.4.3.2)[Smooth Base Change]. If there is a Cartesian diagram
\[
\begin{array}{ccc}
X' & \xrightarrow{g'} & Y' \\
\downarrow{f'} & & \downarrow{f} \\
X & \xrightarrow{g} & Y
\end{array}
\]
that \( f \) is smooth, then for any \( K^\bullet \in D^+(X,\mathbb{Z}/(n)) \), the base change map (5.3.3.18)
\[ f^* Rg_* K^\bullet \to Rg'_* f^* K^\bullet \]
is an isomorphism.

Proof: Cf.[Lei Fu, P391]. \qed

4 Lower shriek functor

5 Cohomology with Compact Support

Cf.[Weil1, P18].

Lemma(6.4.5.1). Extension by 0 commutes with pullback Cf.[KF Lemma4.9].

Def.(6.4.5.2)[Higher Direct Images with Compact Support]. Let \( Y \in \text{Sch}_{qcqs} \), \( f : X \to Y \in \text{Sch}^{\text{sep,ft}} / Y, \mathcal{F} \in \text{Sh}(X_{\text{et}}) \), then \( f \) factors as \( f : X \xrightarrow{j} \overline{X} \xrightarrow{\overline{f}} Y \) where \( j : X \to \overline{X} \) is an open dense subscheme and \( \overline{f} \) is proper, by Nagata compactification (5.8.3.2), then we define the higher direct image with compact support as
\[ Rf! = R\overline{f}_* j! : D^+(X, \text{tor}) \to D^+(Y, \text{tor}). \]

Then this notion is well-defined.

And if \( Y = \text{Spec} k \), define \( H^i_{\text{et}, c}(X, \mathcal{F}) = H^i(\text{Spec} k, Rf! \mathcal{F}) \), called the étale cohomology with compact support.
Proof: To show it is well-defined, notice for any two compactification, we can find a common compactification that dominates them both?, so using lemma(6.4.5.3), we easily show they are isomorphic. □

Lemma(6.4.5.3)[\(i_!\) and Higher Pushforward]. If there is a commutative diagram

\[
\begin{array}{ccc}
X & \xrightarrow{i} & X \\
\downarrow{f} & & \downarrow{\tilde{f}} \\
Y & \xrightarrow{j} & Y
\end{array}
\]

where \(i, j\) are open immersion and \(f, \tilde{f}\) are proper, then there is a natural transformation \(j_!f_* \to \tilde{f}_*i_!\) that induces a natural transformation

\[j_!Rf_* \to R\tilde{f}_*i_!,\]

which is an isomorphism iff \(\tilde{f}\) is proper.

Proof: If this is a Cartesian diagram, then the natural transformation is given by

\[j_!f_* \to \tilde{f}_*i_! \cong \tilde{f}_*i_!f^*f_* \to \tilde{f}_*i_!.
\]

The second isomorphism is by(6.4.5.1)). The rest is by proper base change Cf.[KF P88].

The general case is also easily reduced to the Cartesian case. □

Prop.(6.4.5.4)[Proper Map Induces Map on Proper Pushforward]. If \(g : Y \to X, f : X \to S\) is a proper morphism between schemes separated of f.t. over a Noetherian scheme \(S\), then for any étale Abelian sheaf \(\mathcal{F}\) on \(X\), there is a canonical map

\[g : Rf_!(\mathcal{F}) \to R(f \circ g)_!(\mathcal{F})\]

Proof: Choose a compactification \(X_2 \xrightarrow{j_2} X_2\), then choose a compactification \(X_1 \xrightarrow{i_1} X_1\) of \(i \circ g\), now


Prop.(6.4.5.5)[Properties of Compact Pushforwards].

- (Base Change) If there is a Cartesian diagram

\[
\begin{array}{ccc}
X' & \xrightarrow{h} & X \\
\downarrow{f'} & & \downarrow{f} \\
S' & \xrightarrow{g} & S
\end{array}
\]

that \(f\) is separated of f.t., then there is a natural isomorphism

\[g^*Rf_! \cong R(f \circ h)^*_!\]

- (Composition) For two separated morphisms of f.t, \(R(f_1 \circ f_2)_! = R(f_1)_!R(f_2)_!\), which induces a Leray spectral sequence.
• (Excision) Let \( f : X \to S \) be a separated morphism of f.t, and \( \mathcal{F} \in D^+(X, \text{tor}) \). Let \( Z \subset X \) be a closed subscheme and \( U = X \setminus Z \), then there is a long exact sequence
\[
\cdots \to R^p(\mathcal{F}|_U) \to R^p f_* \mathcal{F} \to R^p(f|_Z)(\mathcal{F}|_Z) \to R^{p+1}(f|_U)_!(\mathcal{F}|_U) \to \cdots
\]

**Proof:**
1: Choose a compactification of \( f \), then it suffices to show \( Rf^! \) and \( j! \) both commutes with base change, which is by proper base change (6.4.3.1) and (6.4.5.1).
2: Two compactification can be splinted, and use (6.4.5.3).
3: Use the long exact sequence applied to the exact sequence (checked on stalks (6.4.1.17))
\[
0 \to j_! j^* \mathcal{F} \to \mathcal{F} \to i_* i^* \mathcal{F} \to 0
\]

**Prop. (6.4.5.6) [Proper Pushforward to Direct Image].** There is a natural map from \( R^i f_! \to R^i f_* \), which is induced by
\[
R^i f_! = R^i j_* j! \to R^i j_* j_! \to R^i f_*
\]
where the second one is edge map of Leray spectral sequence.

In particular, there is a map \( H^i_{\text{ét}}(X, \mathcal{F}) \to H^i_{\text{ét}}(X, \mathcal{F}) \).

**Prop. (6.4.5.7) [Vanishing Result].** If \( f : X \to S \) is separated of f.t. and let \( d = \sup_{s \in S} \dim X_s \), then if \( \mathcal{F} \in D(X, \text{tor}) \) satisfies \( H^p(\mathcal{F})[p] = 0 \) for \( p \geq r \), then
\[
R^p f_* \mathcal{F} = 0, \quad p \geq r + 2d.
\]

**Proof:** Cf.[Conrad L10 P4].

**Prop. (6.4.5.8) [Projection Formula].** If \( X \to S \) is a quasi-projective morphism, \( \mathcal{F} \in D^-(S) \) and \( \mathcal{G} \in D(X) \), then we have a natural isomorphism
\[
\mathcal{F} \otimes^L_S Rf_* \mathcal{G} \cong Rf_!(f^* \mathcal{F} \otimes^L_X \mathcal{G})
\]

**Proof:** We may pass to the compactification, as \( j! \) commutes with \( f^? \).

6 Finiteness Theorems

**Prop. (6.4.6.1).** If \( S \in \text{sch} \) is Noetherian, \( f : X \to S \in \text{sch}^{\text{sep,ft}} / S \), and \( \mathcal{F} \) is a constructible sheaf on \( X \) whose torsion order is invertible in \( S \), then \( R^p f_* \mathcal{F} \) are all constructible on \( Y \).

**Proof:** Cf.[Conrad L10 P5].

**Cor. (6.4.6.2).** If \( X \) is a proper scheme over a separably closed field \( k \) and \( \mathcal{F} \) is a constructible sheaf on \( X_{\text{ét}} \), then \( H^p_{\text{ét}}(X, \mathcal{F}) \) are finite for all \( p \geq 0 \).

**Proof:**

**Lemma (6.4.6.3).** If \( X \to S \) is smooth and proper, and \( F \) is a locally constant finite Abelian sheaf with torsion order invertible on \( S \), suppose \( S \) is Noetherian, then all specialization maps for \( R^p f_* \mathcal{F} \) are isomorphisms.

**Proof:** Cf.[Conrad L10 P5].
Prop. (6.4.6.4) [Proper Smooth Higher Direct Image of LLC Sheaves]. If $X \to S$ is smooth and proper, and $F$ is a locally constant finite Abelian sheaf \((6.4.2.16)\) with torsion order invertible on $S$, then $R^p f_* F$ are locally constant finite sheaves for any $p \geq 0$.

Proof: By \((6.4.2.19)\), we may assume $F = X'$ for some finite étale scheme $X' \to X$. By Noetherian descent \(^{?}\) together with proper base change, we may reduce to the case $S$ is Noetherian. Thus by \((6.4.6.1)\), $R^p f_* F = R^p f_! F$ are constructible, and \((6.4.6.3)\) shows that the stalk maps are isomorphisms. So \((6.4.2.21)\) shows that $R^p f_* F$ are locally constant finite. \(\square\)

7 $\ell$-adic Étale Cohomologies

Artin-Rees Formalism

Def. (6.4.7.1) [Non-Torsion Cohomologies]. Fix a mixed characteristic complete DVR $(\Lambda, \mathfrak{m}, k)$, char $k = \ell$, and $K$ its quotient field. Let $A$ be a Noetherian ring that is $I$-adically complete Hausdorff, let $A_n = A/I^n$.

Notice we use notation $\ell$ instead of $p$ because often the scheme $X \in \text{Sch}$ we consider is $p$-adic and $\ell \neq p$.

Def. (6.4.7.2). The pre Artin-Rees category of $A$-modules has objects $M^\bullet = (M_n) \in \mathbb{Z}$ which are projective systems of $A$-modules with $M_n = 0$ for $n << 0$, and the morphisms in this category are the elements of the set

$$\text{Hom}_{A,R}(M^\bullet, N^\bullet) = \lim \text{Hom}(M^\bullet[d], N^\bullet)$$

An object $M^\bullet$ in the Artin-Rees category is called a null system if for some $\geq 0$ the map $M_{n+} \to M_n$ vanishes for all $n$.

Prop. (6.4.7.3) [Artin-Rees Category]. The pre Artin-Rees category is an Abelian category, and the null systems form a Weak Serre subcategory. Then we define the Artin-Rees category as the quotient category.

Proof: \(\square\)

Prop. (6.4.7.4). If the kernel and cokernel of two systems are all null systems, then they induce isomorphism on inverse limit.

Proof: Cf.[Conrad L15, P5]. \(\square\)

Def. (6.4.7.5). An object $M^\bullet$ in the A-R category is called Artin-Rees $I$-adic if it is represented by a system $M_n$ that $M_n = 0$ for $n < 0$ and $M_n$ is finite over $A_n$, $M_{n+1} \otimes_{A_{n+1}} A_n \to M_n$ is an isomorphism for $n \geq 0$.

Prop. (6.4.7.6). The full subcategory of Artin-Rees $I$-adic modules is an Abelian category, and it is equivalent to the category of finite $A$-modules by the stalk functor.

$\ell$-adic Sheaves

Def. (6.4.7.7). The Artin-Rees category of $\Lambda$-sheaves on $X_0$, strict $m$-adic sheaves are defined as before. It is called constructible $m$-adic sheaf iff it is isomorphic to a system $\{\mathcal{F}_n\}$ that $\mathcal{F}_n$ are all constructible.

It is called lisse $m$-adic if it is isomorphic to a strict $m$-adic system that $\mathcal{F}_n$ are all locally constant finite $\Lambda_n$-modules.
Prop. (6.4.7.8). Constructibility of Artin-Rees Λ-Sheaves are étale local, and stratification local.

Proof: Cf.[Conrad L15, P10].

Prop. (6.4.7.9) [Constructible and Lisse]. Let $\mathcal{F}$ be a constructible $\mathfrak{m}$-adic sheaf, then there is a stratification of $X$ that $\mathcal{F}$ is locally constant finite on each stratum.

Proof: By the stalk criterion of locally constant finite (6.4.2.21), a constructible extension of locally constant finite sheaves is also locally constant finite. So by the exact sequence $1 \to l^{n-1}\mathcal{F}_n \to \mathcal{F}_n \to \mathcal{F}_{n-1} \to 1$, iff we show there is a stratification that all $l^{n-1}\mathcal{F}_n$ are locally constant finite, then by induction all $\mathcal{F}_n$ are locally constant finite. But then $l^{n-1}\mathcal{F}_n$ is a descending chain of quotients of $\mathcal{F}_1$, thus the kernel is ascending thus stabilizes because $\mathcal{F}_1$ is constructible (6.4.2.22), so there are only f.m. such $l^{n}\mathcal{F}_n$, so there is a common stratification.

Cor. (6.4.7.10). Exactness of complexes of constructible sheaves can be checked at stalks.

Proof: Cf.[Conrad L16 P3].

Prop. (6.4.7.11). Constructible $\mathfrak{m}$-adic sheaves are Noetherian: Ascending chain of subsheaves stabilizes.

Proof: Cf.[Conrad L16 P3].

Prop. (6.4.7.12) [Direct Pushforward of $m$-adic Sheaves]. For a constructible $\mathfrak{m}$-adic sheaf $\mathcal{F}$ and a compatifiable morphism $X_0 \to S_0$, we can define $R^i f_* \mathcal{F}$ termwisely, and we have $R^i f_* \mathcal{F}$ is a constructible sheaf, hence so is $R^i f!$.

Proof: Cf.[Weil Conjecture and Étale sheaves, P128].

$\mathbb{Q}_\ell$-Sheaves

Def. (6.4.7.13)[$\mathbb{Q}_\ell$-Sheaves]. For a finite extension $E/\mathbb{Q}_\ell$, the category of $E$-sheaves are the category of constructible $\mathcal{O}_E$-sheaves with the homomorphism given by

$$\text{Hom}_E(\mathcal{F}, \mathcal{G}) = \text{Hom}_{\mathcal{O}_E}(\mathcal{F}, \mathcal{G}) \otimes_{\mathcal{O}_E} E.$$  

We may write $\mathcal{F} \otimes E$ for this object, but the tensor is fake.

The category of $\mathbb{Q}_\ell$-sheaves are the direct limit of categories of $E$-sheaves for $E/\mathbb{Q}_\ell$ finite.

The category of lisse $\mathbb{Q}_\ell$-sheaves are the direct limit of categories of lisse $E$-sheaves for $E/\mathbb{Q}_\ell$ finite.

Def. (6.4.7.14) [Tate Twist Sheaf]. The Tate weist sheaf $\mathbb{Q}_\ell(1)$ is defined to be the lisse $\mathbb{Q}_\ell$ sheaf of the limit system of locally constant finite sheaves $\mu_n$ of rank 1. It is invertible, thus we denote its dual by $\mathbb{Q}_\ell(-1)$. For any $\mathbb{Q}_\ell$-sheaf $\mathcal{F}$, denote $\mathcal{F}(1)$ to be the sheaf $\mathcal{F} \otimes \mathbb{Q}_\ell(1)$.

Prop. (6.4.7.15) [Lisse $\mathbb{Q}_\ell$-Sheaves and $\pi_1(X_0, \overline{\pi})$]. Assume $X_0$ is connected, then for a geometric point $\overline{\pi}$ of $X_0$, the functor $\mathcal{F} \to \mathcal{F}_{\overline{\pi}}$ induces an equivalence between the category of lisse $\mathbb{Q}_\ell$-sheaves to the category of continuous f.d. representations of $\pi_1(X_0, \overline{\pi})$ over $\mathbb{Q}_\ell$.

Proof: By (14.1.1.2) any representation of $\pi_1(X_0, \overline{\pi})$ is in fact an $\mathcal{O}_E$-action for some $E/\mathbb{Q}_\ell$ finite. So by the equivalence (6.3.2.5) (6.4.2.19) and taking limit using (6.4.7.6), we get the result about $\mathcal{O}_E$-sheaves and representations of $\pi_1(X_0, \overline{\pi})$ over $\mathcal{O}_E$. 

□
Cor. (6.4.7.16). We can call a lisse $\mathbb{Q}_l$-sheaf irreducible/semisimple if its corresponding representation is (6.4.7.15). It is called geometrically irreducible/semisimple if $\mathcal{F}$ is irreducible, or equivalently, its corresponding representation is irreducible as a $\pi_1(X, \overline{x})$-representation.

Def. (6.4.7.17)[$\ell$-adic étale Cohomologies]. For $X \in \text{Sch}$, $\ell \in \mathcal{P}$, define

$$H^i_{\text{ét}}(X, \mathbb{Q}_\ell) = (\varinjlim_n H^i(X, \mathbb{Z}/(\ell^n))) \otimes_{\mathbb{Z}_\ell} Q_\ell.$$ 

Comparison Theorems

Prop. (6.4.7.18) [Comparison with Betti Cohomology]. Let $X$ be a smooth complete variety over $\mathbb{C}$, let $A \in \mathbb{A}^b_{\text{fin}}$, then there exists a canonical isomorphism

$$H^q_{\text{ét}}(X, A) \cong H^q_{\text{Betti}}(X, A).$$

Proof: 

Cor. (6.4.7.19). Let $F \in \mathbb{NField}$ and $p$ a prime of $K$ with residue field $k$ of characteristic $p$. Let $X$ be a proper smooth scheme over $\mathcal{O}_{K,p}$, $X = X_k$ and $\overline{X} = X_{\overline{k}}$, then for $\ell \neq p$,

$$H^i_{\text{ét}}(\overline{X}, Q_\ell) \cong H^i_{\text{Betti}}(X_{\mathbb{C}}, Q_\ell).$$

Proof: Let $\text{Spec} \mathcal{O}_{K,p} = \{s, \eta\}$, where $s$ is the special point and $\eta$ the generic point. Let $\overline{\eta}, \overline{s}$ be arithmetic points mapping to $\eta, s$ resp. By proper base change (6.4.3.1), The stalk of higher direct image of $X \rightarrow \mathcal{O}_{K,p}$ along $\overline{s}, \overline{\eta}$ are $H^i_{\text{ét}}(\overline{X}, Q_\ell)$ and $H^i(X_{\overline{k}}, Q_\ell)$ resp., and they are the same by (6.4.6.4). And $H^i(X_{\mathbb{C}}, Q_\ell) \cong H^i_{\text{Betti}}(X, Q_\ell)$ by (6.4.7.18) and the fact $Q_\ell$ is isomorphic to $\mathbb{C}$. 

Prop. (6.4.7.20)[Étale and Fppf Comparison]. Let $X \in \text{Sch}$ and $G$ a smooth commutative group scheme over $X$, then there are natural isomorphisms

$$H^*_{\text{ét}}(X, G) \cong H^*_{\text{fppf}}(X, G).$$

Proof: Cf.[Mil80Etale Cohomologies, Prop. III.3].

$A_f$-Cohomologies

Def. (6.4.7.21)[$A_f$-Cohomologies]. For $X \in \text{Sch}$, define

$$H^p_{\text{ét}}(X, A_f) = (\varinjlim_m H^p_{\text{ét}}(X, \mathbb{Z}/(m))) \otimes A_f.$$ 

Then if $X$ is a smooth complete variety over $\mathbb{C}$, then by (6.4.7.18), there is a canonical isomorphism

$$H^p_{\text{Betti}}(X) \otimes A_f \cong H^p_{A_f}(X).$$

Thus $H^p_{\text{Betti}}(X) \otimes A_f$ is intrinsic in $X$ and $H^p_{A_f}(X)$ free over $A_f$. 

8 Curves

Prop.(6.4.8.1). If \( k \in \text{Field}, k = k^s, X \in \text{Sch}^{\text{sep, ft, dim}=1}/k, \) and \( \mathcal{F} \in \text{Sh}^{\text{tor}}(X_{\text{ét}}), \) then \( H^i_{\text{ét}}(X, \mathcal{F}) = 0 \) for \( i > 2, \) and if \( \mathcal{F} \) is constructible, then \( H^i_{\text{ét}}(X, \mathcal{F}) \) are finite.

Moreover if \( X \) is affine and \( \mathcal{F} \) is locally killed by \( n \) not divisible by \( \text{char}k \) or \( X \) is proper and sections of \( \mathcal{F} \) are locally \( p \)-torsions with \( p = \text{char}k > 0, \) then \( H^2_{\text{ét}}(X, \mathcal{F}) = 0. \)

Proof: Cf. [Conrad L4 P4] and [Tamme].

Lemma(6.4.8.2)[Smooth Complete Curves]. If \( k \in \text{Field}, k = k^s, X \) is a smooth complete curve of genus \( g \) and \( n \in \mathbb{Z} \cap k^s, \) then there are canonical identifications

\[
H^n_{\text{ét}}(X, \mu_n) = \begin{cases} 
\mu_n(k), & q = 0 \\
\text{Pic}^0(X)[n], & q = 1 \\
\mathbb{Z}/n\mathbb{Z}, & q = 2 \\
0, & q \geq 3
\end{cases}
\]

\[
\#H^n_{\text{ét}}(X, \mu_n) = \begin{cases} 
n, & q = 0 \\
n^{2g}, & q = 1 \\
n, & q = 2 \\
0, & q \geq 3
\end{cases}
\]

In particular, because \( \mathbb{Z}/(n) \cong \mu_n, \) we can get the corresponding cohomologies.

Proof: Cf. [Sta]03RQ.

Prop.(6.4.8.3)[Torsion-Freeness]. Let \( k \in \text{Field}, \) \( L \) an \( \ell \)-adic local field, \( X \) a smooth curve over \( k, \) then \( H^i_{\text{ét},c}(X, \mathcal{O}_L) \) are torsion-free.

Proof: Cf. [SGA4 1/2, Chap3.3].

Prop.(6.4.8.4)[Curve and Jacobians]. For a smooth complete curve \( C, \) its first \( \ell \)-adic étale cohomology group equals that of its Jacobian variety.

Proof:

Prop.(6.4.8.5)[Non-Complete Curves]. If \( k \in \text{Field}, k = k^s, \ell \in \mathbb{P} \setminus \text{char}k, \) then

\[
H^i_{\text{ét},c}(\mathbb{A}^1_{k^s}, \mathbb{Q}_\ell) = \begin{cases} 
\mathbb{Q}_\ell, & i = 2 \\
0, & \text{otherwise}
\end{cases}
\]

\[
H^i_{\text{ét},c}(\mathbb{A}^1_{k^s}\setminus\{0\}, \mathbb{Q}_\ell) = \begin{cases} 
\mathbb{Q}_\ell, & i = 1, 2 \\
0, & \text{otherwise}
\end{cases}
\]

Proof: These follow from(6.4.8.2) by excision and(6.4.2.12).

Weil Axioms

Prop.(6.4.8.6)[Compact \( \ell \)-adic Étale Cohomologies]. Let \( k \in \text{Field}, k = k^s, X \in \text{Sch}^{\text{sep, ft, dim}=d}/k, \) \( \Lambda \in \text{Ab}^{\text{tor}} \) with torsion orders prime to \( \text{char}k, \) then

1. \( H^i_{\text{ét},c}(X, \Lambda) \) are finite \( \Lambda \)-modules.

2. \( H^i_{\text{ét},c}(X, \Lambda) = 0 \) if \( i < 0 \) or \( i > 2d. \) And if \( X \) is affine, then \( H^i_{\text{ét},c}(X, \Lambda) = 0 \) if \( i < 0 \) or \( i > d. \)

3. There is a natural isomorphism \( H^{2d}_{\text{ét},c}(X, \Lambda) \cong \Lambda[S], \) where \( S \) is the set of irreducible components of \( X \) of dimension \( d. \)

4. there is a long exact sequence

\[
\cdots \to H^p_{\text{ét},c}(U, \Lambda) \to H^p_{\text{ét},c}(X, \Lambda) \to H^p_{\text{ét},c}(Z, \Lambda) \to H^{p+1}_{\text{ét},c}(U, \Lambda) \to \cdots
\]
5. \( H^i_{\text{ét},c}(A_k^d, \underline{\Lambda}) = \begin{cases} 
\Lambda & i = 2d \\
0 & \text{otherwise}. \end{cases} \)

6. If \( G \) is a connected algebraic scheme over \( k \) acting regularly on \( X \), then \( G(k) \) acts trivially on \( H^i_{\text{ét},c}(X, \underline{\Lambda}) \).

\textit{Proof:} 1 follows from (6.4.6.1). 4 follows from excision (6.4.5.5).
2 follows from (6.4.2.11) and (6.4.2.12).
3: By item 2 and item 4, it suffices to show for \( X \) irreducible.
5: This follows from Künneth formula (6.4.8.9) and (6.4.8.5).
\( \square \)

\textbf{Def. (6.4.8.7)} [Cycle Maps]. Let

\textbf{Cor. (6.4.8.8)} [Homotopy Axiom]. Two maps \( \varphi, \varphi' : X \to Y \in \text{Sch} \) induce the same map on the \( \ell \)-adic cohomology if their graphs are rationally equivalent.

\textit{Proof:} This is because the maps on cohomology depends only on the rational equivalence classes of the graph.
\( \square \)

\textbf{Prop. (6.4.8.9)} [Künneth Formula]. Let \( X, Y \) be complete prevarieties over \( k \), then there exists a natural isomorphism

\[ H^*(X, \mathbb{Q}_\ell) \otimes H^*(Y, \mathbb{Q}_\ell) \cong H^*(X \times Y, \mathbb{Q}_\ell). \]

\textit{Proof:} □

\textbf{Prop. (6.4.8.10)} [Poincaré Duality]. If \( X \) is smooth variety of dimension \( d \) over \( k \), \( \mathcal{F} \) is lisse on \( X \), then there is a natural isomorphism \( H^{2d}_{\text{ét},c}(X, \mathbb{Q}_\ell(d)) \xrightarrow{\text{tr}_X} \mathbb{Q}_\ell \) and a perfect pairing

\[ H^n_{\text{ét},c}(X, \mathcal{F}) \times H^{2d-n}_{\text{ét},c}(X, \mathcal{F}^\vee(d)) \to H^{2d}_{\text{ét},c}(X, \mathbb{Q}_\ell(d)) \xrightarrow{\text{tr}_X} \mathbb{Q}_\ell \]

compatible with Galois action.

\textit{Proof:} Cf. [Conrad L12-13], [Weil 2Bhatt P5].
\( \square \)

\textbf{Trace Formulas}

\textbf{Def. (6.4.8.11)} [Lefschetz Numbers]. Let \( k \in \text{Field}, k = k^s, X \in \text{Sch}^{\text{sep}, \text{ft}} / k, \mathcal{F} \) a constructible \( \mathbb{Q}_\ell \)-sheaf on \( X \), then for any \( g \in \text{Aut}(X) \), define the \textbf{alternating cohomology group}

\[ H_{\text{ét},c}(X, \mathcal{F}) = \sum_{i \geq 0} (-1)^i H^i_{\text{ét},c}(X, \mathcal{F}). \]

and the \textbf{Lefschetz number} to be

\[ \text{tr}(g, X, \mathcal{F}) = \text{tr}(g|H_{\text{ét},c}(X, \mathcal{F})) = \sum_{i \geq 0} (-1)^i \text{tr}(g|H^i_{\text{ét},c}(X, \mathcal{F})). \]

\textbf{Prop. (6.4.8.12)}. Let \( k \in \text{Field}, k = k^s, X, C' \in \text{Sch}^{\text{sep}, \text{ft}} / k, g, h \in \text{Aut}(X), g' \in \text{Aut}(X') \), then

1. \( \text{tr}(g, X, \cdot) \) is additive.
2. If $Z \subset X$ is a closed subscheme and $U = X \setminus Z$, then $\text{tr}(g, X, \mathcal{F}) = \text{tr}(g, U, \mathcal{F}) + \text{tr}(g, Z, \mathcal{F})$.

3. $\text{tr}(g \times g, X \times X', \mathcal{F} \times \mathcal{F}') = \text{tr}(g, X, \mathcal{F}) \text{tr}(g', X', \mathcal{F}')$.

4. If $g, h$ commute, then $\text{tr}(gh, X, \mathcal{F}) = \text{tr}(g, X^h, \mathcal{F})$.

5. If $T$ is a tori acting on $X$, then $\text{tr}(g, X, \mathcal{F}) = \text{tr}(g, X^S, \mathcal{F})$.

Proof: 1, 2, 3 follow from (6.4.8.6).

4, 5: [Deligne-Lustig, Thm3.2] and [Digne and Michel, Prop10.15].
6.5 Pro-Étale Cohomology

Main references are [B-S14] and [Sta]Chap56.

1 Introduction

In his second paper on the Weil conjectures ([Del80]), Deligne introduced a derived category of \(l\)-adic sheaves as a certain 2-limit of categories of complexes of sheaves of \(\mathbb{Z}/l^n\mathbb{Z}\)-modules on the étale-site of a scheme \(X\). This approach is used in the paper by Beilinson, Bernstein, and Deligne ([BBD82]) as the basis for their beautiful theory of perverse sheaves. In a paper entitled “Continuous Étale Cohomology” ([Jan88]) Uwe Jannsen discusses an important variant of the cohomology of a \(l\)-adic sheaf on a variety over a field. His paper is followed up by a paper of Torsten Ekedahl ([Eke90]) who discusses the adic formalism needed to work comfortably with derived categories defined as limits.

2 Ring-Theoretical Stuff

**Def. (6.5.2.1) [étale Local Isomorphism].** A ring map \(A \to B\) is called a local isomorphism if for every prime \(\mathfrak{p} \in \text{Spec} B\), there is a nbhd \(\text{Spec} B_g\) that \(\text{Spec} B_g \to \text{Spec} A\) is an open immersion.

**Prop. (6.5.2.2).** The class of local isomorphisms is stable under base change and compositions. (This follows from (5.4.4.60)).

Moreover, if \(A \to B \to C\) are ring maps that \(A \to B, A \to C\) are both local isomorphisms, then \(B \to C\) is also a local isomorphism.

**Def. (6.5.2.3) [w-Local Rings].** A ring \(A\) is called w-local if \(\text{Spec} A\) is w-local (3.8.4.17). It is called strictly w-local if it is w-local and every f.f. étale map \(A \to B\) has a section. A map of rings is called w-local if it induces a w-local map (3.8.4.17) on the Spec.

**Prop. (6.5.2.4).** A w-local ring \(A\) is strictly w-local iff all local rings of \(A\) at closed pts are strictly Henselian.

**Proof:** Cf.[Pro-Etale Cohomology, Scholze, P10].

**Ind-Zariski Algebra**

**Def. (6.5.2.5) [Ind-Zariski Algebra].** A ring map \(A \to B\) is called ind-Zariski/smooth/étale if \(B\) is a filtered colimit of local isomorphisms/smooth ring maps/étale ring maps \(A \to B_i\).

**Prop. (6.5.2.6) [Properties of Ind-Zariski Algebras].** Ind-Zariski ring maps are stable under base change and composition, by (6.5.2.2).?

If \(A \to B \to C\) are ring maps that \(A \to B, A \to C\) are both ind-Zariski, then \(B \to C\) is also ind-Zariski.

\(A \to B\) be ind-Zariski, then it identifies local rings.

**Proof:**

**Def. (6.5.2.7) [Ind-(Zariski Localization)].** A ring map \(A \to B\) is called a Zariski localization if \(B = \prod_i A_{f_i}\). An ind-(Zariski localization) of \(A\) is a colimit of Zariski localizations of \(A\).
6.5. PRO-ÉTALE COHOMOLOGY

Ind-Smooth Algebra

Ind-Étale Algebra
6.6 Crystalline Cohomology

Main references are [Sta].

1 PD-Schemes

Def. (6.6.1.1) [PD-Schemes]. A pd-scheme is a triple \((S, \mathcal{I}, \gamma)\) where \(S\) is a scheme, \(\mathcal{I}\) is a Qco sheaf of ideals, and \(\gamma\) is a pd-structure on \(\mathcal{I}(4.7.0.1)\). A morphism of pd-schemes is a morphism that all the structure morphisms are morphisms of pd-structures.

Def. (6.6.1.2) [PD-Thickening]. A pd-thickening is a \((U, T, \delta)\) where \(T\) is a thickening of \(U(5.8.9.1)\) with sheaf of ideals \(\mathcal{I}(U = \text{Spec}(\mathcal{I}))\) that \((T, \mathcal{I}, \delta)\) is a pd-structure.

Prop. (6.6.1.3). The fibered product of two morphisms in the category of pd-schemes exists if one of them is a pd-thickening.

Proof: Cf. [Sta]07ME. □

2 Crystalline Site

Def. (6.6.2.1) [Coverings]. A family of morphisms \(\{(U_i, T_i, \delta_i) \rightarrow (U, T, \delta)\}\) of pd-thickenings is called a Zariski/smooth/étale/syntomic/fppf \(\cdots\) if

- \(U_i = U \otimes_T T_i\),
- \(\{T_i \rightarrow T\}\) is a Zariski/smooth/étale/syntomic/fppf \(\cdots\) covering of \(T\).

Def. (6.6.2.2) [Big Crystalline Site]. Let \(p\) be a prime and \((S, \mathcal{I}, \gamma)\) be a pd-scheme over \(\mathbb{Z}(p)\), let \(S_0 = V(\mathcal{I}) \subset S\), and \(X \rightarrow S_0\) a morphism of schemes that \(p\) is nilpotent on \(X\), then the big-crystalline site \((X/S)_{\text{crys}}\) consists of pd-thickenings \((6.6.1.2)\) \((U, T, \delta)\) over \((S, \mathcal{I}, \delta)\) and a morphism of schemes \(U \rightarrow X\), and the topology is the Zariski topology. In fact for any \((U, T, \delta) \in (X/S)_{\text{crys}}, p\) is locally nilpotent in \(T\), by (4.7.0.5).

The crystalline site \((X/S)_{\text{crys}}\) is the strictly full subcategory consisting of objects that \(U \rightarrow X\) is an open immersion.

Notice the structure sheaf that maps \((U, T, \delta)\) to \(\Gamma(\mathcal{O}_U, U)\) is a sheaf of rings on \((X/S)_{\text{crys}}, \text{ called the structure sheaf } \mathcal{O}_{X/S}.\)

Prop. (6.6.2.3) [Comparing with Zariski Site]. The functor

\[ u_{X/S} : (X/S)_{\text{crys}} \rightarrow X_{\text{Zar}} : (U, T, \delta) \rightarrow U \]

is cocontinuous (easy to verify), thus defines a morphism of topoi \(\text{Sh}((X/S)_{\text{crys}}) \rightarrow \text{Sh}(X_{\text{Zar}})\) by (5.1.2.20), which is functorial in \(X\) and \(S\).

Prop. (6.6.2.4) [Finite Limits]. The category \((S/X)_{\text{crys}}\) has all finite limits, and the forgetful functor \((U, T, \delta) \rightarrow U\) preserves finite limits.


Def. (6.6.2.5) [Affine Crystalline Site]. Let \((A, I, \gamma)\) be a pd-structure that \(A\) is a \(\mathbb{Z}(p)\)-algebra, and \(C\) is an \(A/I\)-algebra that \(p\) is nilpotent in \(C\), then the crystalline site \((6.6.2.2)\) \((C/A)_{\text{Cris}}\) is the site whose objects are pd-structures \((B, J, \delta)\) over \((A, I, \gamma)\) that \(p\) is nilpotent in \(B(4.7.0.5)\), together with a map of rings \(C \rightarrow B/J\) over \(A/I\), and \((C/A)_{\text{crys}}\) the full subcategory of objects \(B\) that \(C \rightarrow B/J\) is an isomorphism.

Notice for any object \((B, J, \delta)\) in \((C/A)_{\text{Cris}}, J\) is nilpotent, by (4.7.0.5).
Sheaf of Differentials

Def. (6.6.2.6) [S-Derivations]. Let $\mathcal{F}$ be a sheaf of $\mathcal{O}_{X/S}$-modules on $(X/S)_{\text{crys}}$, then an $S$-derivation $D : \mathcal{O}_{X/S} \to \mathcal{F}$ is a map of sheaves that for any object $(U, T, \delta)$ of $(X/S)_{\text{crys}}$, the map $D : \Gamma(T, \mathcal{O}_T) \to \Gamma(T, \mathcal{F})$ is a pd-derivation over $\Gamma(V, \mathcal{O}_V)$ for any open subset $V \subset S$ that $T \to S$ factors through $V$.

Prop. (6.6.2.7) [Sheaf of PD-Differentials]. Similar to the construction of sheaf of differentials (5.2.4.2), we can construct of sheaf of pd-differentials $\Omega_{X/S, \delta}$ on $(X/S)_{\text{crys}}$, which is a quotient of the sheaf of differentials $\Omega_{X/S}$. And similar to (5.2.4.3), for any $(U, T, \delta) \in (X/S)_{\text{crys}}$, $\Omega_{X/S, \delta}|_{(T/S)_{\text{crys}}} = \Omega_{T/S, \delta}$.

Prop. (6.6.2.8) [A First Order PD-Thickening]. Let $(U, T, \delta) \in (X/S)_{\text{crys}}$, $\mathcal{J}$ the ideal sheaf of $U$, we define a first order thickening $T'$ of $T$: let $\mathcal{O}_{T'} = \mathcal{O}_T \oplus \Omega_{T/S, \delta}$ with the algebraic structure that $\Omega^2_{T/S, \delta} = 0$, and let $\mathcal{J}' = \mathcal{J} \otimes \Omega_{T/S, \delta}$, and define the pd-structure as $\delta'(f, \omega) = (\delta_n(f), \delta_{n-1}(f)\omega)$.

Then $(U, T, \delta')$ is a pd-thickening and $(U, T, \delta) \to (U, T', \delta')$ is a morphism in $(X/S)_{\text{crys}}$. Moreover, there are two ring maps $p_0, p_1 : \mathcal{O}_T \to \mathcal{O}_{T'} : p_0(f) = (f, 0), \; p_1(f) = (f, d_{T/S, \delta}(f))$

Then we get two contraction of the morphism $T \to T'$, and $p_0^* - p_1^*$ is the universal derivation $d_{T/S, \delta}$ included in $\mathcal{O}_{T'}$.

This construction is functorial in $T/S$ by (6.6.2.7) and hence gives a functor of sites $(X/S)_{\text{crys}} \to (X/S)_{\text{crys}}$.

Proof: The verification of the pd-axioms in in [Sta07HH].

Prop. (6.6.2.9) [Second Order PD-Thickening]. There is a further thickening $T''$ of $T'$, which is a second order thickening of $T$:

$$\Omega_{T''} = \mathcal{O}_T \oplus \Omega_{T/S, \delta} \oplus \Omega_{T/S, \delta} \oplus \Omega^2_{T/S, \delta}$$

with the algebra structure given by

$$(f, \omega_1, \omega_2, \eta)(f', \omega'_1, \omega'_2, \eta') = (ff', f\omega'_1 + f'\omega_1, f\omega'_2 + f'\omega_2, f\eta' + f'\eta + \omega_1 \wedge \omega'_2 + \omega'_1 \wedge \omega_2)$$

Let $\mathcal{J}'' = \mathcal{J} \oplus \Omega_{T/S, \delta} \oplus \Omega_{T/S, \delta} \oplus \Omega^2_{T/S, \delta}$, then there is a PD-structure on $\mathcal{J}''$ given by

$$\delta''_n(f, \omega_1, \omega_2, \eta)) = (\delta_n(f), \delta_{n-1}(f)\omega_1, \delta_{n-1}(f)\omega_2, \delta_{n-1}(f)\eta + \delta_{n-1}(f)\omega_1 \wedge \omega_2)$$

This construction is functorial in $T/S$ by (6.6.2.7) and hence gives a functor of sites $(X/S)_{\text{crys}} \to (X/S)_{\text{crys}}$.

Proof: For the details, Cf.[Sta07J3].
3 Crystals

Def. (6.6.3.1) [Crystals]. In situation (6.6.2.2), if $\mathcal{F}$ is a sheaf of $\mathcal{O}_{X/S}$-modules on $(X/S)_{\text{crys}}$, then it restricts to a sheaf $f_T$ on $T$ for every object $(U, T, \delta) \in (X/S)_{\text{crys}}$. And it is functorial. Then $\mathcal{F}$ is called

- a crystal in $\mathcal{O}_{X/S}$-modules if for any morphism $u : (U', T', \delta') \to (U, T, \delta)$ in $(X/S)_{\text{crys}}$, the morphism of $\mathcal{O}_T$-modules $u^* \mathcal{F}_T \to \mathcal{F}_{T'}$ is an isomorphism.
- locally Qco if $\mathcal{F}_T$ is a Qco $\mathcal{O}_T$-module for any $(U, T, \delta) \in (X/S)_{\text{crys}}$.
- Qco as defined in (5.2.2.25).

In particular, $\mathcal{O}_{X/S}$ is a crystal in $\mathcal{O}_{X/S}$-modules.

Connections

Def. (6.6.3.2) [de Rham Complex for $(X/S)_{\text{crys}}$]. On a crystalline site $(X/S)_{\text{crys}}$, if we define $\Omega^i_{X/S, \delta} = \wedge^i \Omega_{X/S, \delta}$ (6.6.2.7), then by (6.2.1.2), the universal $S$-derivative $d_X/S$ gives rise to the de Rham complex

$$\mathcal{O}_{X/S} \to \Omega^1_{X/S, \delta} \to \Omega^2_{X/S, \delta} \to \cdots$$

as $\mathcal{O}_{X/S}$-modules on $(X/S)_{\text{crys}}$.

Proof: The verification of the condition for the quotient $\Omega_X \to \Omega_{X/S, \delta}$ is routine.

Def. (6.6.3.3) [Connections on $(X/S)_{\text{crys}}$]. We define the notion of connection on $(X/S)_{\text{crys}}$ of an $\mathcal{O}_{X/S}$-module $\mathcal{F}$ on $(X/S)_{\text{crys}}$ w.r.t. the differential $\Omega_{X/S, \delta}$, as in (6.2.1.5).

Prop. (6.6.3.4) [Connection of a Crystal]. Any crystal in $\mathcal{O}_{X/S}$-modules $\mathcal{F}$ are equipped with a canonical integrable connection.

Proof: For any $(U, T, \delta) \in (X/S)_{\text{crys}}$, consider the first order thickening $(U', T', \delta')$ given in (6.6.2.8), then there are two projections $p_0, p_1 : T' \to T$ and an inclusion $i : T \to T'$, then by the property of crystals we get isomorphisms

$$p_0^* \mathcal{F}_T \overset{c_0}{\to} \mathcal{F}_{T'} \overset{c_1}{\leftarrow} p_1^* \mathcal{F}_T$$

then $\nabla(s) = p_1(s) - c_1^{-1} c_0(p_0(s))$ vanishes after pulling back to $T$ via $i^*$, so it is in the kernel of $i^*$, which is

$$\mathcal{F}_T \otimes_{\mathcal{O}_T} \Omega_{T/S}$$

by the construction of $T'(6.6.2.8)$. This $\nabla$ is functorial in $T$ as everything is functorial, hence gives a connection on $\mathcal{F}$.

For the integrability, Cf.[[Sta]07J6].

Cor. (6.6.3.5). If $\mathcal{F}$ is a crystal in in Qco modules, then we can define a de Rham complex

$$\mathcal{F} \to \mathcal{F} \otimes_{\mathcal{O}_{X/S}} \Omega_{X/S, \delta} \to \mathcal{F} \otimes_{\mathcal{O}_{X/S, \delta}} \Omega^2_{X/S, \delta} \to \cdots$$

Crystals in Qco modules

Def. (6.6.3.6) [Crystals in Qco Modules]. An $\mathcal{O}_X$-module $\mathcal{F}$ on $(X/S)_{\text{crys}}$ is called a crystal in quasi-coherent modules if it satisfies the following equivalent conditions:

- $\mathcal{F}$ is Qco.
• \( \mathcal{F} \) is locally \( \text{Qco}(6.6.3.1) \) and it is a crystal in \( \mathcal{O}_{X/S} \)-modules.

Moreover, \( \mathcal{F} \) is called a **crystal in finite locally free modules** if \( \mathcal{F} \) is finite locally free.

**Proof:** Cf. [Sta]07IT.

---

**Def. (6.6.3.7) [Notations in Polynomial case].** If in situation (6.6.2.5), \( S = \text{Spec} \, A, X = \text{Spec} \, C \), we let \( P \to C \) be a surjection of \( A \)-algebras with \( P = A[X_i] \), and the kernel is \( J \). Set \( D = D_{P,\gamma}(J)^{\wedge} \) be the \( p \)-adically completed pd-envelope, then \( (D, \hat{\mathcal{J}}, \hat{\gamma}) \) admits a natural pd-structure, by (4.7.0.12).

Let \( D_e = D/p^e \) and \( J_e \) the image of \( \hat{\mathcal{J}} \) in \( D_e \). Denote

\[
\Omega_D = (\Omega_{D/A,\gamma})^{\wedge} = (\Omega_{D_{P,\gamma}(J)/A,\gamma})^{\wedge} = \lim_e \Omega_{D(n)_e/A,\gamma}(4.7.1.4).
\]

By (4.7.1.4), \( \Omega_{D_{P,\gamma}(J)/A,\gamma} = \Omega_{P/A} \otimes P \Omega_{D_{P,\gamma}(J)} \) which is free over \( D_{P,\gamma}(J) \) on \( dx_i \), so \( \Omega_D \) is topologically free over \( D \) on \( dx_i \), and there is a universal derivation \( d : D \to \Omega_D \).

Now let \( J(n) = \ker(P \otimes_A \otimes A \to C) \) where the tensor has \( n + 1 \) factors, and

\[
D(n) = (D_{P \otimes_A \otimes A \otimes A P/A,\gamma}(J(n)))^{\wedge}
\]

with divided ideals \( \hat{\mathcal{J}}(n) \), and also \( D(n)_e = D(n)/p^e, T(n)_e = \text{Spec} \, D(n)_e \), then \( (X, T(n)_e, \gamma(n)) \) is a pd-thickening by (4.7.0.5) for \( e \) large (4.7.0.12), by (4.7.0.5) as \( p \) is nilpotent in \( X \). And

\[
\Omega_{D(n)} = (\Omega_{D(n)_e/A,\gamma(n)})^{\wedge}.
\]

Then \( D(0) = D, D(1), \ldots \) form a cosimplicial pd-structures.

Let \( \mathcal{F} \) be a sheaf of \( \mathcal{O}_{X/S} \)-modules, denote

\[
M(n) = \lim_e \Gamma((X, T(n)_e, \gamma(n)), \mathcal{F})).
\]

**Prop. (6.6.3.8).** Notation as in (6.6.3.7), there is an isomorphism

\[
D(n) \cong (D(\xi_i(j)))^{\wedge}
\]

where \( \xi_i(j) = X_i \otimes 1 \otimes \ldots 1 - 1 \otimes 1 \ldots X_i \otimes 1 \otimes \ldots 1 \).

**Proof:** There is an isomorphism \( P \otimes_A \otimes A \to P \otimes_A \otimes A P + (\xi_i(j)) \), and \( J(n) \) is just generated by \( JP \otimes_A \otimes A P + (\xi_i(j)) \), so this theorem follows from (4.7.0.17).

---

**Crystals and Connections**

**Lemma (6.6.3.9) [Crystals and Connections].** Notation as in (6.6.3.7), there is a functor from the category of crystals in \( \text{Qco} \, \mathcal{O}_{X/S} \)-modules to the category of pairs \( (M, \nabla) \) that

- \( M \) is a \( p \)-adically complete \( D \)-module.
- \( \nabla : M \to M \otimes_D \Omega_D \) is an integrable connection.
- \( \nabla \) is topological quasi-nilpotent: for any \( m \in M \), there are only f.m. pairs \( (i, k) \) that \( \nabla_{\partial_i/\partial x_i}^k(m) \in pM \).
Prop. (6.6.3.10). The functor defined in (6.6.3.9) is an equivalence of categories.

Proof: Cf. [[Sta]07JG].

Def. (6.6.3.11) [Notations in Smooth Case]. Situation as in (6.6.3.7), but this time we choose a smooth $A$-algebra $P'$ and $A \to P' \to C$ with $\ker(P' \to C) = J'$ and do the same as (6.6.3.7) again, to get

$$D' = D_{P',\gamma}(J')$$

and

$$\Omega_{D'} = (\Omega_{D'/A,\gamma})^\wedge = (\Omega_{D'/A,J}/A,\gamma)^\wedge = \lim_e \Omega_{D'/(n)_e/A,\gamma}$$

Prop. (6.6.3.12) [Crystals and Connections in Smooth case]. Situation as in (6.6.3.7) and (6.6.3.9), then we can find a $P = A[X_i]$ that there are maps $a : D \to D', b : D' \to D$ between the completed pd-envelope of $P, P'$ that $a \circ b = \text{id}$ and compatible with the maps $D \to C$ and $D' \to C$, such that the base change along $a, b$ induces an equivalence of categories between the categories of modules with an integrable connection over $D$ as in (6.6.3.9) and the category of modules over $D'$ with an integrable connection.

Proof: We can find $P$ that $P \to C$ factors through a surjection $P \to P'$, hence we get a surjection $a : D \to D'$ the left adjointness of pd-envelope. Let $e$ large that $D'_e$ is a pd-thickening of $C$ over $A$ by (4.7.0.12)(4.7.0.5), then the kernel of $D_e \to D'_e$ is nilpotent by (4.7.0.5), hence by the strongly lifting property (4.4.5.16) of the smooth ring map $P \to P'(4.4.5.21)$ w.r.t. the thickening $D_e \to D'_e$, we find a lift $P' \to D_e$.

Notice $D_{e+i+1} \to D_{e+i} \times_{D'_e} D'_{e+i+1}$ is surjective with nilpotent kernels (because $p^{e+i}D \to p^{e+i}D'$ is surjective), we can use the smooth of $A \to P$ to lift inductively the map $P' \to D_e$ to a map $P' \to D$, thus by universal property of completed pd-envelope extends to a map $b : D' \to D$. It is clear that $a \circ b = \text{id}$.

For the equivalence of categories, Cf. [[Sta]07L5].

Remark (6.6.3.13). In fact this proposition holds with $P'$ being any ring that $A \to P'$ satisfies the strong lifting property (4.4.5.16). In particular, this holds for ind-smooth $A$-algebras (6.5.2.5).

4 Compuations

Prop. (6.6.4.1) [Affine Thickening is Acyclic]. If $T$ is a locally Qco sheaf of $O_X$-modules on $(X/S)$, then $H^p((U, T, \delta), F) = 0$ for any $p > 0$ and $U$ or $T$ affine.
**Proposition (6.6.4.4).** Situation as in (6.6.3.7), if $\mathcal{F}$ is locally $\mathcal{Q}_{co}$ and satisfies: for any morphism $f : (U,T,\delta) \to (U',T',\delta') \in (X/S)_{cr}_{ys}$ that $f : T \to T'$ is a closed immersion the map $f^*\mathcal{F}_{T'} \to \mathcal{F}_T$ is surjective, then the complex

$$M(0) \to M(1) \to \ldots$$

computes $R\Gamma((X/S)_{cr}_{ys}, \mathcal{F})$. Moreover,

$$R\Gamma((X/S)_{cr}_{ys}, \mathcal{F} \otimes_{\mathcal{O}_{X/S}} \Omega^1_{X/S,\delta}) = 0$$

for $i > 0$.

**Proof:** We use (5.3.1.19) for the presheaf $K' = \text{colim}_e h_{(X,T,e,\delta)}$, which satisfies the condition by (6.6.4.2). Then we get a spectral sequence

$$E_1^{p,q} = H^q(K_p', \mathcal{F}) \Rightarrow H^{p+q}(K, \mathcal{F})$$

Notice $K'_n = (\text{colim}_e h_{(X,T(n)e,\delta)})^\sharp$ by (6.6.4.3), so the cohomology

$$R\Gamma(K'_n, \mathcal{F}) = R\lim_e (\Gamma((X,T(n)e,\gamma(n)), \mathcal{F}))$$

Now the surjectivity $f^*\mathcal{F}_{T'} \to \mathcal{F}_T$ is equivalent to the surjectivity $\mathcal{F}_{T'} \to f_*\mathcal{F}_T$, so there is an exact sequence of $\mathcal{Q}_{co}$ $\mathcal{T}'$-sheaves

$$0 \to \mathcal{K} \to \mathcal{F}_{T'} \to f_*\mathcal{F}_T \to 0$$

which implies that $\mathcal{F}((U',T',\delta')) \to \mathcal{F}((U,T,\delta))$ is surjective, by (5.7.4.2) and (5.7.1.3).

Then by (4.6.3.3),

$$R\Gamma(K'_n, \mathcal{F}) = R\lim_e (\Gamma((X,T(n)e,\gamma(n)), \mathcal{F})) = M(n)$$

thus we are done. □
Lemma (6.6.4.5). Situation as in (6.6.3.7), the complex $\Omega_{D(\bullet)}$ is homotopic to 0 as a $D(\bullet)$-cosimplicial module.

Proof: This complex is the $p$-adic completion of the base change of the cosimplicial module $M_\bullet = (\Omega_{P^\bullet_{A/A}})$ under the cosimplicial ring map $P^\bullet_A \to D(\bullet)$. Then it suffices to show $M_\bullet$ is homotopic to 0. For this, the whole thing can be written down clearly, Cf. [Sta]07LA.

Lemma (6.6.4.6). In situation (6.6.3.7), for any cosimplicial module $M^*_\bullet$ over the cosimplicial ring $D^*(\bullet)$ and $i > 0$, the cosimplicial module

$$M_0 \hat{\otimes}_{D(0)} \Omega_D^i \to M_1 \hat{\otimes}_{D(1)} \Omega_D^i \to \cdots$$

is homotopic to 0.

Proof: □

Crystal Case

Prop. (6.6.4.7). Situation as in (6.6.3.7), and let $\mathcal{F}$ be a crystal in Qco modules, and let $(M, \nabla)$ be the corresponding module with connection over $D$ by (6.6.3.9), then the complex

$$M \hat{\otimes}_{D} \Omega_D^*$$

computes $R\Gamma((X/S)_{cryst}, \mathcal{F})$.

Proof: Use the spectral sequence associated to the double complex

$$K^{a,b} = M \hat{\otimes}_{D} \Omega_D^b$$

Then the rows $K^{a,*}$ is acyclic for $a > 0$ by (6.6.4.6) and (8.1.2.21), and $K^{0,*}$ is quasi-isomorphic to $R\Gamma((X/S)_{cryst}, \mathcal{F})$ by (6.6.4.4). Now we look at the other direction, (4.7.1.7) and (6.6.3.8) show that each of the $b$ maps $D \to D(b)$ determines the same quasi-isomorphism

$$M \hat{\otimes}_{D} \Omega_D^* \cong M \hat{\otimes}_{D(b)} \Omega_D^*$$

as their inverse is given by the same $D(b) \to D$. Then it is clear that the $E_2$ page in this direction is $H^a(M \hat{\otimes}_{D} \Omega_D^*)$ in the zero-th row and vanish otherwise, so we get the desired isomorphism by edge morphisms. □

Prop. (6.6.4.8) [de Rham Comparison for Crystalline Cohomology]. In situation (6.6.3.11), let $\mathcal{F}$ be a crystal in Qco modules, and let $(M', \nabla')$ be the corresponding module with connection over $D'$ by (6.6.3.12), then the complex

$$M \hat{\otimes}_{D'} \Omega_{D'}^*$$

computes $R\Gamma((X/S)_{cryst}, \mathcal{F})$.

Proof: Let $b : D' \to D$, $a : D \to D'$ be the maps defined in (6.6.3.12), then by (6.6.4.7), it suffices to prove the base change along $a, b$ induces quasi-isomorphisms

$$M \hat{\otimes}_{D} \Omega_D^* \cong M \hat{\otimes}_{D'} \Omega_{D'}^*.$$
a \circ b \text{ is trivial, thus it suffices to prove that } b \circ a \text{ induces an automorphism of } M \widehat{\otimes}_D \Omega^\bullet_D. \text{ In fact, this is true for any morphism } \rho : D \to D \text{ of pd-algebras over } A \text{ compatible with the map } D \to C:

Write } \rho(x_i) = x_i + z_i, \text{ where } z_i \in J \text{ because } \rho \text{ is compatible with } D \to C. \text{ Then we can factor } \rho \text{ as }

\[
D \xrightarrow{\sigma} D \langle \xi_i \rangle^{^\wedge} \xrightarrow{\tau} C
\]

where } \sigma(x_i) = x_i + \xi_i \text{ and } \tau(\xi_i) = z_i.

Notice that there exists an automorphism } \alpha \text{ of } D \langle x_i \rangle^{^\wedge} \text{ that maps } x_i \text{ to } x_i - \xi_i \text{ and } \xi_i \text{ to } \xi_i. \text{ (Such a map exists because by universal property, it suffices to give a map of pairs }

\[
(P, J) \to D_{P, \gamma}(J)(\xi_i) = D_{P[\xi_i], \gamma}(JP[\xi_i] + (\xi_i))\]

by(4.7.0.17), \text{ and we surely have.}

Now } \alpha \text{ is an automorphism, we have a quasi-isomorphism }

\[
M \widehat{\otimes}_D \Omega^\bullet_D \cong M \widehat{\otimes}_D,\sigma \Omega^\bullet_{D(\xi_i)}
\]

by(4.7.1.7). Also } \tau \text{ induces an isomorphism because it has a right inverse, which is an isomorphism by(4.7.1.7) again, so } \rho \text{ induces an isomorphism.} \Box

Cor.(6.6.4.9) [Crystalline-de Rham Comparison modulo } p]. \text{ In situation(6.6.3.11), if } R \text{ is a smooth } A/p\text{-algebra, then there is a natural quasi-isomorphism }

\[
R \Gamma_{\text{crys}}(R/A) \otimes^L A/p \cong \Omega_{R/(A/p)}^\bullet
\]

of commutative algebra objects.

Proof: we choose } P \text{ to be a smooth lift of } R^? \text{ to } A, \text{ then } J = IP, \text{ and by(4.7.0.11), the pd-structure extends to } P, \text{ thus } D_{P/A, \gamma} = P, \text{ and notice } \Omega^\bullet_{P/A} \text{ is finite projective hence flat, so } \Omega^\bullet_{P/A} \text{ is } K\text{-flat(5.3.3.2), and the left side of is just } \Omega^\bullet_{P/A} \otimes_A A/p = \Omega^\bullet_{R/(A/p)} \text{ by(6.6.4.8)(4.7.1.2) and(4.4.3.6).} \Box

5 Properties

Cf.[Sta]Chap55.24.

Def.(6.6.5.1) [Higher Direct Images]. \text{ Let } p \text{ be a prime number, } (S, T, \gamma) \to (S', T', \gamma') \text{ be a morphism of PD-schemes over } \mathbb{Z}_p \text{ and } f : X/S \to X'/S'_0 \text{ be a morphism of schemes that } p \text{ is locally nilpotent on } X \text{ and } X'. \text{ For the rest, Cf.[Sta]07MJ.}

Def.(6.6.5.2) [F-Crystals]. \text{ In situation(6.6.2.2), let } S = \text{ Spec } A \text{ where } (A, I, \gamma) \text{ is a divided power algebra with } p \in I, \text{ and there is a Frobenius } \sigma \text{ on } A \text{ extending that of } A/I. \text{ Since the absolute Frobenius on } X \text{ and } S_0 \text{ are compatible, thus there is a morphism of crystalline site } (F_X)_{\text{crys}} : (X/S)_{\text{crys}} \to (X/S)_{\text{crys}}.

Then an } F\text{-crystal} \text{ on } X/S \text{ relative to } \sigma \text{ is a pair } (\mathcal{E}, F_\mathcal{E}) \text{ given by a crystal in finite locally free } \mathcal{O}_{X/S}\text{-modules(6.6.3.6) together with a map }

\[
F_\mathcal{E} : (F_X)_{\text{crys}}^* \mathcal{E} \to \mathcal{E}.
\]

A } \text{non-degenerate } F\text{-crystal} \text{ is an } F\text{-crystal that there exists a map } V : \mathcal{E} \to (F_X)_{\text{crys}}^* \mathcal{E} \text{ that } V \circ F_\mathcal{E} = p^i \text{ id for } i \geq 0.
6.7 Prismatic Cohomology

Main references are [[Sta]], [Prisms and Prismatic Cohomology, Scholze], [Notes on Prismatic Cohomology, Bhatt], [Prismatic Cohomology notes, Kedlaya].

1 Prisms

Def. (6.7.1.1) [Prisms]. A prism is a pair $(A,I)$ where $A$ is a $\delta$-ring and $I$ is an ideal of $A$, that $V(I)$ is a Cartier divisor on $\operatorname{Spec} A$, $A$ is derived $(p,I)$-complete, and $p \in I + \varphi(I)A$.

A prism $(A,I)$ is called perfect prism if $A$ is a perfect $\delta$-ring $\text{(4.5.4.25)}$. It is called bounded prism if $A/I$ has bounded $p^\infty$-torsion. It is called crystalline prism if $I = (p)$. It is called orientable if $I$ is principal. It is called oriented if $I = (d)$ for $d$ fixed.

A map of primes is called (faithfully)flat iff the map $A \to B$ is $(p,I)$-completely (faithfully)flat $\text{(4.6.7.1)}$.

Lemma (6.7.1.2). Let $A$ be a $\delta$-ring and $I$ be a locally principal ideal contained in $\operatorname{rad}(A)$ that $(p,I) \subset \operatorname{rad} A$, then the following are equivalent:

- $p \in I^p + \varphi(I)A$.
- $p \in I + \varphi(I)A$.
- There is a f.f. morphism of $\delta$-rings $A \to A'$ where $A'$ is a finite product of localizations of $A$ $\varphi$-stable multiplicative subsets that $IA'$ is generated by a distinguished element $d$ and $d, p \in \operatorname{rad}(A')$.

Proof: $1 \to 2$ is trivial, for $2 \to 3$: Choose $(g_1, \ldots, g_r) = A$ that $IA_{g_i}$ is principal. Let $B = \prod_{i=1}^r A_{g_i}$, so $A \to B$ is f.f. and $IB = (f)$ is principal. Let $A'$ be the localization of $B$ along the ideal $(p, f)\text{(4.1.1.31)}$, then $p, f \in \operatorname{rad} A'$. Then $A \to A'$ is still f.f., because it is flat hence the image is stable under generalization by $\text{(4.4.1.19)}$, so it must be all of $\operatorname{Spec} A$ because it contains $(p,I)$ by construction, and $(p,I) \in \operatorname{rad} A$ by hypothesis.

Now because $p \in \operatorname{rad} A$, each localization of $A$ has a compatible $\delta$-structure, and $\widetilde{A}$ is a finite product of localizations of $A$, thus it has a $\delta$-structure, and $d$ is distinguished by $\text{(4.5.4.23)}$.

$3 \to 1$: We need to check that $p = 0$ in $A/(I^p + \varphi(I)A)$, but this can be checked after base change to $A'$, which is $p = 0 \in A'/\varphi(d))$. This is true, because $d^p = d^p + p\delta(d)$ and $\delta(d)$ is a unit. $\square$

Remark (6.7.1.3) [Examples of Prisms].

- If $A$ is a $p$-torsionfree and $p$-adically complete $\delta$-ring $A$, the pair $(A, (p))$ is a bounded crystalline prism.
- $q$-de Rham cohomology $\text{(4.5.4.24)}$ determines a bounded prism. (completeness and boundedness is clear, and $p \in (d, \varphi(d))$ because ?)
- Breuil-Kisin cohomology $\text{(4.5.4.24)}$ determines a bounded prism. (boundedness is clear, and ?)
- $A_{\text{inf}}$-cohomology $\text{(4.5.4.24)}$ determines a bounded prism. (The same reason as item 2).

Prop. (6.7.1.4) [Universal Oriented Prism]. Let $A_0 = \mathbb{Z}_p\{d, \delta(d)^{-1}\}$ be the localization $\delta$-ring $\text{(4.5.4.15)}$ of the free $\mathbb{Z}_p$-$\delta$-ring on the variable $d$, and let $A$ be the derived $(p,d)$-completion of $A_0$ (it is discrete by $\text{(4.6.7.7)}$), and let $I = (d)$, then $(A,I)$ is a bounded oriented prism, and it is the initial object in the category of bounded oriented prisms.

Moreover, the sequence $(p,d)$ is regular and the Frobenius $\varphi : A/p \to A/p$ is $d$-completely flat.
6.7. PRISMATIC COHOMOLOGY

Proof: It is clearly a prism and universal. For the assertions, firstly we show $A/(p, d) = A_0/(p, d)$: notice $A \otimes_{\mathbb{Z}} A_0/(p, d) = A_0/(p, d)$ by (4.6.7.4), so we can replace $\otimes$ with $\otimes$. Similarly for $A/(p, d^p)$ because $A$ is $(p, d^p)$-complete. Now this map is.

$\phi$ does not preserve coproducts.

Prop. (6.7.1.5). Let $(A, (d))$ be the universal prism (6.7.1.4) and let $B = A \{ \varphi(d)/p \}^{\wedge}$ (derived $(p, d)$-completion), then $B$ is $(p, d)$-complete, $p$-torsionfree and it equals the derived $(p, d)$-completion of the pd-envelope $D_{A, \delta}(d)$ of $(A, (d))$. In particular, $(B, (p))$ is a crystalline prism, by (4.5.4.18).

Proof: $B$ is $p$-complete by (4.6.6.16), as $A$ is $p$-torsionfree. Also $d^p = p(\varphi(d)/p - \delta(d))$, so $B$ is also $(p, d)$-complete. The last assertion follows from (4.7.0.21) and (6.7.1.4).

Cor. (6.7.1.6) [Connection with Crystalline Prism]. In the above situation, $B$ is also a $\delta$-ring by (4.5.4.17), and both $\varphi(d), p$ are distinguished in $B$ and $\varphi(d)$ divides $p$ in $B$, so by (4.5.4.22) $\varphi(d) = (p)$.

Now the composition of maps of $\delta$-rings (4.5.4.5) $\alpha : A \overset{\varphi}{\to} A \to B$ promotes to a morphism of prisms (6.7.1.5) $(A, (d)) \to (B, (p))$ which decompose as

$$(A, (d)) \overset{\varphi}{\to} (A, \varphi(d)) \to (B, (\varphi(d))) = (B, (p))$$

Prop. (6.7.1.7) [Rigidity of Maps]. If $(A, I) \to (B, J)$ is a morphism of prisms, then $I \otimes_A B = J$, in particular, $IB = J$. Conversely, if $B$ is a derived $(p, I)$-complete $\delta$-$A$-algebra, then $(B, IB)$ is a prism iff $B[I] = 0$.

Proof: For the first assertion, it suffices to show that $I \otimes_A B \to J$ is surjective, because they are both invertible sheaves on $B$. Choose f.f. ring morphisms $A \to A', B \to B'$ as in (6.7.1.2) and there is a morphism $A' \to B'$ extending $A \to B$, (by taking $B$ as the localization of $A' \times_A B$ along $(p, J)$ and do the construction again). Then $IB' \subset JB'$ are an inclusion of principal ideals generated by distinguished elements, thus they are equal, by (4.5.4.22), finally we use faithfully flatness.

For the second assertion, notice $B[I] = 0$ iff $I \otimes_A B \to IB$ is an isomorphism. If $(B, IB)$ is a prism, then clearly $I \otimes_A B \to IB$ is an isomorphism, because they are both invertible sheaves. The converse is also trivial.

Prop. (6.7.1.8) [Prism is Nearly Principal]. Let $(A, I)$ be a prism, then the ideal $\varphi(I)A$ is a principal ideal, and any generator is a distinguished element. In particular, if it is a perfect prism, then $I = (f)$ where $f$ is a distinguished element.

Proof: It suffices to prove $\varphi(I)A$ is generated by a single distinguished element, and then use (4.5.4.21). By (6.7.1.2), we can assume $p = a + b$ where $a \in I^p, b \in \varphi(I)A$. Now we show $b$ generates $\varphi(I)A$: choose a f.f. map as in (6.7.1.2), and then it suffices to check that $b : A' \to \varphi(I)A'$ is surjective. Now $\varphi(I)A' = (d), a = xd^p, b = y\varphi(d)$, so it suffices to show $y$ is a unit in $A'$. Now $(p, d) \in \text{rad} A'$, it suffices to show $A'/(p, f, y) = 0$. If not, we localize along $(p, f, y)$, then we may assume $(p, f, y) \in \text{rad} A'$.

The equation $p = a + b$ implies $p(1 - y\varphi(d)) = d^p(x + y)$, and the left side is distinguished because $p$ does and $1 - y\varphi(d)$ is a unit, by (4.5.4.21). Then (4.5.4.22) shows $d^{p-1}(x + y)$ is a unit, then so does $d$, contradicting $d \in \text{rad} A'$.

Remark (6.7.1.9). Notice the proof goes through even $I$ is only a locally principal ideal of $A$. 


Cor. (6.7.1.10). If \((A, I)\) is a prism, the invertible \(A\)-modules \(\varphi^*(I) = I \otimes_{A, \varphi} A\) and \(I^p\) are trivial.

Proof: Cf. [Prisms, Scholze, P25].

Prop. (6.7.1.11)[Properties of Bounded Prisms]. Let \((A, I)\) be a bounded prism, then
1. Any derived \((p, I)\)-complete and \((p, I)\)-completely flat \(A\)-complex \(M \in D(A)\) is discrete and \((p, I)\)-complete. For any \(n \geq 0\), we have \(M[I^n] = 0\) and \(M/I^n M\) has bounded \(p\)-torsion.
2. \(A\) is \((p, I)\)-complete, \(A/I\) is \(p\)-adically complete, \(A[I^n] = 0\) and \(A/I^n\) has bounded \(p\)-torsions.
3. The category of (faithfully)flat prisms over \((A, I)\) identifies with the category of \((p, I)\)-completely (faithfully)flat \(A\)-algebras \(B\) by the bijection \(B \leftrightarrow (B, IB)\).
4. \((Bounded\ Prisms\ are\ fpqc-Locally\ Orientable)\) There is a \((p, I)\)-completely faithfully flat \(\delta\)-\(A\)-algebra \(B\) that \(IB = (d)\), where \(d\) is distinguished and determines a nonzero divisor of \(B\). Also \((B, IB)\) is bounded.

Proof: 1: By (4.6.7.7).
2 follows from 1. For \(A/I\), it is derived \(p\)-complete by (4.6.6.8), then it is \(p\)-adically complete by (4.6.6.16).
3: By definition, a (faithfully)flat \((A, I)\)-prism is \((p, I)\)-completely (faithfully)flat (4.6.7.1). Conversely, by (6.7.1.7), it suffices to show that \(B[I] = 0\), and this follows from item 1.
4: We may choose \(B\) to be the derived \((p, I)\)-completion of the \(\delta\)-ring defined in (6.7.1.2), then it is also \((p, I)\)-completely faithfully flat (4.6.7.4), and by item 2 and 3 it determines a bounded prism \((B, IB)\).

Prop. (6.7.1.12)[The Site of Bounded Prisms]. The prismatic site is the opposite category of the category of bounded prisms where the covers are determined by f.f. map of prisms.

Then the functors that maps \((A, I)\) to \(A\) or \(A/I\) are sheaves on this cohomology with vanishing higher cohomologies.

Proof: To show this is a site, we need to check the base change of covers. If \((C, IC) \xleftarrow{\rho} (A, IA) \xrightarrow{\delta} (B, IB)\) is a diagram that \(b\) is f.f., then we let \(D\) be the derived \((p, I)\)-completion of \(B \otimes^L_A C\), then \(C \rightarrow D\) is also \((p, I)\)-completely f.f. by (4.6.7.5), so by (6.7.1.11) and (6.7.1.11) \(D\) is discrete and \((D, ID)\) is a bounded prism over \((A, IA)\). It is clear this is a base change in the category of bounded prisms.

The assertion about cohomology follows from [Scholze, Prism, 3.12].

Prismatic Envelopes

Prop. (6.7.1.13)[Prismatic Envelopes]. Let \((A, I)\) be a prism, then the forgetful functor from the prisms over \((A, I)\) to \(\delta\)-pairs over \((A, I)\) admits a left adjoint, called the prismatic envelope which maps \((B, J)\) to \(B\{\frac{J}{d}\}^\wedge\).

Proof: If we can construct this locally, then we can construct it globally by gluing and the universal property, so we can localize and assume \(I = (d)\) where \(d\) is distinguished. Let \(B'\) be the free \(\delta\)-ring over \(A\) generated by \(\{x/d | x \in J\}\) (4.5.4.10) and \(B_1\) the derived \((p, d)\)-completion module of \(B\) which is a \(\delta\)-algebra by (4.5.4.18).

If \(d\) is torsion-free in \(B_1\), then \((B_1, (d))\) is a prism that satisfies the universal property. Otherwise we choose the maximal \(d\)-torsion-free quotient (4.1.1.14) (4.5.4.14) and taking the derived \((p, d)\)-completion module, and we can do this to \(\mathbb{N}_0\), where we take the filleted colimit, then it is
$d$-torsion-free and $(p, d)$-complete, by (4.6.6.5) and any prism over $A$ map factors through this chain. □

**Cor. (6.7.1.14).** In the above situation, if $(B, J)$ is $(p, I)$-completely flat over $A$, and $J = (I, x_1, \ldots, x_n)$ where $(x_1, \ldots, x_n)$ is a $(p, I)$-completely regular sequence w.r.t. $A$, then the prismatic envelope of $(B\{\frac{1}{d}\}^\wedge, IB\{\frac{1}{d}\}^\wedge)$ is flat over $(A, I)$ (6.7.1.1).

Moreover, It is compatible with completed derived base change along a $(p, I)$-completely flat change in $(A, I)$, by universal properties and the fact the completed derived base change of it is discrete (4.6.7.5). Also, it is compatible with completed derived base change along a $(p, I)$-completely flat map $(B, J) \to (B', J')$.

**Proof:** It suffices to check locally for $I = (d)$ that $B_1 = (B\{\frac{y}{d}, \ldots, \frac{z}{d}\})^\wedge$ as a simplicial $\delta$-ring is $(p, I)$-completely flat over $A$, then it is discrete and is torsionfree by (6.7.1.11), thus it is a prism over $(A, (d))$ by (6.7.1.7). And for the flat localization, notice the image of $x_1, \ldots, x_n$ is also $(p, I)$-completely regular w.r.t. $A$.

Consider the following diagram of derived $(p, d)$-complete simplicial $\delta$-rings:

$$
\begin{array}{ccccccccc}
Z_p\{z\}^\wedge & \xrightarrow{z \mapsto d} & A & \rightarrow & B & \rightarrow & B\{\frac{x_1}{d}, \ldots, \frac{x_n}{d}\}^\wedge = C \\
\downarrow_{z \mapsto \varphi(y)} & & \downarrow & & \downarrow & & \\
Z_p\{y\}^\wedge & \rightarrow & A' & \rightarrow & B' & \rightarrow & B'\{\frac{x_1}{\varphi(d)}, \ldots, \frac{x_n}{\varphi(d)}\}^\wedge = C' \\
\downarrow & & \downarrow & & \downarrow & & \\
D = A'\{\frac{\varphi(y)}{p}\}^\wedge & \rightarrow & B'' & \rightarrow & B''\{\frac{y_1}{p}, \ldots, \frac{y_n}{p}\} = C''
\end{array}
$$

where each square is completed derived tensor product. Notice the lat term has denominator $p$ because $\varphi(y)$ and $p$ are both distinguished in $\pi_0(D)$, so by (4.5.4.22) $\varphi(y)$ is a unit in $D$.

The leftmost arrow is $(p, z)$-completely f.f. by (4.5.4.10)(4.6.7.4), so all the vertical arrow in the upper row is $(p, z)$-completely flat by (4.6.7.5). Now the map $D \to C''$ is $(p, z)$-completely flat by (4.7.0.24), noticing that the conditions holds, by (4.6.7.5).

Now by definition the $(p, d)$-completely flatness is defined by flatness after base change to $Kos(A, p, d)(8.1.3.5)$, it suffices to show that there is a map $D \to Kos(A', p, d)$. To show this, it suffices to assume $A' = Z_p\{y\} = Z_p[y_1, \ldots, y_n, \ldots]$ and base change. In this case, $p, y$ is a regular sequence, so by (4.7.0.21) $D$ is the derived completion of $DZ_p\{y\}(\{y\})$, and $Kos(A', p, y) = \mathbb{F}_p[y_1, \ldots, y_n]$, so $A' \to Kos(A', p, d)$ factors through $D$ by universal property. □

### 2 Perfect Prisms

**Prop. (6.7.2.1) [Properties of Perfect Prisms].** Let $(A, I)$ be a perfect prism (6.7.1.1), then:

- $I = (d)$ where $d$ is distinguished and is a nonzero-divisor.
- $A$ is $p$-torsionfree and $p$-adically complete, hence there is a natural isomorphism $A \cong W(A/p)$ of $\delta$-rings.
- $A$ is $(p, I)$-complete.

**Proof:** 1: $I$ is principal by (6.7.1.8). $d$ is distinguished by (4.5.4.23), it is nonzero-divisor by definition of prisms.
2: This is because $A$ is $p$-torsionfree by (4.5.4.27) and thus $p$-adically complete by (4.6.6.16), then $A \cong W(A/p)$ by the equivalence in (4.5.4.28).

3: Use item 2, then $A/p$ is perfect by (4.5.4.28), thus $A/p[I^\infty] = A/p[I]$. $A/d[p^\infty] = A/d[p]$ follows from (4.5.4.30).

4: This follows from item 3 and (6.7.1.11).

**Prop. (6.7.2.2) [Perfection of Prisms]**. There is a perfection of prisms functor that maps a prism $(A, I)$ to a perfect prism $(A_{\infty}, IA_{\infty})$ left adjoint to the inclusion functor.

**Proof**: Let $A_{\infty}^{\prime} = A_{\text{perf}}$ be the perfection of $A$ as a $\delta$-ring (4.5.4.26), and $A_{\infty}$ be the derived $(p, I)$-complete of $A_{\infty}^{\prime}$ as a $\delta$-ring (4.5.4.18), then the universal property follows form that of derived completion and perfection once we proved that $A_{\infty}$ is perfect and $IA_{\infty} = (d)$ where $d$ is a nonzero-divisor.

$A_{\infty}$ is perfect because the Frobenius is isomorphism on $A_{\text{perf}}$ and derived $(p, I)$-completion and $(p, \varphi(I))$-completion coincide (they have the same radical (4.6.6.15)).

$A_{\infty}$ is $p$-adically complete because it is $p$-torsionfree (4.5.4.27), and then use (4.6.6.16).

Now (6.7.1.9) and the fact $A_{\infty}$ is perfect shows $IA_{\infty} = (d)$ where $d$ is distinguished, and (4.5.4.30) shows $d$ is a nonzero-divisor, so we are done. □

**Prop. (6.7.2.3) [Perfect Prisms are Final]**. Let $(A, I)$ be a perfect prism, then for any prism $(B, J)$, a map $A/I \to B/J$ will induce a map of prisms $(A, I) \to (B, J)$.


This map will induce a map $A \cong W((A/I)^{\emptyset}) \to W((B/J)^{\emptyset})$. And there is a Fontaine’s functor $W((B/J)^{\emptyset}) \to B(10.3.9.7)$ which is a $\delta$-map. Thus we obtain a map $A \to B$. And this map can be seen to be lifting $A/I \to B/J$. □

### 3 Integral Perfectoid Rings

**Def. (6.7.3.1) [Integral Perfectoid Rings]**. A commutative ring $R$ is called an integral perfectoid ring if it has the form $A/I$ for a perfect prism $(A, I)$. An equivalent definition of an integral perfectoid ring is given in (6.7.3.6).

**Def. (6.7.3.2) [Special Fiber]**. For an integral perfectoid ring $R$, then special fiber of $R$ is defined to be $\overline{R} = R/\sqrt{p}R$. It is perfect, by (6.7.3.5).

**Prop. (6.7.3.3) [Perfect Prisms and Integral Perfectoid Rings]**. The mapping $(A, I) \to A/I$ defines an equivalence of categories between perfect prisms and integral perfectoid rings, where the converse is given by $R \mapsto (A_{\text{inf}}(R), \ker(A_{\text{inf}}(R) \to R))(4.5.1.15)$.

**Proof**: To show $A \cong A_{\text{inf}}(A/I)$, by (4.5.4.28), it suffices to show there is a natural isomorphism $A/p \cong (A/I)^{\emptyset}$. By (4.5.1.18), $(A/I)^{\emptyset}$ identifies with $d$-adic completion of $A/p$. Then it suffices to show $A/p$ is $I$-adically complete, which is by (4.6.6.16), as $A/p$ is derived $d$-complete because $A$ does (4.6.6.8).

Now we have the Fontaine’s map $A = A_{\text{inf}}(A/I) \to A/I$, this map is surjective because $\varphi : A/(p, I) \to A/(p, I)$ is surjective as $A/p$ is perfect. Also this is just the quotient map $A \to A/I$ because they are equal when modulo $p$, and then use (4.5.4.28).

**Cor. (6.7.3.4)**. Any perfect $\mathbb{F}_p$-algebra is an integral perfectoid ring corresponding to a crystalline prism, by (4.5.4.28).

Any integral perfectoid ring is $p$-adically complete, by (6.7.1.11).
Prop. (6.7.3.5). If $R$ is a perfectoid ring, then
- $R$ is semiperfect.
- There exists an element $\varpi \in R$ that admits a compatible system $\varpi^{1/p^n}$ of $p$-power roots s.t. $\varpi = pu$ for a unit $u$ and the kernel of the Frobenius $\varphi : R/p \to R/p$ is generated by $\varpi^{1/p}$.
- $\sqrt{p}R = \bigcup_n (\varpi^{1/p^n})$, and it is flat.

Proof: 1: Let $R = A/d$ where $A = A_{inf}(R)$, then $R/p = A/(p,d)$, so $\varphi_{R/p}$ is surjective, as $A/p = R^\circ$ is perfect.

2: Notice $d = [a_0] - pu$ for a unit $u \in A$ by (4.5.4.30), then we can take $\varpi$ to be the image of $[a_0]$ in $R$, and then $\varpi^{1/p^n} = [a_0^{1/p^n}]$.

3: firstly the LHS contains the RHS, and $R/\bigcup_n (\varpi^{1/p^n})$ is perfect hence reduced, so the two sides are equal. To check it is flat, we need to check that $M \otimes^L_R \sqrt{p}R$ is discrete, or equivalently $M \otimes^L_R R \in D^{\geq -1}$ where $R = R/\sqrt{p}R$ is perfect. But there is a distinguished triangle $M \otimes^L_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p[-1] \to M \to M^{[1]}(\mathbb{Q}_p)$ is $\mathbb{Z}_p$-flat and the fact $[1] = 0$, it suffices to prove $M \otimes^L_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p \otimes^L_R R \in D^{\geq -2}(R)$. Now $M \otimes^L_{\mathbb{Z}_p} \mathbb{Q}_p/\mathbb{Z}_p$ has cohomology groups $p^\infty$-torsion, so using canonical truncation, it suffices to show $M \otimes^L_R R \in D^{\geq -1}$ for any $p^\infty$-torsion $M$. Because tensoring commutes with filtered colimits, it suffices to show for $M$ an $R/p^n$-module. Now using exact sequences like 

$$0 \to M[p]/M[p^2] \to M/M[p^2] \to M[p]/M[p^2] \to 0,$$

we can reduce to the case $M$ is an $R/p$-module.

Now there is a commutative diagram 

$$A_{inf}(R) \longrightarrow A_{inf}(R) \quad \downarrow \quad \downarrow \quad A_{inf}(R) \longrightarrow R$$

and $d$ is $p$-torsionfree in both $A_{inf}(R)$ and $A_{inf}(R)$ (4.5.4.30), and $d = [a_0] - pu = pu \in W(R)$ (as $a_0 = 0 \in R$), so $R = W(R)/d$ and this is a Tor-independent pushout square. Thus $M \otimes^L_R R \cong M \otimes^L_{W(R)} W(R)$. As $p$ is nonzero divisor in both $A_{inf}(R)$ and $A_{inf}(R)$, and $pM = 0$, we have a similar diagram quotient by $p$, and by the same reason $M \otimes^L_{W(R')} W(R) \cong M \otimes^L_{R'} R$. Now the kernel of $R^b \to R$ is of the form $(f^{1/p^n})$, where $f$ corresponds to $(\omega^{1/p^n})$, so the claim follows from (4.5.1.8).

4: notation as in the proof of item2, it suffices to show the $A$-module $R[p]$ is annihilated by $[a_0^{1/p^n}]$ for $n \geq 0$. But $R[p] = A/d[p] = A/p[d] = R^b[d]$, and $d = [a_0]$ on $R^b$, which is perfect, so we are done. \hfill \square

Prop. (6.7.3.6) [Equivalent Definition of Integral Perfectoid Rings]. A commutative ring $R$ is an integral perfectoid ring if and the following are satisfied:
- $R$ is $p$-adically complete and $R/p$ is semiperfect.
- The kernel of $\theta_R : A_{inf}(R) \to R$ (4.5.1.15), notice $R$ is $p$-adically complete is principal.
- There exists some $\varpi \in R$ that $(\varpi^p) = (p)$.

And if $R$ is $p$-torsionfree, the condition2 can be replaced by: $R$ is $p$-normal.??.
Prop.(6.7.3.7)[Pushout of Integral Perfectoid Rings]. Integral perfectoid rings are closed under pushouts in the category of derived p-complete rings: i.e. if $C \leftarrow A \rightarrow B$ are maps of integral perfectoid rings, then $B \widehat{\otimes}_A C$ is also an integral perfectoid ring.

Proof: Let $R = C^\flat \otimes_{A^\flat} B^\flat = C^\flat \otimes_{A^\flat} B^\flat$ which is a perfect ring, by(A.5.1.3) and(A.5.1.8). Then we have

$$W(R) = W(A^\flat) \widehat{\otimes}_W(A^\flat) W(B^\flat),$$

because this can be checked via derived Nakayama(A.6.6.10). Now use the fact $A = W(A^\flat)/d$ for some distinguished element $d$, and then $B = W(B^\flat)/d, C = W(C^\flat)/d$ by rigidity(A.7.1.7), and $d$ is nonzero-divisor in $W(B^\flat), W(C^\flat), W(R)$ by(A.4.5.28), so taking derived base change along $W(A^\flat) \rightarrow A$, we get

$$D = W(R)/d = B \widehat{\otimes}_A C,$$

and $W(R)$ is a perfect prism, by(A.7.1.7), so $D = W(R)/d$ is an integral perfectoid ring and equals $B \widehat{\otimes}_A C$. 

Cor.(6.7.3.8). The category of integral perfectoid rings is closed under arbitrary colimits and products in the category of derived p-complete rings.

But it is not closed under equalizers: Notice by Ax-Sen-Tate, $(\mathcal{O}_p)^{\operatorname{Gal}(\overline{\mathbb{Q}}_p/\mathbb{Q}_p)} = \mathbb{Z}_p$, but $\mathbb{Z}_p$ is not an integral perfectoid by(A.7.3.6).

Proof: It suffices to show it is closed under products and sums?.
6.7. PRISMATIC COHOMOLOGY 757

Prop. (6.7.3.9) [Gluing]. Let $R$ be an integral perfectoid ring, $\overline{R} = R/\sqrt{pR}, S = R/R[\sqrt{pR}], \overline{S} = S/\sqrt{pS}$, then $\overline{R}, S, \overline{S}$ are perfectoids, and the square

$$
\begin{array}{ccc}
R & \rightarrow & S \\
\downarrow & & \downarrow \\
\overline{R} & \rightarrow & \overline{S}
\end{array}
$$

is both a homotopy fiber square (4.6.1.2) and pullback square. Moreover,

- $S$ is $p$-torsionfree.
- $\sqrt{pR}$ maps isomorphically onto $\sqrt{pS}$.
- $R[\sqrt{pR}]$ maps isomorphically to $\ker(R \rightarrow S)$, thus $x \mapsto x^p$ is bijective on $R[\sqrt{pR}]$.

In particular, any integral perfectoid ring is a fiber product of integral rings that is either perfect or $p$-torsionfree.

Proof: By (6.7.3.5), $R[\sqrt{pR}] = R[p^\infty]$. In particular, $S$ is $p$-torsionfree. Now if we know this is a homotopy fiber square, then we get 2, 3 by comparing the kernel. And if we know the kernel, then this is a pushout square by (4.1.1.23). So it suffices to show this is a homotopy fiber square.

Let $d = [a_0] - pu$ for a distinguished element of $A = A_{\inf}(R)$ that $R = A/(d)$, and the ideal $I = (a_0^{1/p^\infty}) \subset R^p$ and $J = R^p[I]$. Then the square

$$
\begin{array}{ccc}
W(R^p) & \rightarrow & W(R^p/J) \\
\downarrow & & \downarrow \\
W(R^p/I) & \rightarrow & W(R^p/I + J)
\end{array}
$$

is a homotopy fiber square: all vertices are $p$-torsionfree and $p$-adically complete, and the square gives a fiber square when modulo $p^n$(use induction on $n$ and (4.5.1.9)), and then take derived $p$-completions. Next we apply.

□

Cor. (6.7.3.10). Integral perfectoid rings are reduced.

Proof: By (6.7.3.9), we may assume $R$ is $p$-torsionfree or perfect. Thus it suffices to assume $R$ is $p$-torsionfree. Let $\varpi \in R$ that $\varpi^p = pu$ as in (6.7.3.6). If $x^p = 0$, we show inductively that $x \in \varpi^nR$. If $x = \varpi^n y$, then $y^p = 0$ as $R$ is $p$-torsionfree. Now the kernel of Frobenius $\varphi : R/p \rightarrow R/p$ is generated by $\varpi$, thus we have $y \in \varpi R$, so we can use induction.

□

4 Prismatic Site

Remark (6.7.4.1). In this subsection, fix a bounded prism $(A, I)$, all formal schemes over $A$ are assumed to have the $(p, I)$-adic topology, and formal schemes over $A/I$ are assumed to have the $p$-adic topology.

Def. (6.7.4.2) [Prismatic Site]. Let $(A, I)$ be a bounded prism and $X$ be a smooth $p$-adic formal scheme over $A/I$, let $(X/A)^\Delta$ be the site whose objects are bounded prisms $(B, IB)$ over $(A, I)$ together with a map $\text{Spf}(B/IB) \rightarrow X$ over $A/I$. The morphisms are the natural one, and the coverings in $(X/A)^\Delta$ are f.f. maps of prisms $(B, IB) \rightarrow (C, IC)$. There are structure sheaves $\mathcal{O}_\Delta((B, IB)) = B$ and $\mathcal{O}_\Delta((B, IB)) = B/IB$. They are sheaves by (6.7.1.12).

Thus $\mathcal{O}_\Delta$ is valued in $(p, I)$-complete $\delta$-$A$-algebras and $\mathcal{O}_\Delta$ is valued over $p$-complete-algebras (4.6.6.16).
**Def. (6.7.4.3)** [Perfect Prismatic Site]. The perfect prismatic site \((X/A)_{\Delta}^{\text{perf}}\) is the full subcategory of \((X/A)_{\Delta}\) consisting of perfect prisms. By (6.7.3.3), objects in this site are equivalent to the category of perfectoid rings \(R\) over \(A/I\) with a map \(\text{Spf } R \to X\).

**Remark (6.7.4.4).** If we further restrict to the site of perfect prisms \((S, I)\) that \(S/I\) is integrally closed in \(S[i^{\frac{1}{p}}]\), then we will get the notion of diamond of \((X[i^{\frac{1}{p}}], X)\), in sense of [?].

**Def. (6.7.4.5)** [Absolute Prismatic Site]. For a \(p\)-adic formal scheme \(X\) the absolute prismatic site consisting of bounded prisms \((B, J)\) with a map \(\text{Spf } B/IB \to X\).

**Prop. (6.7.4.6)** [Prismatic Site and Étale Site]. Let \(\mathcal{F}\text{sch}/X\) be the category of \(p\)-adic formal schemes over \(X\) with the étale topology, then there is a natural functor \(\mu: (X/A)_{\Delta} \to \mathcal{F}\text{sch}/X\) sending \((B, IB)\) over \(X\) to \(\text{Spf } B/IB \to X\).

This functor is cocontinuous: for any \(p\)-completely étale map \(B/IB \to C\), it is a derived \(p\)-completion of some étale map \(B/IB \to C\) by (4.6.7.9), and this can be lifted to a map \(B \to S_C\) by (6.7.1.11)(4.3.10.6) and (4.3.10.9), and we choose the \((p, I)\)-completion of \(S_C\), then it is a prism that lifts \(C\). Thus by (5.1.2.20) defines a morphism of topoi:

\[\mu: \text{Sh}((X/A)_{\Delta}) \to \text{Sh}(\mathcal{F}\text{sch}/X).\]

Also there is a natural map of topoi \(\text{Sh}(\mathcal{F}\text{sch}/X) \to \text{Sh}(X_{\text{ét}})\) by restriction, by (4.6.7.1). So we get a morphism of topoi

\[\nu: \text{Sh}((X/A)_{\Delta}) \to \text{Sh}(X_{\text{ét}}).\]

In particular, for any étale formal scheme \(U\) over \(X\), by definition of \(\mu(5.1.2.11)\), for any sheaf \(\mathcal{F}\),

\[(\nu_* \mathcal{F})(U/X) = H^0((U/A)_{\Delta}, \mathcal{F}|_{(U/A)_{\Delta}}).\]

**Cor. (6.7.4.7)** [Prismatic Complex and Hodge-Tate Complex]. In the above situation, we define prismatic complexes

\[\Delta_{X/A} = R\nu_* \mathcal{O}_X \in D(X_{\text{ét}}, A)\]

and the Hodge-Tate complex

\[\overline{\Delta}_{X/A} = R\nu_* \overline{\mathcal{O}}_X \in D(X_{\text{ét}}, \mathcal{O}_X).\]

The Frobenius action on \(\mathcal{O}_\Delta\) induces a \(\varphi\)-semi-linear map \(\Delta_{X/A} \to \Delta_{X/A}\). And there is a relation

\[\overline{\Delta}_{X/A} \cong \Delta_{X/A} \otimes_A^L A/I \in D(X_{\text{ét}}, A/I)\]

by the Grothendieck spectral sequences associated to the diagram of functors:

\[
\begin{array}{ccc}
\text{Mod}((X/A)_{\Delta}, \mathcal{O}_\Delta) & \xrightarrow{- \otimes \mathcal{O}_\Delta} & \text{Mod}((X/A)_{\Delta}, \overline{\mathcal{O}}_\Delta) \\
\downarrow^{\Gamma((X/A)_{\Delta}, -)} & & \downarrow^{\Gamma((X/A)_{\Delta}, -)} \\
\text{Mod}(X_{\text{ét}}, A) & \xrightarrow{} & \text{Mod}(X_{\text{ét}}, A/I)
\end{array}
\]
Affine Case

Def.(6.7.4.8) [Situation]. In this subsection, fix a bounded prism $(A, I)$ and a $p$-completely smooth $A/I$-algebra $R$ (or equivalently the $p$-adic completion of an étale $A$-algebra, by(4.6.7.9) and(4.6.6.16), and they define the same site by the universal property of completion).

Prop.(6.7.4.9) [Prismatic Site over Affine Formal Scheme]. The prismatic site of $R$ relative to $A$, denoted by $(R/A)_\Delta$ is the site whose objects are bounded prisms over $(A, I)$ together with an $A/I$-algebra map $R \to B/IB$. And it is endowed with the indiscrete topology(5.1.1.2), so sheaves on this site is just presheaves.

There are two natural sheaves on this site, $\mathcal{O}_\Delta$ maps a prism $(B, IB)$ to $B$ which is valued in $(p, I)$-complete $\delta$-$A$-algebras, and $\mathcal{O}_\Delta$ which maps a prism $(B, IB)$ to $B/IB$ which is valued in $p$-complete $R$-algebras(4.6.6.16)

Prop.(6.7.4.10) [Compare with Indiscrete Topology]. If $(X/A)_\Delta' \subset (X/A)_\Delta$ is a continuous map of sites that the former is endowed with the indiscrete topology, then it is a morphism of sites, by(5.1.2.14), so this induces a morphism of topoi

$$\text{Sh}((X/A)_\Delta) \to \text{Sh}((X/A)_\Delta')$$

by(5.1.2.19), then we have the Leray spectral sequence(5.3.1.10)

$$E_2^{p,q} = H^p(C', R^q f_*(\mathcal{F}^*)) \Rightarrow H^{p+q}(C, \mathcal{F}^*).$$

and by(5.3.1.8)(5.3.1.7) and(6.7.1.12), we have a natural isomorphism

$$R\Gamma((X/A)_\Delta', \mathcal{F}) \to R\Gamma((X/A)_\Delta, \mathcal{F})$$

for $\mathcal{F} = \mathcal{O}_\Delta$ or $\mathcal{O}'_\Delta$.

How to Compute the Prismatic Complex in the Affine Case

Lemma(6.7.4.11)[Weakly Final Object]. Let $(A, I)$ be a prism and let $R$ be a $p$-completely smooth $A/I$-algebra, then the category $(R/A)_\Delta$ admits a weakly final object. Moreover, we can choose it to be flat over $(A, I)$.

Proof: Let $F_0$ be the derived $(p, I)$-completion of a free $\delta$-ring over $A$ on the set $R$, then there is a surjection of $A$-algebras $F_0 \to R$, with kernel $J$ derived $(p, I)$-complete. Then(6.7.1.13) applied to the $\delta$-ring $(F_0, J)$ gives a prism $(F, IF)$ over $(A, I)$, and by construction it is an object of $(R/A)_\Delta$. And it is weakly final because of the universal properties of $F_0$(4.5.4.10) and $F$(6.7.1.13).

For the flatness, we temporarily call a $\delta$-pair $(B, J)$ good if

- $B$ is $(p, I)$-completely flat over $A$ and $J$ is $(p, I)$-complete.
- the prismatic envelope is flat over $(A, I)$ and its formation commutes with completed derived base change on a $(p, I)$-completely flat map $B \to B'$.

Then we need to show that $(F_0, J)$ is good. We have the following observations:

- Good pairs are stable under filtered colimit in the category of $\delta$-pairs $(B, J)$ that $J$ is derived $(p, I)$-complete. (Because filtered colimits of flat modules are flat(4.4.1.6).)
- If $(B, J)$ is a $\delta$-pair over $A$ with $B$ completely $(p, I)$-flat over $A$, and $B \to B'$ is a $(p, I)$-completely f.f. map that $(B', JB')$ is good, then $(B, J)$ is good. (This follows from(6.7.1.13) and the f.f. descent(6.7.1.13).)
Then we can write $B$ as a filtered colimit of $(p,I)$-complete algebras $B_n \to R$, and the kernel of each of them is locally generate by a $(p,I)$-completely regular sequence, so we can use the observations to pass to f.f. localization and filtered colimit to show that $(B,J)$ is good. Cf.[Prism, Scholze, 3.14].

\[\square\]

**Lemma (6.7.4.12) [Products].** The category $(R/A)\_\wedge$ admits products.

**Proof:** For $\delta$-rings $B, C \in (R/A)\_\wedge$, we can take the $\delta$-ring colimit $D_0 = B \otimes_A C$ (4.5.4.13), but it may not be compatible with $R$-actions. Instead, let $J$ be the kernel of the natural map

$$D_0 \to D_0/ID_0 \to B/IB \otimes_{A/IA} C/IC \to B/IB \otimes_R C/IC,$$

then $(D_0, J)$ is a $\delta$-ring over $(A, I)$, and then we can use (6.7.1.13) to get a prism $(D, ID)$ over $(A, I)$, then the maps $R \to B/IB \to D_0/ID_0 \to D/ID$ and $R \to C/IC \to D_0/ID_0 \to D/ID$ are equal (because they all factor through $D/J$), thus giving a product object in $(R/A)\_\wedge$. \[\square\]

**Prop. (6.7.4.13) [Čech-Alexander Construction for Prismatic Cohomology].** By (5.3.1.20)(6.7.4.10) and the lemmas (6.7.4.11)(6.7.4.12) above, the prismatic complex $\Delta_{R/A}$ is represented by the complex

$$F^0 \to F^1 \to F^2 \to \ldots.$$

In particular, $F^0 = F$ as constructed in (6.7.4.11) and each $F^n$ are $(p, I)$-completely $A$-flat, $I$-torsion-free and $(p, I)$-complete $\delta$-rings by (6.7.1.11) and (6.7.1.14).

Moreover, this complex is the prismatic envelope functor applied to the Čech nerve of $A \to F_0$, w.r.t. the Čech nerve $F^*$ of ideals $J^* = \ker(F^* \to F_0 \to R)$, because prismatic envelope is a left adjoint hence commutes with tensor product of pairs (6.7.1.13).

**Cor. (6.7.4.14).** $\Delta_{R/A}$ is derived $(p, I)$-complete and $\bar{\Delta}_{R/A}$ is derived $p$-complete, because each term of the complex $F^*$ is derived $(p, I)$-complete, so does its cohomology groups (4.6.6.8), thus so does $\Delta_{R/A}$ itself. Similarly for $\bar{\Delta}_{R/A}$, because each term of $F^*/I$ is $p$-complete (6.7.4.13) hence derived $p$-complete, by (4.6.6.16).

### 5 Hodge-Tate Comparison

**Def. (6.7.5.1) [Breuil-Kisin Twist].** Let $I$ be an invertible ideal of $A$, then for any $A/I$-module $M$, we define the **Breuil-Kisin twist** of $M$ as $M\{n\} = M \otimes (I/I^2)^n$. Notice this definable for $n \in \mathbb{Z}$ because $I/I^2$ is an invertible $O_{A/I}$-module, by definition (6.7.1.1). Also it is definable in the level of $D(A/I)$, as $(I/I^2)^n$ is locally free thus flat.

**Def. (6.7.5.2) [Completed de Rham Complex].** The **completed de Rham complex** is the derived $p$-completion of the de Rham complex of $\Omega_{X/(A/I)}$. We will use the derived $p$-completed de Rham complex in the sequel. It has a property that it coincides with the $p$-completion of its separate terms by (4.6.7.8) and (4.6.6.16) and the fact $\Omega_{X/(A/I)}$ is finite projective hence flat (4.4.5.12).

In fact, as $\Omega_{X/S}$ is finite locally free, the derived $p$-completion is just by tensoring $- \otimes_{R_0} R$, where $R_0$ is a smooth $A$-algebra that $R_0^0 = R$ by (4.6.7.9). In particular, the completed de Rham complex is compatible with base change and $p$-completely étaleextension, because the ordinary de Rham complex does (4.4.3.6)(4.4.7.6).
Prop. (6.7.5.3) [Hodge-Tate Comparison Theorem]. We have a structure map $\eta^0: O_X \to H^0(\overline{\Delta}_{X/A})$, and $H^\bullet(\overline{\Delta}_{X/A})$ is a dga by (4.6.1.3) applied to $M^\bullet = \Delta_{X/A}$ and (4.6.2.1) noticing $\mathcal{O}_\Delta$ is a sheaf of algebras. then the universal property of de Rham complex (6.2.1.4) and lemma (6.7.5.4) shows $\eta^0$ extends to a map 

$$\eta^o_R: \Omega^\bullet_{X/(A/I)} \to H^\bullet(\overline{\Delta}_{X/A})$$

of sheaves of $A/I$-dgas on $X_{\et}$.

Then this is an isomorphism of differential graded $A/I$-algebra. In particular $\overline{\Delta}_{X/A} \in D(X_{\et}, A/I)$ is a perfect complex with $H^i(\overline{\Delta}_{X/A}) \cong \Omega^i_{X/(A/I)}\{-i\}$.

Proof: The proof of the isomorphism is given in (6.7.6.10). □

Lemma (6.7.5.4). For any local section $f \in O_X(U)$, the differential $\beta_I(f) \in H^1(\overline{\Delta}_{X/A})\{1\}(U)$ squares to $0$.

Proof: This follows from (6.7.6.9) in the affine line case because $H^2(\overline{\Delta}_{X/A})\{1\}(U) = 0$, and for the general case, use the étale localization (6.7.6.2) and base change theorem (6.7.6.1), noticing that cup product survives through derived tensor product. □

Cor. (6.7.5.5) [Base Change]. The formation of $\Delta_{X/A} \in D(X_{\et}, A)$ commutes with base change along a bounded prism $(A, I A) \to (B, I B)$: Let $g: X_B = X \otimes_{Spf A/I A} Spf B/IB \to X$ be the projection, then

$$(g^*\Delta_{X/A})^\wedge \cong \Delta_{X_B/B}, \quad (g^*\overline{\Delta}_{X/A})^\wedge \cong \overline{\Delta}_{X_B/B}$$

where $(\cdot)^\wedge$ is the derived $(p, I)$-completion or $p$-completion.

Proof: Because both side are derived $(p, I)$-complete, we take their cylinder object and by derived Nakayama w.r.t. $B/(p, I)$ (4.6.6.10) it suffices to show the second, which is true because this is true for completed de Rham complexes (6.7.5.2). □

6 Proof of Hodge-Tate Comparison

The strategy is as follows: we study the affine case to construct and prove the Hodge-Tate comparison isomorphism in the affine case, and then this gives the construction of Hodge-Tate map in the general case, then we can also prove the general Hodge-Tate comparison by localizing at affine subschemes, so the affine case is important.

To prove the Hodge-Tate comparison isomorphism in the affine case, we use étale localization to reduce to the polynomial case, and then use flat base change to reduce to the oriented case. Then we use a slick strategy to reduce to the crystalline case, and finally reduce to crystalline comparison.

Lemma (6.7.6.1) [Base Change]. Let $R$ be a $p$-completely smooth $A/I$-algebra and $(A, I) \to (A', I')$ be a map of bounded prisms that $A \to A'$ has finite $(p, I)$-complete Tor amplitude (4.6.7.1). If $R' = R \otimes_A^{L} A'$ for the the base change, then the natural map induces an isomorphism

$$\Delta_{R/A}^{\wedge_L} A' \cong \Delta_{R'/A'}, \quad \overline{\Delta}_{R/A}^{\wedge_L} A' \cong \overline{\Delta}_{R'/A'}$$

Proof: We use the Čech nerve of a weakly final object (6.7.4.13) to compute the cohomology, then we notice the $(p, I)$-completed base change $- \otimes_A^{L} A'$ applied termwise to the Čech nerve of $A \to F^0$ is the Čech nerve of $A \to F^0 \otimes_A A'$, which is weakly final in $(R'/A')_\Delta$, by the universal property and the fact $(p, I)$-completed base change is a left adjoint.
Finally we use (4.6.7.8) to see that this termwise completed derived base change just represents \( \Delta_{R/A} \widehat{\otimes} L A' \) because each term of the prismatic envelope \( F \) is \((p, I)\)-completely flat over \( A \) and the completed derived base change of \( F^n \) is discrete by (6.7.4.13).

**Lemma (6.7.6.2) [Étale Localization].** Let \( R \to S \) be a \( p \)-completely étalemap of \( p \)-completely smooth algebras, then the natural map

\[
\overline{\Delta}_{R/A} \widehat{\otimes} L S \to \overline{\Delta}_{S/A}
\]

is an isomorphism.

**Proof:** Firstly the forgetful functor \((R/A)_{\Delta} \to (S/A)_{\Delta}\) has a right adjoint, described as follows: a prims \((B, IB) \in (B/S)_{\Delta}\) induces a \( p \)-completely étalemorphism of (discrete) rings \( B/IB \to B/IB \widehat{\otimes} L R S \) by (4.6.7.5), and by Elkik’s algebrization (4.6.7.9), this is a derived \( p \)-completion of some étalemap \( B \to T_0 \), and we can lift it to some étalemap \( B \to S_0 \) by Henselian pair property (4.6.6.12)(4.3.10.9), then we can also take the derived \((p, I)\)-completion (discrete by (6.7.1.11)) \( S_B \) of \( S_0 \), then \( S_B/IS_B \cong B/IB \widehat{\otimes} L R S \). So we have the following base change diagram:

\[
\begin{array}{ccc}
B & \longrightarrow & S_0 \\
\downarrow & & \downarrow \\
B/IB & \longrightarrow & T_0 \\
& & \downarrow \\
& B/IB \widehat{\otimes} L S & \longrightarrow & B/IB \widehat{\otimes} L S
\end{array}
\]

For the adjointness, it suffices for every prism \((T, IT)\) with morphisms \( B \to T, B/IB \widehat{\otimes} L S \to T/IT \), we can lift to a map \( S_B \to T \). But if we consider the \( p \)-completely étalemap \( T \to T \widehat{\otimes} B S \) and its base change, it suffices to find a section of this map, and this is by Henselian pair \((T, IT)(4.3.10.6)(6.7.1.11)(4.3.10.9)\). Moreover, \( S_B \) has a \( \delta \)-structure by (4.5.4.19) so it is clearly a prism, and the right adjoint \( F \) just takes \((T, IT) \to (S_B, IS_B)\).

This right adjoint preserves weakly final objects and products, and it is just the completed derived tensor \( - \widehat{\otimes} L S \) when modulo \( I \) by construction, so when combined with (4.6.7.8) we get the conclusion.

**Remark (6.7.6.3).** Notice these two lemmas (6.7.6.1)(6.7.6.2) are consequences of Hodge-Tate comparison isomorphism, once we proved it!

**Crystalline Comparison in Characteristic \( p \)**

**Prop. (6.7.6.4)[Crystalline Comparison in Characteristic \( p \)]** Let \((A, (p))\) be a crystalline prism and let \( I \subset A \) be a pd-ideal with \( p \in I \), in particular the Frobenius \( A/p \to A/p \) factors through \( A/I \) by (4.7.0.3), inducing a map \( \psi = \psi_I : A/I \to A/p \). Let \( R \) be a smooth \( A/I \)-algebra and let \( R^{(1)} = R \otimes_{A/I, \psi} A/p \), then there is a canonical

\[
\Delta_{R^{(1)}/A} \cong R \Gamma_{\text{crys}}(R/A)
\]

of \( E_{\infty} \)-\( A \)-algebras compatible with Frobenius action.

**Proof:** ?
Cor. (6.7.6.5). If we have a smooth $R$ over $A/p$ and let $\tilde{R} = R \otimes_{A/p} A/I$, then $\tilde{R}^{(1)} = \varphi_* R$, and we can apply this theorem to $\tilde{R}$ to get a canonical isomorphism

$$\varphi^* \Delta_{R/A} \cong R^{\text{crys}}(\tilde{R}/A)$$

of $E_\infty$-$A$-algebras compatible with Frobenius action.

Lemma (6.7.6.6) [Hodge-Tate Comparison for the Affine Line over $(\mathbb{Z}_p, (p))$]. If $(A, (p))$ is a $p$-torsionfree crystalline prism and $R = F_p(X)$, then the Hodge-Tate map constructed in (6.7.5.3) is an isomorphism.

**Proof:** WARNING: This proof will not use the construction of the Hodge-Tate map in degree $>1$ and this lemma will be used in the proof of Hodge-Tate map in the general case, so there is no cycle in the reasoning.

The map

$$\Omega^\bullet_{R^{(1)}}(A/p) \rightarrow H^*(R^{\text{crys}}(R/A) \otimes^L_A A/p) \{*\} \cong H^*(\Delta_{R^{(1)}}/A \otimes^L_A A/I) \{*\} = H^*(\Delta_{R^{(1)}}/A) \{*\}$$

is an isomorphism by Cartier isomorphism $\mathfrak{?}$, where the middle is by prismatic-crystalline comparison (6.7.6.4).

It suffices to check that this is the Hodge-Tate map for $R^{(1)}(A/p)$. But the Hodge-Tate map is induced by the inclusion $O_X \rightarrow H^0(T_X/S)$. It is fairly easy to check the proof of (6.7.6.4) and (6.6.4.9) the composition is also the canonical one. Finally if we choose $F_p(X) = R = R^{(1)}$, then we get the desired Hodge-Tate isomorphism. □

Lemma (6.7.6.7) [Hodge-Tate Comparison for $(\mathbb{Z}_p, (p))$]. If $(A, (p))$ is a $p$-torsionfree crystalline prism and $R = F_p[X_1, \ldots, X_n]$, then the Hodge-Tate map constructed in (6.7.5.3) is an isomorphism.

**Proof:** The proof is the same as that of (6.7.6.6), notice now we already have the Hodge-Tate Comparison map. □

**Direct proof of the Hodge-Tate comparison for $(\mathbb{Z}_p, (p))$**

The proof of (6.7.6.6) and (6.7.6.7) is sloppy because we somehow lose track of whether the composition morphism is the Hodge-Tate comparison map. As the situation is so explicit, we decided to give a direct proof.

**Mix Characteristic Case**

Prop. (6.7.6.8) [Comparing with the Characteristic $p$]. Let $A$ be a universal oriented prism in any characteristic and $A \rightarrow B$ as in (6.7.1.5), let $\alpha : (A, (d)) \xrightarrow{\sim} (A, (d)) \rightarrow (B, (p))$, then $\alpha$ is a map of prisms by (6.7.1.6), and:

1. $\alpha/p$ factors as $A/p \rightarrow A/(p, d) \rightarrow A/(p, d^p) \rightarrow B/p = D_{A/p}(d)$ where the first map has finite Tor amplitude and the last two maps are f.f., thus $\alpha/p$ has finite Tor amplitude.

2. The functor $\hat{\alpha}^* : D_{\text{comp}}(A, (p, d)) \rightarrow D_{\text{comp}}(B, (p))$ reflects isomorphisms.

3. For any $p$-completely smooth $A/I$-algebra $R$, let $R_B = R \hat{\otimes} A B$, then the map

$$ \hat{\alpha}^* \Delta_{R/A} \rightarrow \Delta_{R_B/B} $$

is an isomorphism.
Proof: 1: It factors because \( d^p = p! \gamma_p(d) \in pB \), and \( B/p = D_{A/p}((d)) \) by (4.7.0.16), noticing \( D_A((d)) = D_A((p,d)) \). The first map is of finite Tor amplitude (4.6.7.1) because \( d \) is a nonzero divisor in \( A/p \) by (6.7.1.4). \( \varphi \) is f.f. because it is a base change of \( \varphi_{A/p} \) and the latter is f.f. (6.7.1.4). The last one is f.f. because it is a free summand as \( D_{A/p}((d)) = A/p[X_1, X_2, \ldots]/(a^p, X_1^p, X_2^p, \ldots) \) by (4.7.0.20).

2: Because \( D_{\text{comp}}(A, I) \) is a weak Serre subcategory of \( D(A) \) (4.6.6.8), to show it reflects isomorphisms, by item1 and derived Nakayama applied to \( - \otimes^L_B B/p \), it suffices to show if \( X \in D_{\text{comp}}(A, (p,d)) \), if \( X \otimes^L_A A/p \otimes^L_{A/p} A/(p,d) = 0 \), then \( X = 0 \), but \( X \otimes^L_A A/p \otimes^L_{A/p} A/(p,d) = X \otimes^L_A A/(p,d) \), and this follows from derived Nakayama again.

3: \( \alpha \) has finite \((p,d)\) Tor amplitude by (4.6.7.3) and (6.7.1.4), so 3 follows from (6.7.6.1).

**Final Proof**

Prop. (6.7.6.9) [Hodge-Tate Comparison in the Affine Line Case]. In situation (6.7.4.8), If \( R = A/I(X) \), \( \eta^0_R : R \to H^0(\overline{\mathbb{F}}_{R/A}) \) and the twisted morphisms \( \eta^1_R \{ -1 \} : \Omega^1_{R/(A/I)}(\{ -1 \}) \to H^1(\overline{\mathbb{F}}_{R/A}) \) defined by the universal property of \( \Omega_{R/(A/I)} \) are isomorphisms, and \( H^i(\overline{\mathbb{F}}_{R/A}) = 0 \) for \( i > 1 \).

In particular, by étale localization of prismatic cohomology (6.7.6.2), lemma (6.7.5.4) holds for any \( p \)-completely smooth algebra \( R \) over \( A/I \). But this doesn’t say that higher cohomologies vanish for any \( R \), this is because cup product can survive derived tensor but cohomology groups cannot.

Proof: In this case, \( \Omega_{R/S} \) is topologically free over \( R \), thus we can choose a map

\[
\eta : R \oplus \Omega^1_{R/A}(-1)[-1] \to \overline{\mathbb{F}}_{R/A}
\]

lifting \( \eta^0_R \oplus \eta^1_R \{ -1 \} \).

Firstly if \( (A, I) = (\mathbb{Z}_p, (p)) \), this case is done by (6.7.6.6).

Next, if \( (A, (d)) \) is oriented, then there is a map of prisms from the universal oriented prism (6.7.1.4) \( A_0 \to A \), then we have a pushout diagram of simplicial commutative rings

\[
\begin{array}{ccc}
A_0 & \longrightarrow & A \\
\downarrow^\alpha & & \downarrow^\beta \\
\mathbb{Z}_p & \longrightarrow & D_0 \longrightarrow E = A \widehat{\otimes}_{A_0} D_0
\end{array}
\]

and \((E, (p))\) is a simplicial prism.

Now the warning is what we have done so far can all be extended to the derived algebraic geometry setting, or at least to the "animated commutative algebra" setting!

We denote the composite of the lower row as \( \gamma \), because \( \widehat{\gamma}^* \) reflects isomorphisms, so does \( \widehat{\beta}^* \), and we can show \( \widehat{\beta}^* \overline{\mathbb{F}}_{R/A} \cong \widehat{\gamma}^* \overline{\mathbb{F}}_{F_p(X)/\mathbb{Z}_p} \), and identifies the Hodge-Tate map: This is because we are in the polynomial case, so we can make the construction of \( \Delta_{R/A} \) clear: we just take the \( F^0 \) to be the derived \((p, I)\)-completion of the free \( \delta\)-rings \( A\{X\} \) in the construction of weakly final object (6.7.4.11), then the resulting Čech-Alexander complex is free and compatible with base change in the complex level.

Also \( \beta \) has finite \((p,d)\)-Tor amplitude because \( \alpha \) has because \((p,d)\) is regular in \( A_0 \) (6.7.1.4), also \( \gamma \) has finite \( p \)-Tor amplitude because \( E \) is \( p \)-torsionfree by (6.7.1.11), and use (4.6.7.3). So we are reduced to the \((\mathbb{Z}_p, (p))\) case, which we have done.

Finally, for a general bounded prism \((A, I)\), we can reduce to the oriented case by base change along the f.f. extension defined in (6.7.1.11), then we reduce to the orientable case by (6.7.6.1).
Prop. (6.7.6.10) [Hodge-Tate Comparison Theorem in General]. The map
\[ \eta^\bullet_R : \Omega^\bullet_{X/(A/I)} \to H^\bullet(\overline{\Delta}_{X/A}); \{ \bullet \} \]
constructed in (6.7.5.3) is an isomorphism of sheaves of \( A/I \)-dgas on \( X_{\acute{e}t} \).

Proof: Because we already have the Hodge-Tate comparison map, it suffices to prove the theorem for affine subscheme \( \text{Spf} \ R \), and because both prismatic cohomology and de Rham complex are étale-local (6.7.6.2) (6.7.5.2), it suffices to prove for the polynomial case. In this case, \( \hat{\Omega}_A^i \) is topological free over \( R \), then we can lift the Hodge-Tate map (6.7.5.3) to the level of chain complexes:
\[ \eta : \bigotimes_{i=0}^n \Omega^i_{R/(A/I)} \{-i\} \{-i\} \to \overline{\Delta}_{R/A}. \]
And then the rest is the same as the proof of (6.7.6.9), where in the \((\mathbb{Z}_p, (p))\) case, we use (6.7.6.7) instead of (6.7.6.6). \( \Box \)

**de Rham Comparisons**

Prop. (6.7.6.11) [de Rham Comparison]. In situation (6.7.4.2), if \( W(A/I) \) is \( p \)-torsionfree, then there is a natural isomorphism
\[ \overline{\Delta}_{X/A} \otimes_{A, \varphi} A/I \cong \Omega^\bullet_{X/(A/I)} \]
of commutative algebra objects in \( D(A/I) \).

Proof: Cf. [Sholze, Prism, 6.4]. It suffices to construct locally a functorial isomorphism \( \hat{\Delta}_{R/A} \otimes_{A, \varphi} A/I \cong \Omega^\bullet_{R/(A/I)} \) and then glue.

Let \( A \to W(A/I) \) be the canonical map, and \( \psi : A \to W(A/I) \), then it takes \( I \) into \((p)\). But the map \( \psi/p : A/I \to W(A/I)/p = A/I \) factors through \( A/(p, I) \), thus \( R' \) also equals \( R/p \otimes_{A/(p, I)} W(A/I)/p \), so there is a base change diagram:
\[
\begin{array}{ccc}
R & \longrightarrow & R/p \\
\uparrow & & \uparrow \\
A/I & \longrightarrow & A/(p, I)
\end{array}
\]
\[
\begin{array}{ccc}
& & \psi_{(p, [p])} \\
& & \uparrow \\
& & W(A/I)/p = A/I
\end{array}
\]

Base change for prismatic cohomology (6.7.5.5) gives an isomorphism
\[ \hat{\Delta}_{R/A} \otimes_{A, \varphi} W(A/I) \cong \hat{\Delta}_{R'/W(A/I)}. \]

Note that \( W(A/I) \to A/(p, I) \) is a pd-thickening with ideal \((p, [p])\), so we can use crystalline comparison w.r.t. the crystalline prism \((W(A/I), (p))\) to show that
\[ \hat{\Delta}_{R/(1)/W(A/I)} \cong R\Gamma_{\text{crys}}((R/p)/W(A/I)). \]

Then finally we use the crystalline de Rham comparison to get the desired result. \( \Box \)

**Remark (6.7.6.12).** The technical condition \( W(A/I) \) is \( p \)-torsionfree can be removed, by [Sholze, Prism, 15.4].
7 Derived de Rham Cohomology

Def. (6.7.7.1) [Derived de Rham Cohomology]. For an \( \mathbb{F}_p \)-algebra \( k \), the derived de Rham cohomology functor \( dR_{-/k} : \mathcal{C}Alg / k \to D(k) \) is the left derived functor of the functor \( \text{Poly}_k \to D(k) \) given by \( R \to \Omega^\bullet_{R/k} \) via (8.1.4.1).

Prop. (6.7.7.2) [Derived Cartier Isomorphism].

Regular Semiperfect Rings

Def. (6.7.7.3) [Regular Semiperfect Rings]. Let \( k \) be a perfect ring, a regular semiperfect ring over \( k \) is an \( k \)-algebra of the form \( R/I \) where \( R \) is a perfect \( k \)-algebra and \( I \) is an ideal generated by a regular sequence.

Prop. (6.7.7.4). Let \( k \) be a perfect field and \( S \) be a regular semiperfect ring, then

8 Derived Prismatic Cohomology

Prop. (6.7.8.1) [Derived Hodge-Tate Comparison].

9 \( q \)-de Rham Cohomology

Prop. (6.7.9.1) [Hodge-Tate isomorphism via \( q \)-de Rham Complex]. Cf. [Bhatt, Prism, 5.3.9].

10 \( \acute{E} \)tale Comparison

Prop. (6.7.10.1) [Frobenius Fixed Points]. Fix an \( \mathbb{F}_p \)-algebra \( B \) with an element \( t \), let \( D(B[F]) \) be the derived category of Frobenius \( B \)-modules: this is a category whose objects are \( (M, \phi) \) where \( M \in D(B) \) and \( \phi \) is a morphism \( M \to M \otimes_B \phi \). And let \( D_{\text{comp}}(B[F]) \) be the full subcategory spanned by pairs \( (M, \phi) \) where \( M \in D_{\text{comp}}(B, t) \).

Given \( (M, \phi) \in D_{\text{comp}}(B[F]) \), let \( M_{\phi=1} = R \text{Hom}_{D(B[F])}((B, \phi), (M, \phi)) \in D(F_p) \), called the Frobenius fixed pts of \( M \).

Prop. (6.7.10.2). Fix an \( \mathbb{F}_p \)-algebra \( B \) with an element \( t \), then

- The functor \( D_{\text{comp}}(B[F]) \to D(F_p) \) given by \( M \to M_{\phi=1} \) and \( M \mapsto (M[t^{-1}])_{\phi=1} \) commute with colimits.
- For any \( (M, \phi) \in D_{\text{comp}}(B[F]) \) and

11 Almost Purity
6.8 Motives

Main references are [Sta][Chap45], [Ful98], [Kle94] and [Mil12].

1 Weil Cohomology Theories

**Def. (6.8.1.1)** Let $k \in \text{Field}$, the full subcategory of $\text{Sch}/k$ consisting of smooth projective schemes over $k$ is denoted by $\text{SmProj}/k$.

Any $X \in \text{SmProj}/k$ has a decomposition $X = \bigsqcup_n X_n$ into clopen subschemes that $X_n$ is equidimensional of dimension $n$ by (6.1.2.28). Thus we can talk about Rings $\text{CH}^*(X)$ and $\text{GH}^*(X)$ (6.1.2.29).

**Def. (6.8.1.2)** [Correspondences]. Let $k \in \text{Field}$ and $X,Y \in \text{SmProj}/k$ the group of correspondences from $X$ to $Y$ of degree $r \in \mathbb{Z}$ is defined to be

$$\text{Corr}_{\text{rat}}^r(X,Y) = \bigoplus_d \text{CH}^{d+r}(X_d \times_k Y)_Q \subset \text{CH}^r(X \times Y)_Q.$$ 

Similarly we can define Grothendieck correspondences $\text{Corr}_{\text{num}}^r(X,Y)$.

**Def. (6.8.1.3)** [Compositions of Correspondences]. Let $X,Y,Z \in \text{SmProj}/k$, there is a composition of correspondences map

$$\text{Corr}^r(Y,Z) \times \text{Corr}^s(X,Y) \to \text{Corr}^{r+s}(X,Z) : (c',c) \mapsto c' \circ c = \text{pr}_{13*}(\text{pr}_{23}^* c' \cdot \text{pr}_{12}^* c').$$

Then composition of correspondences are $\mathbb{Q}$-linear and associative.

**Proof**: Cf. [Sta][FG0].

**Prop. (6.8.1.4)** [Tensor Product of Correspondences]. Let $X,Y,X',Y' \in \text{SmProj}/k$, there is a tensor product of correspondences map

$$\otimes : \text{Corr}^r(X,Y) \times \text{Corr}^s(X',Y') \to \text{Corr}^{r+s}(X \times_k X', Y \times_k Y') : (c,c') \mapsto \text{pr}_{13*}(c \cdot \text{pr}_{24}^* c').$$

which is $\mathbb{Q}$-linear and associative, and commutes with compositions in both coordinates.

**Prop. (6.8.1.5)**. $\text{Corr}^0(\mathbb{P}_k^1) = \text{CH}^1(\mathbb{P}_k^1 \times \mathbb{P}_k^1)_Q \cong \mathbb{Q} \oplus \mathbb{Q}$, where a basis is given by $c_0 = \{0\} \times \mathbb{P}_k^1$ and $c_2 = [\mathbb{P}_k^1 \times \{0\}]$. And the diagonal $\Delta = c_0 + c_2$.

Also $c_0 \circ c_0 = c_0, c_2 \circ c_2 = c_2, c_0 \circ c_2 = 0 = c_2 \circ c_0$, so $\text{Corr}^0(\mathbb{P}_k^1) \cong \mathbb{Q} \oplus \mathbb{Q}$ as a $\mathbb{Q}$-algebra.

**Def. (6.8.1.6)** [Push and Pull via Correspondences]. Let $c \in \text{Corr}_{\text{rat}}^r(X,Y)$, we can define the

- (Pullback): $\text{CH}_k(Y) \to \text{CH}_{k-r}(X) : \beta \mapsto c^*(\beta) = \text{pr}_{1*}(c \cdot \text{pr}_{2*}^* \beta)$.
- (Pushforward): $\text{CH}^k(X) \to \text{CH}^{k+r}(Y) : \alpha \mapsto c_*(\alpha) = \text{pr}_{2*}(c \cdot \text{pr}_{1*}^* \alpha)$.

by using stratification and (6.1.2.12)(6.1.2.9).

**Prop. (6.8.1.7)** [Correspondences and Chow Groups].

- There are canonical isomorphisms

  $$\text{CH}_{-r}(X)_Q \cong \text{Corr}_{\text{rat}}^r(X, \text{Spec} k)$$

  s.t. pullbacks by correspondences correspond to compositions.
• There are canonical isomorphisms

\[ \text{CH}^r(X)_\mathbb{Q} \cong \text{Corr}^r_{\text{rat}}(\text{Spec } k, X) \]

s.t. pushforwards by correspondences correspond to compositions.

**Proof:** Cf. [Sta]0FG0.

**Cor. (6.8.1.8).** Pushforwards and pullbacks by correspondences commute with compositions, by (6.8.1.7) and (6.8.1.3).

**Prop. (6.8.1.9) [Graphs].** Let \( f : X \to Y \in \text{SmProj} / k \), its transposed graph \( \Gamma^t_f \) defines a correspondence \( [\Gamma^t_f] \in \text{Corr}^0(Y, X) \). \( [\Gamma_{\text{id}_X}] \in \text{Corr}^0(X, X) \) is denoted by \( [\Delta_X] \).

**Def. (6.8.1.10) [Transpose].** Let \( X, Y \in \text{SmProj} / k \) be equidimensional, then the isomorphism \( X \times_k Y \cong Y \times_k X \) induces a transpose isomorphism

\[ (-)^t : \text{Corr}^r(X, Y) \to \text{Corr}^{\dim X-\dim Y+r}(Y, X). \]

In particular, when \( f : X \to Y \in \text{SmProj} / k \) and \( X, Y \) are equidimensional, then \( [\Gamma^t_f]^t = [\Gamma_f] \).

**Prop. (6.8.1.11).** Let \( \alpha \in \text{Corr}^*(X, Y), \beta \in \text{Corr}^*(Y, Z) \), then

1. \( (\beta \circ \alpha)^t = \alpha^t \circ \beta^t \).
2. If \( \beta = [\Gamma^t_g] \), then \( \beta \circ \alpha = (\text{id}_Y \times g)^t \alpha \).
3. If \( \alpha = [\Gamma^t_f] \), then \( \beta \circ \alpha = (f \times \text{id}_Z)_* \beta \).
4. If \( \alpha = [\Gamma^t_f], \beta = [\Gamma^t_g] \), then \( \beta \circ \alpha = [\Gamma^t_{fg}] \).
5. \( \Delta_Y \circ \alpha = \alpha, \quad \beta \circ \Delta_Y = \beta \).

**Proof:**

1: This follows from commutativity and naturality of intersection products.

2: By (6.1.4.6) and (6.1.8.9),

\[ [\Gamma^t_f] \circ \alpha = \text{pr}_{13}\times \text{pr}^*_2 [\Gamma^t_g] \cdot \text{pr}^*_1 \alpha = \text{pr}_{13}((1, g, 1)_*(1, g, 1)^t \text{pr}^*_1 \alpha) = (1, g)^t \alpha. \]

3 is similar to item 2.

4, 5 follow from item 2, 3.

**Prop. (6.8.1.12) [Push and Pull by Graphs].** Let \( f : X \to Y \in \text{SmProj} / k \), then

- Pushforward by \( [\Gamma_f]^t \) agrees with the Gysin map \( f^t : \text{CH}^r(Y) \to \text{CH}^r(X) \).
- Pullback by \( [\Gamma_f]^t \) agrees with the pushforward \( f_* : \text{CH}_*(X) \to \text{CH}_*(Y) \).

**Proof:** These follows from (6.8.1.7) and (6.8.1.11).

**Prop. (6.8.1.13).** Let \( f : Y \to X \in \text{SmProj} / k \) where \( X, Y \) are equidimensional, then there are commutative diagram of correspondences

\[
\begin{align*}
X \times Y & \xrightarrow{[\Gamma^t_f] \circ \Delta_Y} Y \times Y \xrightarrow{[\Gamma^t_{\Delta_Y}]} Y \\
& \downarrow \Delta_X \circ [\Gamma_f] \quad \quad \quad \quad \downarrow [\Delta_X] \circ [\Gamma_f] \\
X \times X & \xrightarrow{[\Gamma^t_{\Delta_X}]} X \xrightarrow{[\Delta_X]} \text{Spec } k
\end{align*}
\]
Prop. (6.8.1.11). It suffices to show that \((\text{id}_X 	imes f)^*(\Delta_X)_*[X] = (f 	imes \text{id}_Y)_*(\Delta_Y)_*[Y]\). But both sides equal \([\Gamma_f^1]\). \((\text{id}_X 	imes f)^1[\Delta_X] = [\Gamma_f^1]\) follows from [Sta]0F7?.

\[\square\]

**Prop. (6.8.1.14) [Virtual Number of Coincidences].** Let \(X,Y \in \text{SmProj} / k, \alpha, \beta \in \text{Corr}^*(X,Y)\), then

\[
\text{pr}_1(\alpha \cdot \beta) = (\beta^t \circ \alpha) \cdot \Delta_X = (\alpha^t \circ \beta) \cdot \Delta_X.
\]

In particular, if \(X,Y\) are equidimensional of dimension \(n\), and \(\alpha, \beta \in \text{Corr}^0(X,Y)\), then the virtual number of coincidence of \(\alpha\) and \(\beta\), defined as \(\int_{X \times Y} \alpha \cdot \beta\), equals the virtual number of fixed points of \(\beta^t \circ \alpha\).

**Proof:** Cf.[Ful98]P309.

\[\square\]

**Def. (6.8.1.15) [Degenerate Correspondences].** Let \(X,Y \in \text{SmProj} / k\), then the subgroup of degenerate correspondences from \(X\) to \(Y\) is the subgroup of \(\text{Corr}^*(X,Y)\) generated by exterior products \(\text{CH}^*(X) \times \text{CH}^*(Y)\). The subgroup of degenerate correspondences from \(X\) to \(Y\) is denoted by \(I(X,Y)\).

Then \(I(X,X)\) is a two-sided ideal in \(\text{Corr}^*(X,X)\), and is stable under transpose if \(X\) are equidimensional.

**Def. (6.8.1.16) [Valence].** Let \(X \in \text{SmProj}^n / k\), then \(\alpha \in \text{Corr}^0(X,X)\) is said to be of valence \(\nu\) iff \(\alpha + \nu[\Delta_X] \in I(X,X)\).

**Def. (6.8.1.17) [Degree of Correspondences].** Let \(X,Y,Z \in \text{SmProj}^n / k\) be irreducible, then for \(\alpha \in \text{Corr}^n(X,Y)\), the degrees of \(\alpha\) is defined to

\[
\alpha_*[X] = \text{pr}_{2*}(\alpha) = d_2(\alpha)[Y], \quad \alpha^*[Y] = \text{pr}_{1*}(\alpha) = d_1(\alpha)[X].
\]

Then

- Let \(\beta \in \text{Corr}^n(Y,Z)\), then \(d_i(\beta \circ \alpha) = d_i(\alpha)d_i(\beta)\).
- If \(P \subset X\) is a rational point, then \(d_1(\alpha) = \int_{X \times Y} \alpha \cdot [P \times Y]\).

**Proof:** 1 is clear. 2 follows by composing with the correspondence \([\Gamma_P] \in \text{Corr}^{-n}(P,X)\).

\[\square\]

**Pre-Weil Cohomology Theories**

**Prop. (6.8.1.18) [Non-Existence of a Q-Cohomology Theory].** For any \(p \in \mathbf{P} \cup \{0\}\), there exists an alg.closed field of characteristic \(p\) s.t. there doesn’t exist a cohomology theory on the category of smooth projective varieties over \(k\) with coefficients in \(\mathbb{Q}\) that specializes to the étale cohomology with \(\mathbb{Q}_\ell\) coefficients, where \(\ell \in \mathbf{P} \cap \{p\}\).

**Proof:** For \(p = 0\), take \(k = \mathbb{C}\). For a smooth projective variety \(X\) over \(k\), it is defined over a subfield \(k_0\) finite over \(\mathbb{Q}\). Let \(\Gamma = \text{Gal}(k/k_0)\), then \(\Gamma\) acts on \(H^*(X,\mathbb{Q}_\ell)\). If \(H^*(X,\mathbb{Q}_\ell)\) is specialized from a Q-cohomology \(\widetilde{H}^*(-,\mathbb{Q})\), then the continuous \(\Gamma\)-action on \(H^*_\text{ét}(X,\mathbb{Q}_\ell)\) stabilizes \(\widetilde{H}^*(X,\mathbb{Q})\). But it is known that

\[
H^*_\text{ét}(X,\mathbb{Q}_\ell) \cong H^*_{\text{Betti}}(X,\mathbb{Q}) \oplus \mathbb{Q}_\ell,
\]

so \(\dim_{\mathbb{Q}} \widetilde{H}^*(X,\mathbb{Q}) = \dim H^*_{\text{Betti}}(X,\mathbb{Q}) < \infty\). Then because infinite Galois group is uncountable, \(\Gamma\) acts \(\widetilde{H}^*(X,\mathbb{Q})\) through a finite quotient. But this is not true in general.\(\square\) In fact, This contradicts Tate’s conjecture.
If $p > 0$, let $k = \overline{F}_p$ and $E$ be an supersingular elliptic curve over $k$, which exists by (13.8.3.10), then $\text{End}(E) \otimes \mathbb{Q}$ is a definite quaternion algebra $Q$ over $\mathbb{Q}$, and $\dim_{\mathbb{Q}} H^1_{\acute{e}t}(E, \mathbb{Q}_x) = 2(13.5.6.15)$, so if $H^*(X, \mathbb{Q}_x)$ is specialized from a $\mathbb{Q}$-cohomology $\widetilde{H}^*(-, \mathbb{Q})$, $\dim_{\mathbb{Q}} \widetilde{H}^1(E, \mathbb{Q}) = 2$, and $\text{End}(E) \otimes \mathbb{Q}$ acts on it. But there is no ring homomorphism $\mathbb{Q} \rightarrow M_2(\mathbb{Q})$. □

**Def. (6.8.1.19) [Weil Cohomology Theories].** Let $k, F \in \text{Field}$, char $F = 0$, then a pre-Weil cohomology theory over $k$ with coefficients in $F$ is given by a tuple $(F(1), H^*, \gamma, \text{tr})$, where

1. $F(1)$ is a 1-dimensional vector space over $F$. And denote $F(n) = F(1)^{\otimes n}$, $F(-n) = (F(n))^*$, and for any $V \in \text{Vect}_F$, define $V(n) = V \otimes F(n)$.
2. $H^*$ is a functor $H^* : \text{SmProj}/k \rightarrow \mathcal{C}^{\text{Ringgr}}/F$. $H^*(X)$ is called the cohomology ring of $X$, and its multiplication is denoted by $\cup$.
3. For every $X \in \text{SmProj}/k$ and $i \in \mathbb{N}$, $\gamma_X$ is a homomorphism $\gamma_X : CH^i(X) \rightarrow H^{2i}(X)(i)$, called the cycle class maps of $X$.
4. For any $X \in \text{SmProj}^d/k$, $\text{tr}_X$ is a map $\text{tr}_X : H^{2d}(X)(d) \rightarrow F$, called the trace map of $X$.

The trace map is sometimes also denoted by $\int_X$.

that satisfy the following properties:

**Poincaré duality:** For any $X \in \text{SmProj}^d/k$,

1. $\dim_F H^i(X) < \infty$ for any $i$ and $H^i(X) = 0$ unless $0 \leq i \leq 2n$.
2. $H^i(X) \times H^{2d-i}(X)(d) \xrightarrow{\cup} H^{2d}(X)(d) \xrightarrow{\text{tr}_X} F$ is a perfect pairing.

**Künneth formula:** For any $X, Y \in \text{SmProj}/k$,

$$H^*(X) \otimes_F H^*(Y) \rightarrow H^*(X \times_k Y) : (a, b) \mapsto \text{pr}_1^* a \cup \text{pr}_2^* b$$

is an isomorphism in $\mathcal{C}^{\text{Ringgr}}/F$.

**Cycle class map is natural:**

1. For any $f : X \rightarrow Y \in \text{SmProj}/k$, $\gamma(f^! \beta) = f^* \gamma(\beta)$ for $\beta \in H^*(Y)$ and $\gamma(f_* \alpha) = f_* \gamma(\alpha)$ for $\alpha \in H^*(X)$.
2. $\gamma(a \cdot b) = \gamma(a) \cup \gamma(b)$.
3. $\int_{\text{Spec } k} \gamma(\text{Spec } k) = 1$.

$H^*$ is called a Weil cohomology theory if moreover it satisfies:

- For $X \in \text{SmProj}/k$ and $\Gamma(X, \mathcal{O}_X) = k'$, then the natural map $H^0(\text{Spec } k') \rightarrow H^0(X)$ is an isomorphism.

**Prop. (6.8.1.20) [Pushforward].** Let $k, F \in \text{Field}$ and $H^*$ be a pre-Weil cohomology theory, for $f : X \rightarrow Y \in \text{SmProj}/k$ where $\dim X = d, \dim Y = e$, we can define a pushforward map of cohomology $H^{2d-*}(X)(d) \rightarrow H^{2e-*}(Y)(e)$ via Poincaré duality, i.e.

$$\int_X f^* b \cup a = \int_Y b \cup f_* a$$

for any $a \in H^{2d-i}(X)(d), b \in H^i(Y)$. Then

- $f_*(f^* b \cup a) = b \cup f_* a$.
- $g_* f_* = (gf)_*$.

**Proof:** Use duality and the corresponding properties of $f^*$. □
Prop. (6.8.1.21) \([H^*(\text{Spec } k)]\). Let \(k, F \in \text{Field} \) and \(H^*\) be a pre-Weil cohomology, then \(H^i(\text{Spec } k) = 0\) unless \(i = 0\), and there is a unique \(F\)-algebra isomorphism \(H^0(\text{Spec } k) \cong F\), sending \(\gamma([\text{Spec } k])\) to 1 and \(\text{tr}_{\text{Spec } k}\) is identity under this identification.

**Proof:** Cf. [Sta]0FHE.

Prop. (6.8.1.22) \([\text{Coproducts}]\). Let \(k, F \in \text{Field} \) and \(H^*\) be a pre-Weil cohomology, then for \(X, Y \in \text{SmProj} /k\), \(H^*(X \coprod Y) \to H^*(X) \times H^*(Y)\) is an isomorphism.

**Proof:** Cf. [Sta]0FHJ.

**Weil Cohomology Theories**

Prop. (6.8.1.23) \([\text{Characterizing Weil Cohomology Theories}]\). Let \(k, F \in \text{Field} \) and \(H^*\) be a pre-Weil cohomology theory, for \(X \in \text{SmProj} / k\) and \(\Gamma(X, O_X) = k'\), the following are equivalent:

- There exists f.m. geometric points \(x_1, \ldots, x_r \in X\) s.t. \(H^0(X) \to H^0(x_1) \oplus \ldots H^0(x_r)\) is injective.
- The map \(H^0(\text{Spec } k') \to H^0(X)\) is an isomorphism.

If these hold, then \(H^0(X)\) is finite étale over \(F\). Moreover, if \(X\) is equidimensional of dimension \(d\), then these are further equivalent to

- The classes of closed points of \(X\) generate \(H^{2d}(X)(d)\) as a module over \(H^0(X)\).

Prop. (6.8.1.24) \([\text{Non-negativeness}]\). Let \(k, F \in \text{Field} \) and \(H^*\) be a Weil cohomology theory, then for any \(Y \in \text{SmProj} /k\), \(H^i(Y) = 0\) for \(i < 0\).

**Proof:** If \(H^i(Y) \neq 0\) for some \(Y \in \text{SmProj} / k\) and \(i < 0\), we may assume \(Y\) is irreducible by (6.8.1.22), and also we may assume \(i = -2j\) is even by changing \(Y\) to \(Y \times Y\) using Künneth formula. Then take \(X = Y \times (\mathbb{P}^1_k)^j\), then Künneth formula shows

\[
H^0(Y) \oplus H^i(Y) \otimes H^2(\mathbb{P}^1_k)^{\otimes j} \subset H^0(X),
\]

so \(H^0(X)\) cannot be isomorphic to \(H^0(\text{Spec } \Gamma(X, O_X)) = H^0(\text{Spec } \Gamma(Y, O_Y)) \cong H^0(Y)\).

Prop. (6.8.1.25). \ (?) Let \(k, F \in \text{Field} \) and \(H^*\) be a Weil cohomology theory, then

- If \(X \in \text{SmProj}^d / k\), then \(\text{tr}_X \circ \gamma = \deg : \text{CH}^d(X) \to F(6.1.2.27).
- If \(X, Y \in \text{SmProj} / k\), then \(\text{tr}_{X \times Y} = \text{tr}_X \otimes \text{tr}_Y\) via Künneth formula (6.8.1.19). In particular, for \(a \in H^{2 \dim X}(X)(\dim X), b \in H^*(\dim Y)\), \(\text{pr}_{2,*}(a \otimes b) = (\int_X a)b \in H^*(Y)\).

**Proof:** 1: This holds for \(X = \text{Spec } k\) by hypothesis, and also for any other \(x \in X(k)\) by pushforward.

2: For any \(x \in X(k), y \in Y(k)\), by item 1, \(\gamma([x \times y]) \in H^{\text{top}}(X \times Y)\) is mapped to 1 in \(F\) via \(\text{tr}_{X \times Y}\), and it equals \(\gamma([x]) \otimes \gamma([y])\) by (6.8.1.19) as \([a \times b] = \text{pr}_1^*(a) \cdot \text{pr}_2^*(b)\). The latter is also mapped to 1 in \(F\) by \(\text{tr}_X \otimes \text{tr}_Y\).

For the last assertion, notice \(\int_Y \text{pr}_{2,*}(a \otimes b) \cup c = \int_{X \times Y} (a \otimes b) \cup (1 \otimes c) = (\int_X a) \int_Y (b \cup c)\) \[\Box\]

Prop. (6.8.1.26). If \(Z \in \text{CH}^*(X)\) satisfies \(mZ\) is algebraically trivial for some \(m \in \mathbb{Z}^*\), then \(\gamma_X(Z) = 0\).

**Proof:** Cf. [Algebraic Cycles and the Weil Conjecture, Kleiman, Prop1.2.1]. \[\Box\]
**Prop. (6.8.1.27) [Trace Formula].** Let $k, F \in \text{Field}$ and $H^*$ be a Weil cohomology theory, then for $X \in \text{SmProj} / k$,

$$
\sum_{i=0}^{2 \dim X} (-1)^i \dim_F H^i(X) = \text{deg}([\Delta_X] : [\Delta_X]) = \text{deg}(c_d(T_X) \cap [X]).
$$

**Proof:** Cf. [Sta]0FH0. \(\square\)

**Conj. (6.8.1.28) [Betti Numbers].** Let $k, F \in \text{Field}, k = \bar{k}$ and $H^*$ be a Weil cohomology theory, it is true that for a smooth projective variety over $k$, the numbers $\beta_i = \dim_F H^i(X)$ are independent of $F$ and the cohomology theory?

**Proof:** \(\square\)

2 Pure Motives

**Conj. (6.8.2.1) [Category of Motives].** Let $k \in \text{Field}$, then there should be a category of motives $M(k)$ s.t.

- $M(k)$ is a Tannakian category over $\mathbb{Q}$.
- There is a functor $h$ from the category of smooth projective varieties over $k$ to $M(k)$.
- Every correspondence $X \to Y$ of degree 0 defines a map $hX \to hY$.
- Every Weil cohomology theory on the category of smooth projective varieties over $k$ factors uniquely through $h$.

**Proof:** \(\square\)

**Def. (6.8.2.2) [Chow Motives].** The category $M_{\text{rat}}(k)$ of Chow motives over $k$ consist of triples $(X, e, m)$ where $X$ is a smooth projective variety over $k$, $e$ is an idempotent in $\text{Corr}_{\text{rat}}^0(X, X)_\mathbb{Q}$ and $m \in \mathbb{Z}$. And morphisms in $M_{\text{rat}}(k)$ are defined to be

$$
\text{Hom}((X, e, m), (Y, f, n)) = f \circ \text{Corr}_{\text{rat}}^{n-m}(X, Y) \circ e.
$$

The category $M_{\text{eff}}(k)$ of effective Chow motives over $k$ is defined to be the full subcategory of $M_{\text{rat}}(k)$ consisting of triples $(X, e, 0)$.

There is a contravariant functor $\text{SmProj} / k \to M_{\text{eff}}(k) : X \mapsto (X, [\Delta_X], 0)$ and $f \mapsto [\Gamma_f^\dagger]$.

**Def. (6.8.2.3) [Grothendieck Motives].** The category $M_{\text{num}}(k)$ of Grothendieck motives over $k$ consist of triples $(X, e, m)$ where $X$ is a smooth projective variety over $k$, $e$ is an idempotent in $\text{Corr}_{\text{num}}^0(X, X)_\mathbb{Q}$ and $m \in \mathbb{Z}$. And morphisms in $M_{\text{num}}(k)$ are defined to be

$$
\text{Hom}((X, e, m), (Y, f, n)) = f \circ \text{Corr}_{\text{num}}^{n-m}(X, Y) \circ e.
$$

The category $M_{\text{eff}}(k)$ of effective Grothendieck motives over $k$ is defined to be the full subcategory of $M_{\text{num}}(k)$ consisting of triples $(X, e, 0)$.

**Prop. (6.8.2.4).** There are natural functors $M_{\text{eff}}(k) \to M_{\text{eff}}(k)$ and $M_{\text{rat}}(k) \to M_{\text{num}}(k)$

**Def. (6.8.2.5) [Twists].** In $M_{\text{rat}}(k)$ or $M_{\text{num}}(k)$, define $1(n) = (\text{Spec } k, 1, n)$, and for any object $M$, define $M(n) = M \otimes 1(n)$. 
Prop. (6.8.2.6). $M_{\text{rat}}(k)$ and $M_{\text{num}}(k)$ are Karoubian categories\(3.3.1.15\) and symmetric monoidal categories with identity $1(0)$\(6.8.2.5\).

Proof: The symmetric monoidal structure is given by\(6.8.1.3\). It is clearly an additive category. To show it is Karoubian, for $M = (X,e,m) \in M_{\text{rat}}(k)$, $p \in \text{End}(M)$ be an idempotent, then $p = epe$, and $N = (X,p,m) \in M_{\text{rat}}(k)$, and $p : N \to M$ is a morphism. \hfill \box

Prop. (6.8.2.7). $h(P_1^k) = 1 \oplus 1(-1) \in M_{\text{rat}}(k)$.

Proof: Cf.\textmd{[Sta]0FGG}. \hfill \box

Prop. (6.8.2.8) \textmd{[M_{\text{rat}}(k) as Inverting $c_2$]} For any $\mathbb{Q}$-Karoubian category $\mathcal{C}$ and a symmetric monoidal functor $f : M_{\text{rat}}^{\text{eff}}(k) \to \mathcal{C}$ s.t. $f(c_2)f(P_1^k)$ is an invertible object, $f$ factors uniquely through a symmetric monoidal functor $M_{\text{rat}}(k) \to \mathcal{C}$.

Proof: Cf.\textmd{[Sta]0FGH}. \hfill \box

Prop. (6.8.2.9) \textmd{[Left Duals]} Let $X \in \text{Sm}_{\text{proj}}/k$ be equidimensional of dimension $d$, then $h(X)(d)$ is a left dual of $h(X)$. In particular, every element in $M_{\text{rat}}(k)$ has a left dual.

Proof: Cf.\textmd{[Sta]0FGI, 0FGJ}. \hfill \box

Def. (6.8.2.10) \textmd{[Chow Groups of Motives]} Let $k \in \text{Field}$ and $M = (X,e,m) \in M_{\text{rat}}(k)$, the $i$-th Chow group of $M$ is defined to be

$$\text{CH}^i(M) = e \circ \text{CH}^{i+m}(X)_\mathbb{Q} = \text{Hom}(1(-i),M).$$

Then each $\text{CH}^i$ defines a functor $M_{\text{rat}}(k) \to \text{Vect}_\mathbb{Q}$ via pushforwards?.

Prop. (6.8.2.11) \textmd{[Manin]} Let $k \in \text{Field}$ and $M \in M_{\text{rat}}(k)$. If $c : M \to N \in M_{\text{rat}}(k)$ satisfies that for $X \in \text{Sm}_{\text{proj}}/k$, the map $c \otimes 1 : M \otimes h(X) \to N \otimes h(X)$ induces isomorphisms on Chow groups, then $c$ is an isomorphism.

Proof: Cf.\textmd{[Sta]0FGN}. \hfill \box

Prop. (6.8.2.12) \textmd{[Weil Cohomologies and Motives]} Let $k,F \in \text{Field}$, $k = \bar{k}$, char $F = 0$, then a classical Weil cohomology over $k$ with coefficients in $F$ is equivalent to a $\mathbb{Q}$-linear monoidal functor $G : M_{\text{rat}}(k) \to \mathcal{C} \text{Ring}^{gr}/F$ together with an isomorphism $F[2] \to G(1(1))$ s.t.

- $G(j(X)) \subset \mathcal{C} \text{Ring}^{gr}_{\geq 0}/F$.
- $\dim F G^0(h(X)) = 1$.

Proof: Cf.\textmd{[Sta]0FH3}. \hfill \box

3 Mixed Motives

Remark (6.8.3.1). The motives are conjectured to be the subcategory of semisimple objects in a larger category of mixed motives.

There is at present no definition of a category of mixed motives, but several mathematicians have constructed triangulated categories that are candidates to be its derived category; it remains to define a $T$-structure on one of these categories whose heart is the category of mixed motives?.
4 Standard Conjectures

Main references are [Kle94].

Prop.(6.8.4.1) [Jannsen]. The endomorphism ring of any \( M \in M_{\text{num}}(k) \) is semisimple.


Conj.(6.8.4.2) [Lefschetz Standard Conjecture]. Let \( k, F \in \text{Field}, k = \bar{k} \) and \( H^* \) be a Weil cohomology theory, \( X \subset \text{SmProj}^d / k \), then the Lefschetz operator \( L : CH^i(X) \to CH^{i+2}(X) \) satisfies for any \( i \leq d \),
\[
L^{n-i} : H^i(X) \to H^{2d-i}(X)
\]
is an isomorphism?. and for \( i \leq d \) we can define
\[
\Lambda = (L^{d-i+2})^{-1} L(L^{d-i}) : H^i \to H^{i-2}, \Lambda = L^{n-i} L(L^{n-i+2})^{-1} : H^{2n-i+2}(X) \to H^{2n-i}(X),
\]
then this \( \Lambda \) is induced from a correspondence from \( X \) to \( X \) of degree \(-1\).

Conj.(6.8.4.3) [Standard Conjecture D]. Let \( k, F \in \text{Field}, k = \bar{k} \) and \( H^* \) be a Weil cohomology theory, then for \( X \in \text{SmProj} / k \), a cycle \( Z \in CH^*(X) \) is numerically trivial iff \( \gamma_X(Z) = 0 \).

Remark(6.8.4.4). This conjecture was shown by Lieberman for varieties of dimension \( \leq 4 \) and for Abelian varieties.

Conj.(6.8.4.5) [Künneth Standard Conjecture]. Let \( k \in \text{Field} \). Assume the conjecture D holds, which implies \( \text{Corr}^r_{\text{num}}(X) \) can acts on \( H^*(X) \) for any Weil cohomology \( H^* \).

Then for any \( X \in \text{SmProj} / k \), there exists a decomposition of \( \Delta_X \in \text{Corr}^\dim X_{\text{num}}(X \times X) \) into orthogonal idempotents
\[
\Delta_X = h^0(X) + \ldots + h^{2\dim X}(X)
\]
s.t. it induces the decomposition
\[
H^*(X) = H^0(X) \oplus H^1(X) \oplus \ldots \oplus H^{2\dim X}(X)
\]
for any Weil cohomology theory \( H^* \).

Remark(6.8.4.6) [Murre]. Murre even conjecture that such a decomposition exists in \( CH^*(X) \) with certain properties, which is equivalent to a filtration on \( CH^*(X) \), conjectured by Beilinson and Bloch.?

Prop.(6.8.4.7) [Hodge Standard Conjecture]. Let \( k, F \in \text{Field}, k = \bar{k} \) and \( H^* \) be a Weil cohomology theory, \( X \subset \text{SmProj}^d / k \), \( P_k(X) = \ker(L|H^k(X)) \) be the primitive cohomologies, \( A^i(X) = \gamma_X(CH^i(X)) \), then for any \( i < d/2 \), the \( \mathbb{Q} \)-valued pairing on \( A^i(X) \cap P^{2i}(X) \):
\[
(x, y) \mapsto (-1)^i(L^{r-2i}x, y)
\]
is positive definite.

Remark(6.8.4.8). This conjecture is true in characteristic 0 by Hodge theory. This conjecture is shown for surfaces by Grothendieck(1958). This conjecture is shown for Abelian varieties of dimension 4 by Ancona(2020).
**Prop.(6.8.4.9).** The conjecture D implies the Lefschetz standard conjecture. The Hodge standard conjecture and the Lefschetz standard conjecture implies conjecture D.

*Proof:* [□]

**Prop.(6.8.4.10) [Hodge Conjecture and Standard Conjecture].** The Hodge conjecture(13.16.4.3) implies the Lefschetz and Künneth standard conjectures and conjecture D for varieties over fields of characteristic 0.

*Proof:* [□]

**Prop.(6.8.4.11).** If the Lefschetz standard conjecture and the Hodge standard conjecture hold, then for any $X \in \text{SmProj}/k$,

- $\text{Corr}^*(X, X)$ is a semisimple $\mathbb{Q}$-algebra.

- (Generalized Riemann Hypothesis) If $k$ is a finite field with Frobenius $\varphi$, then for any Weil cohomology $H^*$, the Frobenius action $\Phi$ on $H^i(X)$ is semisimple with characteristic polynomial in $\mathbb{Z}[T]$, and eigenvalues of absolute value $q^{i/2}$.

*Proof:* Cf.[Kle94]P19. [□]

**Prop.(6.8.4.12) [Tate Conjecture and Standard Conjectures].** The Tate conjecture implies Lefschetz, Künneth standard conjectures and conjecture D for $\ell$-adic étale cohomology over any field.

*Proof:* [□]
7  Algebraic Geometry II: Group Theory

7.1 Group Schemes I: Structure Theory

Main references are [Sta]Chap38, [Mil17].

1 Group Schemes

Def.(7.1.1.1) [Group Scheme]. A monoid scheme over $S$ is a monoid object in the Cartesian monoidal category $\text{Sch}/S$. The category $\text{Grp}_S$ of group schemes over $S$ consists of group objects in the Cartesian category $\text{Sch}/S(3.1.1.61)$.

An open/closed subgroup scheme of a group scheme $G/S$ is an open/closed subscheme of $G/S$ that represents a subgroup functor of $G/S$.

A smooth/flat/separated/... group scheme is a group scheme $G/S$ that $G$ is smooth/flat/separated/... over $S$.

We have the left(right)translation for an elements in $G(R)$, equivalently, a natural transformation on $G$, and base change $(G \otimes_S S')(T'/S') = G(T'/S')$

Remark(7.1.1.2) [Yoneda Interpretation]. We do not need to verify all the relations, whenever we have a functorial commutative group structure on all the set $\text{Hom}(T, G)$, we immediately recover the map $m : G \times G \rightarrow G$ as $\text{pr}_1 \cdot \text{pr}_2 \subset G(G \times G)$, $\text{inv} : G \rightarrow G$ as $\text{inv}$ in $G(G)$, $u : S \rightarrow G$ as $e$ in $G(S)$, by Yoneda lemma.

Cor.(7.1.1.3) [Group Schemes as Functors]. From the Yoneda Interpretation and strong Yoneda lemma(7.7.1.1), a group scheme over $S$ is equivalent to a contravariant functor

$\text{Aff}_S \rightarrow \text{Grp} : R \mapsto \text{Hom}(\text{Spec} R, G)$

(or equivalently a functor $\text{Sch}_S \rightarrow \text{Grp}$) that is represented by a scheme over $S$.

In particular, the category of affine group scheme over $\text{Spec} R$ is equivalent to the category of commutative Hopf algebras over $R(2.9.2.1)$.

Def.(7.1.1.4) [Categorical Group Definitions]. Because we can regard group schemes as functors by(7.1.1.3), we can define categorical constructions of group schemes:

- (Trivial Group Scheme) $S$ is a trivial group scheme over $S$. It is the zero object in $\text{Grp}_S$, denoted by $e$.

- (Commutative Group Schemes) A group scheme $G$ is called a commutative group scheme if each $G(R)$ is commutative.

- ([n]G) For any $n \geq 1$, the natural transformation of commutative groups functors $x \mapsto x^n$ induces a morphism of commutative group schemes $[n] : G \mapsto G$ for any group scheme $G$. 
(Semi-Direct Product) Let $G$ be a group scheme acting on a group scheme $H$, then we can form a semi-direct product group scheme $G times H$ representing the functor $T \mapsto G(T) \rtimes H(T)$. and $G \rtimes H$ is isomorphic to $G \times H$ as schemes.

(Kernel) For a homomorphisms of group schemes $\varphi : G \to H$ over $R$, we define the kernel group scheme $\ker \varphi$ representing the functor $R \mapsto \ker(\varphi(R))$. It is represented by the fibered product

$$
\ker \varphi \to \Spec R \\
\downarrow \quad \quad \downarrow e_H \\
G \xrightarrow{\varphi} H
$$

then it is a group scheme over $R$.

When $G, H$ are affine group schemes, it corresponds to the cokernel Hopf algebra defined in (2.9.2.17).

(Short Exact Sequences) A sequence of homomorphisms of algebraic groups $e \to N \to G \xrightarrow{q} Q$ is called an exact if they are exact as sheaves in $\Sh(\Aff_S)$ (or $\Sh(S\text{ch}_S)$). Exact sequences are stable under base change of fields.

(Quotient Scheme) Let $H \subset G$ be subgroup schemes. If $\tilde{G}/\tilde{H}$ is representable, then it is called the quotient group scheme, denoted by $G/H$.

(Monomorphism) A homomorphism $H \to G$ of group schemes is called a monomorphism if $\tilde{H} \to \tilde{G}$ is injective.

(Quotient Map) A homomorphism $H \to G$ of group schemes is called a quotient map if $\tilde{G} \to \tilde{H}$ is surjective.

(Normal/Characteristic/Central Subgroups) A subgroup scheme $H$ of $G$ is called normal/characteristic/central if $H(R)$ is normal/characteristic/central in $G(R)$ for any $k$-algebra $R$.

(Normalizing) Let $H, N$ be subgroup schemes of $G$, then we say $H$ normalizes $N$ if $H$ is contained in the normalizer of $N$ in $G$.

(Product Subgroup) Let $H, N$ be algebraic subgroups of an algebraic group $G$ such that $H$ normalizes $N$, then we define $NH \subset G$ be the algebraic subgroup that is the image of the homomorphism $N \times H \to G$, if it is representable.

(Generated Subgroup Scheme) Let $\{X_i \to G\}$ be a family of maps to a group scheme $G$, then the smallest algebraic subgroup $H$ of $G$ generated by $\varphi_i$ is called the generated subgroup scheme if it is representable, denoted by $\langle X_i, \varphi_i \rangle$. It is clear such generated subgroup scheme commutes with base change of fields.

(Commutator Subgroup) If $H_1, H_2$ are subgroups of $G$, let $[H_1, H_2]$ be the subgroup generated by the commutators of $H_1, H_2$ if it is representable. Or equivalently, it is the subgroup generated by the map $H_1 \times H_2 \to G : [h_1, h_2] \mapsto h_1 h_2 h_1^{-1} h_2^{-1}$.

(Derived Series) For a group scheme $G$, define $G^{(1)} = [G, G]$ and define inductively $G^{(n+1)} = [G^{(n)}, G^{(n)}]$.

• (Subnormal Series) For a group scheme $G$, a **subnormal series** is a finite sequence of algebraic subgroups $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_r = e$ s.t. $G_{i+1}$ is normal in $G_i$.

• (Solvable Group Schemes) A **solvable group scheme** is a group scheme $G$ that has a subnormal series $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_s = \{e\}$ that each quotient $G_i/G_{i+1}$ is commutative.

• (Nilpotent Group Schemes) A **nilpotent group scheme** is a group scheme $G$ that has a subnormal series $G = G_0 \triangleright G_1 \triangleright \cdots \triangleright G_s = \{e\}$ that each quotient $G_i/G_{i+1}$ is central in $G/G_{i+1}$. Such a sequence is called a **central series**

• (Perfect Group Schemes) A group scheme $G$ is called **perfect** if $G = [G, G]$.

**Lemma (7.1.1.5) [Butterfly Lemma].** Let $H_1, H_2$ be algebraic subgroups of an algebraic group $G$, $N_1, N_2$ are normal subgroups of $H_1$ and $H_2$, then there is a canonical isomorphism of algebraic groups:

$$N_1(H_1 \cap H_2)/N_1(H_1 \cap N_2) \cong N_2(H_2 \cap H_1)/N_2(H_2 \cap N_1).$$

**Proof:** Use the Butterfly lemma for groups *(2.1.9.2)* and shiffy. □

**Def. (7.1.1.6) [Translation Map].** For $G \in Zp/S$ and any $a \in G(S)$, there is a (left)translation map

$$l_a : G \cong S \times S G \xrightarrow{(a, id)} G \times S G \xrightarrow{m} G,$$

and it satisfies $l_a, l_b$ by associativity.

**Prop. (7.1.1.7) [Common Group Schemes].**

- $D(\Gamma) = \text{Spec } \mathbb{Z}[\Gamma]$ for a group $\Gamma$ *(2.9.2.3)*.
- $\mu_n = \mathbb{Z}[T]/(T^n - 1)$(2.9.2.5)
- $G_a = \mathbb{Z}[T]$(2.9.2.6)
- $\Gamma = \text{Spec } \prod_{\gamma \in \Gamma} \mathbb{Z}$(2.9.2.9).
- $\alpha_{pr} = \text{Spec } F_p[X]/XP^r$(2.9.2.15).
- $V_a = \text{Spec } \text{Sym}(V^\vee)$(2.9.2.8).

**Prop. (7.1.1.8).** Hom$(G_{m,R}, G_{a,R}) = 0$.

**Proof:** Such a homomorphism corresponds to an element $f(T) = \sum a_i T^i$ s.t. $\sum a_i T^i \otimes T^i = \sum a_i (T^i \otimes 1 + 1 \otimes T^i)$, which implies $a_i = 0$ for all $i$. A homomorphism $G_{m,R} \to G_{a,R}$ corresponds to an element $f(T) = \sum a_i T^i$ s.t. $\sum a_i T^i \otimes T^i = \sum a_i (T^i \otimes 1 + 1 \otimes T^i)$, which implies $a_i = 0$ for all $i$. □

**Prop. (7.1.1.9).** Hom$(G_{a,R}, G_{m,R}) = 0$.

**Proof:** The proof is the same as that of *(7.1.1.8)*. □

**Prop. (7.1.1.10).** If $R$ is reduced, then Aut$(G_{a,R}) \cong R$. 
Proof: Any endomorphism of $G_{a,R}$ is of the form $X \mapsto a_0 + a_1 X + \ldots + a_n T^n$. If it is an automorphism, then for any prime ideal $p$, $a_0 \notin p$ and $a_i \in p, i > 0$, thus $a_0$ is a unit and $a_i$ are nilpotent for $i > 1$, so $a_i = 0$ for $i > 1$. □

Prop. (7.1.1.11). For $G \in \mathfrak{Grp}/S$, there is a Cartesian diagram:

$$
\begin{array}{ccc}
G & \xrightarrow{\Delta_{X/S}} & G \times_S G \\
\downarrow & & \downarrow \left( (g,g') \mapsto m(i(g),g') \right) \\
S & \xrightarrow{e} & G
\end{array}
$$

This can be seen by a testing scheme $T$.

Cor. (7.1.1.12) [Separatedness]. $G \in \mathfrak{Grp}/S$ is (quasi-)separated iff $e$ is qc (closed immersion). In particular, if $S$ is a field, then $G$ is separated.

Def. (7.1.1.13) [Character Group]. A character of a group scheme $G$ is a homomorphism $G \to \mathbb{G}_m$. It is easy to see that a character of $G$ is equivalent to a group-like element (2.9.2.19) in $\Gamma(G)$. The characters of $G$ form a group, denoted by $X(G)$. $X(G)(k)$ is denoted by $X^*(G)$.

Moreover, let $k^s/k$ be a separable closure, then the character group of $G_{k^s}$ is denoted by $X^*(G)$.

In particular, if $G$ is an algebraic group scheme over a field, then the set of characters of $G$ are linearly independent, by (2.9.2.20).

Prop. (7.1.1.14) [Sheaf of Differentials is Parallel]. If $f : G \to S \in \mathfrak{Grp}/S$, then there are canonical isomorphisms

$$\Omega_{G/S} \cong f^* \mathcal{C}_{G/S} \cong f^* e^* \Omega_{G/S}.$$ 

In particular, if $S$ is the spectrum of a local ring, then $\Omega_{G/S}$ is a free $\mathcal{O}_G$-module.

Proof: By base change, $\Omega_{G \otimes_S G/S} = \pi_0^* \Omega_{G/S}$, and the transition map

$$\tau : G \otimes_S G \to G \otimes_S G : (g,h) \mapsto (m(g,h),h)$$

is an automorphism of $G \otimes_S G$ over $G$, so there is an isomorphism

$$\tau^* \pi_0^* \Omega_{G/S} \cong \pi_0^* \Omega_{G/S}$$

but $\pi_0 \circ \tau = m$, showing this isomorphism is $m^* \Omega_{G/S} \cong \pi_0^* \Omega_{G/S}$. Now pulling this isomorphism along the isomorphism by $(e \circ f, id) : G \to G \otimes_S G$ we obtain the isomorphism

$$\Omega_{G/S} \cong f^* e^* \Omega_{G/S}.$$ 

Finally $e^* \Omega_{G/S} \cong \mathcal{C}_{S/G}$ by (5.5.5.14). □

Prop. (7.1.1.15). If $k \in \text{Field}$, then any $G \in \mathfrak{Grp}/k$ is geo.reduced.

Proof: Cf. [Sta] 0470. ? □

Prop. (7.1.1.16) [Galois Descent]. Let $k \in \text{Field}, G \in \mathfrak{Grp}/k$ and $K/k$ is a Galois extension with Galois group $\Gamma$. If $H'$ is a subgroup of $G \otimes_k K$, then $H'$ is stable under the action of $\Gamma$ iff there exists a subgroup $H$ of $G$ that $H \otimes_k K = H'$. In this case, $H$ is unique.
Proof: Use (5.1.5.19) and (5.1.5.22). □

Prop. (7.1.1.17). Let $X,Y$ be varieties over a field $k$ that both have at least one $K$-point, and $X$ is complete. Then any morphism $X \times Y \to G$ to a group scheme $G$ over $k$ factorizes as $f(x,y) = g(x)h(y)$, where $f:X \to G$ and $h: Y \to G$.

Proof: Fix a $y_0 \in Y(K)$ and define a morphism $g: X \to G : x \mapsto f(x,y_0)$, then the morphism $F: X \times Y \to G : (x,y) \mapsto g(x)^{-1}f(x,y)$ is constant on $X \times \{y_0\}$. Then the rigidity lemma (5.10.1.20) and (7.1.1.12) shows $F(x, y) = h(y)$ where $h: Y \to G$ is a morphism. Then we are done. □

Cor. (7.1.1.18). Any morphism from a $\mathbb{P}^1_K$ to a group scheme $G$ is constant.

Proof: Let $(x_0, x_1)$ be a homogenous coordinate of $\mathbb{P}^1$, consider the morphism $s: \mathbb{P}^1 \times \mathbb{A}^1 \to \mathbb{P}^1 : (x_0, x_1) \times y \mapsto (x_0, x_0 + x_1y)$. Let $f: \mathbb{P}^1 \to G$ be a morphism, consider the composition

$$\mathbb{P}^1 \times \mathbb{A}^1 \xrightarrow{s} \mathbb{P}^1 \xrightarrow{f} G$$

then by (7.1.4.19), $f \circ s$ factors as $f(s(x,y)) = g(x)h(y)$.

We take $y = 0$, then $s(x, 0) = x$, and $g(x) = f(x)h(0)^{-1}$. Thus $f(s(x,y)) = f(x)h(0)^{-1}h(y)$. Next we take $x = (0,1)$, then $s((0,1), y) = (0, 1)$, and $f((0,1)) = f((0,1))h(0)^{-1}h(y)$. This shows $h(y) = h(0)$ is constant, thus $f(s(x,y)) = f(x)$. Finally, let $x = (0, 1)$, then $s((0,1), y) = y$, and $f(y) = h(0)$ is constant. □

Cor. (7.1.1.19). Let $U$ be an open subset of $\mathbb{P}^1$, then any morphism from $U$ to a group variety $G$ is constant. In particular, $G$ contains no rational curve, and any morphism from a rationally connected variety to $G$ is constant, in particular $\mathbb{P}^n_K$.

Proof: Any rational map from $\mathbb{P}^1$ to $G$ can be extended to a morphism, by (5.11.1.15), thus it is constant, by the proposition above. □

Prop. (7.1.1.20) [Singularity in Codimension]. Let $S \in \text{Sch}$ be normal and Noetherian, $Z, G \in \text{Sch}/S$ s.t. $Z/S$ is smooth and $G/S$ is a smooth separated $S$-group scheme. If $\varphi : Z \to G$ is an $S$-rational map, then every irreducible component of $X \setminus \text{dom}(\varphi)$ is of codimension 1.


Classification of groups schemes of height 1 over a field

Quotients of Group Schemes

Prop. (7.1.1.21) [Grothendieck]. Let $G$ be a group scheme of f.t. over $S$ and $H$ is a closed subgroup scheme of $G$. If $H$ is proper and flat over $S$ and if $G$ is quasi-projective over $S$, then the quotient functor $\overline{G}_{fppf}/\overline{H}_{fppf}$ is representable, denoted by $G/H$.

Proof: Cf.[Grothendieck, A. Technique de descente et theoremes d’6xistence en geometrie algebrique, III]. □

Cor. (7.1.1.22) [Existence of Quotient Space]. Let $H \to G$ be a monomorphism of algebraic groups over a field $k(7.1.5.6)$, then the quotient functor $\overline{G}_{fppf}/\overline{H}_{fppf}$ is representable by an algebraic scheme. And $G \to G/H$ is faithfully flat.
Proof: Cf. [Mil17b] P605. □

Cor. (7.1.1.23) [Quotient by Normal Subgroups]. Every normal algebraic group $N$ of an algebraic group $G$ arises as the kernel of a quotient map $G \to G/N$. And if $G$ is affine, $G/N$ is also affine.

Proof: This is a corollary of (7.1.1.22) and (7.1.1.26) and (7.1.1.27). The second assertion follows from [Mil17] P103. □

Cor. (7.1.1.24) [Quotient Map is a Cokernel]. Let $q : G \to Q$ be a quotient map of algebraic groups over $k$ and let $N$ be the kernel, then every homomorphism $G \to H$ whose kernel contains $N$ factors uniquely through $q$.

Prop. (7.1.1.25). Let $G/H$ be a quotient space, then the map

$$(g, h) \mapsto (g, gh) : G \times H \mapsto G \times_{G/H} G$$

is an isomorphism.

Proof: This is because for any $R$, $G(R) \times H(R) \to G(R) \times G(R)/H(R)$ is an isomorphism, and use the fact $G(R)/H(R) \subset (G/H)(R)$ as $G/H$ is a subfunctor of $G/H$. □

Cor. (7.1.1.26). For any $k$-algebra $R$, the nonempty fibers of $G(R) \to G/H(R)$ are cosets of $H(R)$. In particular, the fiber over $o \in G/H$ is just $H$.

Cor. (7.1.1.27) [Quotient is a Torsor]. $G$ is a (fppf) $H$-torsor over $G/H$.

Proof: This follows from (7.1.1.22) and (7.1.1.27). □

Prop. (7.1.1.28) [Additivity of Dimensions]. Let $G$ be an algebraic group and $H$ an algebraic subgroup, then

$$\dim G = \dim H + \dim G/H.$$ 

Proof: This follows from (5.6.3.17) and (7.1.1.26). (Notice $G(k) \to H(k)$ is surjective (7.1.5.5)). □

Thm. (7.1.1.29) [Homomorphism Theorem]. Every homomorphism of algebraic groups $f : G \to H$ factors uniquely as

$$G \xrightarrow{q} I \xrightarrow{i} H$$

where $q$ is a quotient map and $i$ is a monomorphism. $I$ is called the image of $f$.

Proof: Let $N = \ker(f)$, and $q : G \to I = G/N(7.1.1.23)$, then by (7.1.1.24), $f$ factors through $I$ via a monomorphism $I$ by (7.1.1.21). □

Cor. (7.1.1.30). A homomorphism of algebraic groups is a quotient map iff it is an epimorphism in the category of algebraic schemes.

Proof: For any homomorphism of group schemes $\varphi : G \to H$, factor it as in (7.1.1.29), then we can form the quotient space $H/I$, so if it is an epimorphism, $I = H$, and $\varphi$ is a quotient map. Conversely, if it is a quotient map, then $\mathcal{O}_H \to \varphi_* \mathcal{O}_G$ is injective by (7.1.5.3), thus it is an epimorphism. □

Cor. (7.1.1.31). If $f$ is surjective and $H$ is reduced, then $f$ is a quotient map.
Prop.(7.1.1.32). Let $H, N$ be subgroup schemes of $G$ with $N$ normal, then the canonical map

$$N \rtimes H \to G$$

is an isomorphism iff $N \cap H = e$ and $NH = G$.

Proof: This follows from the exact sequence $e \to N \cap H \to N \rtimes H \to NH \to e$. □

Prop.(7.1.1.33)[Isomorphism Theorem]. Let $H, N$ be algebraic subgroups of an algebraic group $G$ such that $H$ normalizes $N$, then $H \cap N$ is a normal algebraic subgroup of $H$, and the natural map

$$H/H \cap N \to HN/N$$

is an isomorphism.

Proof: The isomorphism is induced by shification of the natural isomorphism

$$TR : H(R)/H(R) \cap N(R) \cong H(R)N(R)/N(R)(2.1.3.8).$$

□

Prop.(7.1.1.34)[Correspondence Theorem]. Let $N$ be a normal algebraic subgroup of an algebraic group $G$, then

- An algebraic subgroup $H$ of $G$, the inverse image of the image of $H$ in $G/N$ is $HN$.
- The map $H \mapsto H/N$ is a bijection between the set of algebraic subgroups of $G$ containing $N$ to the set of algebraic subgroups of $G/N$.
- An algebraic subgroup $H$ of $G$ containing $N$ is normal in $G$ iff $H/N$ is normal in $G/N$, in which case the natural map $G/H \to (G/N)/(H/N)$ is an isomorphism.


Prop.(7.1.1.35)[Group Formation]. WARNING: the category $\mathcal{A}lg\mathcal{G}rp_k$ of algebraic groups is not Abelian, not even an exact category, but it is a group formation(3.2.2.1), and its subcategory $\mathcal{C}\mathcal{A}lg\mathcal{G}rp_k$ of commutative algebraic groups is an Abelian category, by(7.1.1.23)(7.1.5.2)(7.1.1.4).

Also the subcategory of affine algebraic groups is a Serre subcategory, by(7.1.1.23) and(7.1.5.29).

Cor.(7.1.1.36). By taking shification, it can be shown that the same categorical properties of $\mathcal{G}rp$ holds for $\mathcal{A}lg\mathcal{G}rp_k$, such as the nine lemma, five lemma, and the restrictive snake lemma.

2 Finite Groups

Main references are [Finite Flat Group Schemes and $p$-Divisible Groups, Jakob], [Finite Group Schemes, Pink], [Introduction to Finite Group Schemes], [Finite Flat Group Schemes, Tate].

Def.(7.1.2.1)[Finite Locally Free Group Schemes]. A finite Locally Free group scheme is a group scheme $G$ that is finite locally free(5.6.2.22) over $S$. It is said to have order/rank $d$ if $G$ is finite locally free of rank $d$ over $S$, where $d$ is a locally constant integral-valued function on $S$.

Def.(7.1.2.2)[Finite Groups]. A finite locally free group scheme over a field $k$ is called a finite group scheme over $k$. An infinitesimal group scheme is a finite group scheme $G$ s.t. $|G| = e$. 
Prop. (7.1.2.3) [Cartier]. Let \( k \) be a field of characteristic 0, then
- Every affine finite commutative group scheme over \( k \) is finite étale.
- If \( k \) is alg.closed, then there is an equivalence of categories between finite commutative group schemes over \( k \) and \( \text{Ab} \), by \( G \mapsto G(k) \) and \( \Gamma \mapsto \Gamma_k \).

Proof: 1: by (2.9.2.22) and (4.4.7.20).
2: \( \Gamma_k \) is clearly affine commutative group schemes over \( k \). If \( A \) is finite locally free Hopf algebra over \( k \), then it is finite étale by item 1 and isomorphic to a finite product of copies of \( k \). Now the equivalence is clear. \( \square \)

Prop. (7.1.2.4) [Finite Group Schemes of Order Invertible in \( S \) is Finite Étale]. A finite group scheme \( G \) over \( S \) of order invertible in \( S \) is finite étale.

Proof: Cf. [Jakob, P45]. \( \square \)

Prop. (7.1.2.5) [Finite Étale Group Schemes]. Let \( X \) be a connected smooth scheme with a geometric point \( x \), then there is an equivalence of categories:

\[
\{\text{Finite étale group schemes over } X\} \leftrightarrow \{\text{Finite groups with a continuous action of } \pi_1(X, x)\}
\]

by (6.3.2.5). In particular, constant group schemes correspond to finite groups with trivial \( \pi_1(X, x) \) actions.

Cor. (7.1.2.6). The category of finite étale commutative group schemes over \( X \) is Abelian.
The category of commutative group schemes over \( X \) of order invertible in \( X \) is Abelian, by (7.1.2.4).

Commutative Finite Groups

Prop. (7.1.2.7) [Cartier Duality]. Let \( G \) be a finite commutative locally free group scheme over \( S \), then \( \mathcal{O}_G \) is a finite locally free \( \mathcal{O}_S \)-Hopf algebra, then \( \text{Hom}_{\mathcal{O}_S}(\mathcal{O}_G, \mathcal{O}_S) = \mathcal{O}_G^\vee \) is again a finite locally free \( \mathcal{O}_S \)-Hopf algebra (5.2.5.2), and thus \( \text{Spec} \mathcal{O}_G \) is a finite locally free group scheme over \( S \), called the Cartier dual \( G^D \) of \( G \).

Moreover, this Cartier dual of \( G \) represents the Hom sheaf \( \text{Hom}_{\text{Sch}}(G, \mathbb{G}_m) \).
If \( G \) is dual to \( G' \), then their base changes are dual, too.
Finally, \((G^D)^D = G \) by (5.2.5.2), so Cartier duality is a contravariant autoequivalence of the category of commutative finite locally free group schemes over \( S \).

Proof: For the Hom sheaf, we need to show

\[
G^D(T) \cong \text{Hom}_T(G \otimes_S T, \mathbb{G}_m,T)
\]

for any \( T/S \). Notice a \( g \in G^D(T) \) corresponds to an \( R \)-algebra morphism \( g \in \text{Hom}_{\mathcal{O}_S}(\mathcal{O}_G', \mathcal{O}_T) = \mathcal{O}_G \otimes_{\mathcal{O}_S} \mathcal{O}_T (5.2.5.2) \) that satisfies

\[
(\Delta \otimes \text{id}_T)(g) = g \otimes_T g \in (\mathcal{O}_G \otimes_{\mathcal{O}_S} \mathcal{O}_G) \otimes_{\mathcal{O}_S} \mathcal{O}_T, \quad (\epsilon \otimes \text{id}_T)(g) = 1
\]

Also, \( g \) is a unit, as

\[
g \cdot (i \times \text{id}_T)(g) = \mu \circ ((\text{id}_{\mathcal{O}_G} \otimes \eta) \otimes \text{id}_T)(g \otimes g) = \mu \circ ((\text{id}_{\mathcal{O}_G} \otimes \epsilon) \otimes \text{id}_T) \circ (\Delta \otimes \text{id}_T)(g) = (\eta_{\mathcal{O}_G} \otimes \text{id}_T)(\epsilon \otimes \text{id}_T)(g) = 1
\]
prop. (7.1.2.8) [Γ is Cartier Dual to D(Γ)]. Let Γ be a finite commutative group and S be a scheme, then ΓS is Cartier dual to D(Γ)S.

Proof: By (7.1.2.7), it suffices to show for S = Spec Z. Now Γ = ∏γ∈Γ Z, and Δ(γ) = ∑gg′=γ eg ⊗ eg'. Let fγ ∈ Γ∨ be dual to εγ, then

\[ f_γ \cdot f_γ' = \sum_{g \in Γ} Δ^∨(f_γ \otimes f_γ')(e_g)f_g = \sum_{g \in Γ} f_γ \otimes f_γ'(\sum_{st=g} e_s \otimes e_t)f_g = f_γ f_γ' \]

so Γ∨ ∼= Z[Γ], and

\[ Δ(γ) = \sum_{g, g' \in Γ} \mu^∨(f_γ)(e_g \otimes e_{g'})f_g \otimes f_{g'} = f_γ f_γ. \]

Cor. (7.1.2.9). Z/nZ is Cartier Dual to μn.

Prop. (7.1.2.10) [αp is Cartier Dual to αp]. Over a Fp-scheme S, the group scheme αp,S is Cartier dual to itself.

Proof: By (7.1.2.7), it suffices to show for S = Spec Fp. Then αp = Fp[X]/Xp with

\[ Δ(X) = X \otimes 1 + 1 \otimes X, \quad ε(\alpha) = 0, S(\alpha) = −X. \]

Let Yi ∈ α∨p dual to Xi then

\[ Y_i Y_j = \sum_{k=0}^{p-1} Δ^∨(Y_i \otimes Y_j)(X^k)Y_k = \sum Y_i \otimes Y_j(Δ(X^k))Y_k = \sum Y_i \otimes Y_j(\sum_{a+b=k} \binom{k}{a} X^a \otimes X^b)Y_k = \binom{i+j}{i} \]

Now \(\binom{i+j}{i}\) is unit, so α∨p = Fp[Y]/Yp where Y = Y1. and

\[ Δ(Y) = \sum_{a, b} \mu^∨(Y)(X^a \otimes X^b)Y_a \otimes Y_b = \sum Y(X^{a+b}) = Y \otimes 1 + 1 \otimes Y, \]

so α∨p = αp.

Prop. (7.1.2.11). If G1, G2 are finite groups over a field k, then there are no non-trivial homomorphism from G1 to G2 or from G2 to G1 if G1 is étale and G2 is connected.

Proof: Cf. [Van de Geer, P67].

Prop. (7.1.2.12). If \(e \to G_1 \to G \to G_2 \to e\) is an exact sequence of finite locally free group schemes over S, then rank(G) = rank(G1) · rank(G2).

Proof: Cf. [Van de Geer, P68].

Prop. (7.1.2.13). Let char k = p > 0, then the rank of any finite group over k is a power of p.
Proof: Cf.[Van de Geer, P68].

Cor. (7.1.2.14). Let \( \text{char } k = p > 0 \), then a finite group over \( k \) is étale and coétale iff \( p \nmid \text{rank}(G) \).

Proof: Cf.[Van de Geer, P68].

Prop. (7.1.2.15). Over a \( \mathbb{F}_p \)-scheme \( S \), the three group schemes \( \mathbb{Z}/p\mathbb{Z}_S, \mu_p, \alpha_p \) are mutually non-isomorphic.

Proof: We may take a fiber and assume \( S = \text{Spec } K \), then \( \mathbb{Z}/p\mathbb{Z}_S \) is reduced, \( \mu_p \) is non-reduced and \( \alpha_p \) is non-reduced. Then we can look at the reducedness of the group scheme and its Cartier dual.

Prop. (7.1.2.16)[The Order Kills the Group, Deligne]. If \( G \) is a finite locally free commutative group scheme over \( S \) of constant order \( n \), then \( [n]_G = 0 : G \rightarrow G \).

Proof: Cf.[Jakob P12].

Finite Locally Free Group Schemes over Henselian Local Rings

Remark (7.1.2.17). Throughout this subsubsection, let \( R \) be a Henselian local ring \((R, m)\).

Prop. (7.1.2.18).

Proof:

Cor. (7.1.2.19). Let \( R \) be a equicharacteristic Henselian local ring of characteristic \( p > 0 \), then every finite locally free group scheme over \( R \) of prime order is automatically commutative.

Proof: Cf.[Shatz, P50].

Cor. (7.1.2.20). Let \( R \) be a strict Henselian local ring with residue field of characteristic \( p > 0 \), then any connected finite locally free group scheme over \( R \) has order \( p^t \) for some \( t > 0 \).

Proof: Cf.[Shatz, P50].

Commutative \( p \)-Group Schemes

Cf.[Finite Flat Group Schemes, Tate] Section 4.

3 Groupoid Schemes

Cf.[Sta] Cha 38, 39.

4 Algebraic Groups over Fields

All group schemes \( G \) in this subsection are algebraic over a field \( k \).

Prop. (7.1.4.1)[Smoothness and Geo.Reducedness]. For a locally algebraic group scheme \( G \) over a field \( k \), smoothness is equivalent to geo.reduced at a closed point.

Proof: If \( G \) is smooth, then it is geo.regular thus geo.reduced. The converse follows from (7.2.1.10).
Cor. (7.1.4.2) [Cartier]. Any locally algebraic group scheme over a field of char 0 is smooth.

Proof: This is a consequence of (7.1.1.15) and (7.1.4.1). Alternative proof: \( \Omega_{G/k} \) is free, by (7.1.1.14), so it is smooth by (5.6.4.15).

Prop. (7.1.4.3) [Reduced Structure]. If \( G_{\text{red}} \) is geo.reduced, then it is a subgroup of \( G \). This is the case if \( k \) is perfect.

Proof: This is because \( G_{\text{red}} \times G_{\text{red}} \) is reduced so the multiplication factors through \( G_{\text{red}} \times G_{\text{red}} \).

□

Prop. (7.1.4.4) [Smoothness in Characteristic \( p \)]. Let \( G \) be an affine algebraic group scheme over a perfect field \( k \) of characteristic \( p \neq 0 \), and \( r \geq 0 \), then image of the relative Frobenius \( F_{G/k} : G \to G^{(p^r)} \) is geo.reduced group scheme when \( r \) is sufficiently large.

Proof: To show it is a group scheme, notice \( F^r \) is a homomorphism and use homomorphism theorem (7.1.1.29). And it corresponds to

\[
\Gamma(G) \otimes_{k,\phi^r} k \to \Gamma(G) : a \otimes c \mapsto cac^r.
\]

The image of which is just \( \Gamma(G)^{p^r} \) as \( k \) is perfect. To show it is geo.reduced, we can assume \( k \) is alg.closed, then the nilradical \( N \) of \( \Gamma(G) \) is nilpotent, so some \( N^m = 0 \), and then the image is reduced for any \( p^r > m \).

□

Prop. (7.1.4.5) [Smoothness and Tangent Space]. A locally algebraic group scheme \( G \) over a field is smooth iff it is regular iff \( \dim_k T_e \leq \dim_e G \), where \( e \) is the identity element.

Proof: By homogeneity and the fact smooth locus is open, \( G \) is smooth iff it is smooth at \( e \). Now \( e \) is a rational point, by (4.4.5.26), \( G \) is smooth at \( e \) iff it is regular at \( e \).

□

Prop. (7.1.4.6) [Closed Subgroups and Points]. Let \( G \) be a locally algebraic subgroup over \( k \) and \( S \subset G(k) \) a closed subgroup, then there is a unique reduce closed subgroup \( H \) of \( X \) that \( H(k) = S \). Moreover, \( H \) is geo.reduced. The algebraic subgroups of \( G \) arising in this way are exactly those that \( H(k) \) is schematically dense in \( H \). Linear In particular, when \( k \) is sep.closed, then \( H \mapsto H(k) \) is a bijection between closed subgroups of \( G \) and closed subgroups of \( G(k) \), by (5.4.3.10).

Proof: Let \( H \) be a reduced closed subscheme of \( G \) that \( H(k) = S \), then \( S \) is dense in \( |H| \) and \( H \) is reduced, so by (5.4.3.5) and (5.4.3.8) shows \( S \) is schematically dense in \( H \) and \( H \) is geo.reduced. Therefore \( H \times H \) is reduced and thus multiplication map \( H \times H \to G \) factors through \( H \), also does inversion and unit, so \( H \) is a subgroup of \( G \).

The converse is also true.

□

Cor. (7.1.4.7) [Zariski Closure]. Let \( G \) be a locally algebraic subgroup over \( k \) and \( S \subset G(k) \) a subgroup, then there is a unique geo.reduced closed subscheme \( H \) of \( G \), called the Zariski closure of \( S \) in \( G \), such that \( H(k) \) is the Zariski closure of \( S \subset G(k) \).

Prop. (7.1.4.8) [Algebraic Group Scheme is Quasi-Projective]. Any algebraic group scheme over a field \( k \) is quasi-projective.

Proof: Cf. [Sta]0BF7.

□
Prop. (7.1.4.9) [Center Subgroup]. For a locally algebraic group scheme $G$ over a field $k$, its center is an algebraic subgroup of $G$.

Proof: Cf. [Sta]0BF8. □

Prop. (7.1.4.10). Every étale normal subgroup of a connected algebraic group is central.

Proof: This is because the automorphism group scheme of an étale group scheme is étale. □

Prop. (7.1.4.11) [Identity Component]. For a locally algebraic group $G$ over a field $k$, consider its identity component $G^0$, then

- It commutes with the formation of identity component commutes with base change of fields.
  In particular, $G^0$ is geo.connected.

- $G$ is locally connected (5.4.1.23), thus $G^0$ is clopen in $G$.

- $G^0$ is a characteristic algebraic subgroup of $G$.

Proof: 1, 2 follows from (5.4.3.15).

3: By (5.4.3.12), $G^0 \times G^0$ is connected, thus $G^0 \times G^0$ is mapped into $G^0$, and it is an open subscheme, thus it is an algebraic subgroup of $G$. □

Cor. (7.1.4.12) $[\pi_0(G)]$. Let $G$ be a locally algebraic group, then group structure induces a group structure on the maximal étale subalgebra of $\Gamma(G)$, thus $G \to \pi_0(G)$ is a group homomorphism (6.3.1.1), which is faithfully flat by (6.3.1.3), and the stabilizer of the identity in $\pi_0(G)$ is just $G^0$ by (6.3.1.3) again. Thus $\pi_0(G) = G/G^0$ by (7.2.1.11).

Prop. (7.1.4.13). Every connected component of a locally algebraic group $G$ over a field $k$ is irreducible.

Proof: By (7.1.4.11), $G^0_K$ is connected. To show it is irreducible, it suffices to consider its reduced structure, and in this case it is smooth (Notice in this case $G^0_{\text{red}}$ is an algebraic group because $G^0_{\text{red}} \times G^0_{\text{red}}$ is reduced). Thus no closed point is connected in two irreducible component, thus it is irreducible. Then $G^0$, as a quotient space of $G^0_K$ is also irreducible.

For another connected component $H$, choose a closed point $h$, let $L$ be a finite normal extension of $k$ containing $k(h)$, then each connected component of $H_L$ maps surjectively onto $H$, thus contains one of the finitely many inverse images of $h$ in $H_L$. And they are all rational points, thus isomorphic to $G^0_L$, which is irreducible, thus $H$ is also irreducible. □

Cor. (7.1.4.14) [Connected Algebraic Group is Geo.Irreducible]. A connected algebraic group over a field is geo.irreducible by (7.1.4.11) and (7.1.4.13).

Cor. (7.1.4.15). If $G$ is a connected algebraic group over a field $k$, then for any non-empty open subschemes $U, V$ of $G$, $U \times V \to G$ is surjective.

Proof: By (5.4.1.29), it suffices to check on closed points. Let $p$ be a closed point, by base change, we may assume $x \in G(k)$, then $xV^{-1} \cap U \neq \emptyset$ as $G$ is geo.irreducible (7.1.4.14), thus $x \in UV$. □

Cor. (7.1.4.16). Every connected component of a locally algebraic group scheme over a field $k$ is algebraic over $k$. 
Proof: For the identity component, take a non-empty affine open subset $U$, then $U^2 = G^0$ by (7.1.4.15), thus $G^0$ is quasi-compact. For the other components, the same proof as that of (7.1.4.13) shows they are also quasi-compact. □

Def. (7.1.4.17) [Torsion Component]. Let $G$ be a locally algebraic commutative group over $k$, then $G^\tau = \cup_{n>0}[n]^{-1}G^0 \subset G$ is an open group subscheme, called the torsion component of $G$. Forming $G^\tau$ commutes with change of fields, and if $G^\tau$ is quasi-compact, it is a clopen subgroup.

Prop. (7.1.4.18). Let $G$ be a locally algebraic commutative group over $k$, then any algebraic subgroup of $G$ is contained in $G^\tau$. In particular, if $G^\tau$ is algebraic over $k$, then it is the maximal algebraic subgroup of $G$.

Proof: As $H$ is qc, it is covered by f.m. translates of $G^0$, thus $G^0$ has finite index in $G^0H$, which means $[n](H) \subset G^0$ for some $n \in \mathbb{Z}_+$. □

Prop. (7.1.4.19). Let $X, Y$ be varieties over a field $k$ that both have at least one $K$-point, and $X$ is complete. Then any morphism $X \times Y \to G$ to a group scheme $G$ over $k$ factorizes as $f(x, y) = g(x)h(y)$, where $f : X \to G$ and $h : Y \to G$.

Proof: Fix a $y_0 \in Y(K)$ and define a morphism $g : X \to G : x \mapsto f(x, y_0)$, then the morphism $F : X \times Y \to G : (x, y) \mapsto g(x)^{-1}f(x, y)$ is constant on $X \times \{y_0\}$. Then the rigidity lemma (5.10.1.20) and (7.1.1.12) shows $F(x, y) = h(y)$ where $h : Y \to G$ is a morphism. Then we are done. □

Cor. (7.1.4.20). Any morphism from a $\mathbb{P}^1_K$ to a group scheme $G$ is constant.

Proof: Let $(x_0, x_1)$ be a homogenous coordinate of $\mathbb{P}^1$, consider the morphism $s : \mathbb{P}^1 \times \mathbb{A}^1 \to \mathbb{P}^1 : (x_0, x_1) \times y \mapsto (x_0, x_0 + x_1y)$. Let $f : \mathbb{P}^1 \to G$ be a morphism, consider the composition

$$\mathbb{P}^1 \times \mathbb{A}^1 \xrightarrow{s} \mathbb{P}^1 \xrightarrow{f} G$$

then by (7.1.4.19), $f \circ s$ factors as $f(s(x, y)) = g(x)h(y)$.

We take $y = 0$, then $s(x, 0) = x$, and $g(x) = f(x)h(0)^{-1}$. Thus $f(s(x, y)) = f(x)h(0)^{-1}h(y)$. Next we take $x = (0, 1)$, then $s((0, 1), y) = (0, 1)$, and $f((0, 1)) = f((0, 1))h(0)^{-1}h(y)$. This shows $h(y) = h(0)$ is constant, thus $f(s(x, y)) = f(x)$. Finally, let $x = (0, 1)$, then $s((0, 1), y) = y$, and $f(y) = h(0)$ is constant. □

Cor. (7.1.4.21). Let $U$ be an open subset of $\mathbb{P}^1$, then any morphism from $U$ to a group variety $G$ is constant. In particular, $G$ contains no rational curve, and any morphism from a rationally connected variety to $G$ is constant, in particular $\mathbb{P}^n_K$.

Proof: Any rational map from $\mathbb{P}^1$ to $G$ can be extended to a morphism, by (5.11.1.15), thus it is constant, by the proposition above. □

Def. (7.1.4.22) [Anti-Affine Group Schemes]. An anti-affine algebraic group is an algebraic group over $k$ s.t. $\Gamma(G) = k$. For example, Abelian varieties are anti-affine by (5.10.1.12)

Prop. (7.1.4.23). Let $\varphi : G \to H$ be a homomorphism of algebraic groups over $k$ that $G$ is anti-affine and $H$ is connected, then $\varphi$ factors through the center of $H$ (7.1.4.9).

Proof: Cf. [?]P151. □

Cor. (7.1.4.24). If $G$ is a connected algebraic group over $k$, then every anti-affine algebraic subgroup is contained in the center of $G$.

Cor. (7.1.4.25). Any anti-affine algebraic group is commutative and connected.

Proof: $G \to \pi_0(G)$ is surjective but $\pi_0(G)$ is affine thus this map is trivial, so $G$ is connected. Then it is also commutative by (7.1.4.24). □
Construction of Algebraic Groups

Prop. (7.1.4.26) [Generated Closed Subgroup]. Let \( \varphi_i : X_i \to G \) be a family of maps from algebraic schemes \( X \) to an algebraic group over a field \( k \).

- If \( X_i \) and \( G \) are all affine, then the generated group scheme is representable by an algebraic subgroup \( H \).
- If \( X_i \) are all geo.reduced. Then the generated group scheme is representable by a smooth subgroup \( H \).

Moreover, in both cases, if there is only a single map \( \varphi : X \to G \) and \( X \) is geo.connected, and \( e \subset \varphi(X) \), then \( \langle X, \varphi \rangle \) is geo.connected.


Def. (7.1.4.27) [Commutator Group]. Let \( G \) be an algebraic group that is affine or smooth, then \([G,G]\) exists by (7.1.4.26), and:

- \([G,G]\) is the intersection of all normal subgroups \( H \) of \( G \) s.t. \( G/H \) is commutative.
- For a field extension \( k'/k \), \([G_{k'},G_{k'}] = [G,G]_{k'}\).
- If \( G \) is geo.connected/smooth, then \([G,G]\) is also geo.connected/smooth.
- If \( G \) is an affine smooth geo.connected group scheme, then \([G,G]\) is the unique smooth geo.connected subgroup scheme that satisfies \([G,G](\overline{k}) = [G(\overline{k}),G(\overline{k})]\).

2: This is formal.
3: This follows from (7.1.4.26).
1: Cf. [Mil17] P130. □

Def. (7.1.4.28) [Transporter]. Let \( G \times X \to X \) be an action of an algebraic group on a scheme, and \( Y, Z \) be subschemes of \( X \), \( Z \) is a closed subscheme and \( Y \) is an algebraic scheme, then the functor

\[
R \mapsto \{ g \in G(R) | gY_R \subset Z_R \}
\]

is represented by a closed subscheme of \( G \), called the transporter \( T_G(Y,Z) \).

Proof: \( T_G(Y,Z) \) is in fact the sheaf \( \mathcal{H}om(Y,Z) \setminus \mathcal{H}om(Y,X) \) \( G \), and notice \( \mathcal{H}om(Y,Z) \to \mathcal{H}om(Y,X) \) is a closed subfunctor \( 7.1.1.3 \), thus \( T_G(Y,Z) \) is a closed subfunctor of \( G \), thus represented by a closed subscheme of \( G \). □

Cor. (7.1.4.29). Let \( G \times X \to X \) be an action of an algebraic group on a scheme, and \( Y, Z \) be closed subschemes of \( X \), then the functor

\[
R \mapsto \{ g \in G(R) | gY_R = Z_R \}
\]

is represented by a closed subscheme of \( G \).

Proof: In this case, the functor is represented by the closed subscheme \( T_G(Y,Z) \cap \text{inv}(T_G(Z,Y)) \). □

Cor. (7.1.4.30) [Stablizer]. Let \( G \times X \to X \) be an action of an algebraic group on a scheme, and \( Y \) be closed subschemes of \( X \), then the functor

\[
\text{Stab}_G(Y) : R \mapsto \{ g \in G(R) | gY_R = Y_R \}
\]

is represented by a closed subscheme of \( G \), called the stabilizer subgroup of \( Y \).
7.1. GROUP SCHEMES I: STRUCTURE THEORY

Def. (7.1.4.31) [Normalizer].

Def. (7.1.4.32) [Centralizer].

**Group Varieties**

Def. (7.1.4.33) [Group Varieties]. A group variety over a field $k$ is a $k$-variety (5.10.1.3) that is also a group scheme.

Prop. (7.1.4.34) [Group Varieties are Smooth]. A group variety over $k$ is smooth by (7.1.4.1). Conversely, any smooth connected algebraic group over $k$ is a group variety, by (7.1.4.14) (7.1.1.12).

Prop. (7.1.4.35) [Tangent Bundle Trivial]. For a group variety over a field $k$, $T_{X,e}$ is the tangent space at $e$, then there is a natural isomorphism $\Omega_{X/k} \cong T^\ast_{X,e} \otimes_{O_X}$. Also true for $T_X$ (because $\Omega_{X/k}$ is locally free as $X$ is smooth (7.1.4.34) (5.10.1.14)).

Proof: There should be another proof using relation in (5.5.5.14)?

Use a dual number characterization of tangent spaces and tangent vector fields (5.6.4.22) (5.10.1.15), then notice a tangent vector $\tau \in T_{X,e}$ is a $S = k[\varepsilon]$-point of $X$, then right translation gives a translation $x_s \to X_s$ that is invariant on $X$, which gives a tangent vector on $X$.

So there is a map $T_{X,e} \otimes O_X \to \Omega_{X/k}$. To check isomorphism, both are locally free of the same rank, so it suffices to show it is surjective. But on closed pts, pass to Nakayama, this is clearly true, so it is surjective by (5.10.1.13). □

Prop. (7.1.4.36) [Dimension Theorem]. Let $\varphi : G \to H$ be a surjective homomorphism of group varieties, then

$$\dim(G) = \dim(H) + \dim(\ker(\varphi)).$$

Proof: This is a consequence of (5.6.3.19), as the fiber over any closed pt is isomorphic to a field base change of $\ker(\varphi)$. □

Prop. (7.1.4.37). Every binational homomorphism of a connected affine group varieties is an isomorphism.

Proof: Such an isomorphism induces a homomorphism $A \to B$ of integral Hopf algebras that is an isomorphism on the fraction field, then it is an isomorphism by (2.9.2.24). □

Def. (7.1.4.38) [Quasi-Central Homomorphisms]. A quasi-central homomorphism $\varphi : G' \to G$ of group varieties over $k$ is a homomorphism the kernel of $\varphi(\overline{k})$ is central in $G'(\overline{k})$.

Prop. (7.1.4.39). If a homomorphism of group varieties $\varphi : G' \to G$ is quasi-central and the kernel of Lie($\varphi$) is central, then $\ker(\varphi) \subset Z(G')$.

Proof: Cf. [Bruhat-Tits, 2.1]. □

Prop. (7.1.4.40) [1-Dimensional Group Varieties]. Let $G$ be a group variety over a field $k = \overline{k}$, then either $G \cong G_a$, $G_m$ or an elliptic curve.

Proof: Cf. [Sil99]. □
5 Homomorphisms

Prop.(7.1.5.1) [Connected-étale Sequence]. Cf.[Mil17]P14, [Finite Flat Group Schemes, Tate]Section3.7 and [Mil17b]P117.

Prop.(7.1.5.2)[Algebraic Subgroups are Closed]. Algebraic subgroups $H$ of an algebraic group $G$ are closed subgroups. In particular, an algebraic subgroup of an affine algebraic group is affine.

**WARNING:** $H$ must first be an algebraic group, so we can use Chevalley theorem to show it is locally closed.

**Proof:** As $H_{k'} \to H$ is a quotient map (5.4.6.3), we can assume $k$ is alg.closed, and also assume $H,G$ are reduced. Now Chevalley shows that the image is a constructible set of $G$. Then we can consider all on the level of $k$ points, because $G$ is Jacobson. Then $H \cap G(k)$ is the closure of $H(k)$ in $G(k)$, thus it is also a subgroup of $G(k)$, and we can consider the coset of $H(k)$ in $H(k)$ in $H(k)$, $H$ is open in $H$, and $H$ is compact, and also $H(k)$ is compact because $G$ is Jacobson, so there are only f.m. coset, thus $H(k)$ is also closed in $H(k)$, thus $H$ is also closed in $H$, so $H = H$. □

Prop.(7.1.5.3)[Characterizing Quotient Maps]. The following conditions on a homomorphism $\varphi : G \to Q$ of algebraic groups are equivalent:

1. $\varphi$ is fully faithful.
2. $\varphi$ is a quotient map (7.1.1.4).
3. The homomorphism $O_Q \to O_G$ is injective.

**Proof:** 1 $\to$ 2 follows from the very definition of fat subfunctors, as f.f. map is a fppf cover. Cf.[Mil17]P109. □

Prop.(7.1.5.4). Let $\varphi : G \to H$ be a surjective homomorphism of group schemes and $H$ is reduced, then $\varphi$ is a quotient map.

**Proof:** The hypothesis implies $G(k)$ acts transitively on $H(k)$, thus $\varphi$ is faithfully flat by (7.2.1.4). □

Prop.(7.1.5.5)[Check Quotient Map on Closed Points]. Let $\varphi : G \to H$ be a quotient map of locally algebraic groups, then $\varphi : G(k) \to H(k)$ is surjective. The conversely is also true if $H$ is reduced. In particular, if $e \to N \to G \to H \to e$ is an exact sequence, then $e \to N(k) \to G(k) \to H(k) \to e$ is exact.

Moreover, if $\varphi$ is étale, then $\varphi : G(k^s) \to H(k^s)$ is also surjective.

**Proof:** This follows from the fact for any $x \in H(k)$ (resp. $k^s$), $G_x$ is non-empty and locally algebraic (resp. étale) over $k(x)$, thus has a $k$ (resp. $k^s$-point).

For the converse, notice the image of $\varphi$ has the same $k$-points as $H$, thus it equals $H$ as $H$ is reduced and locally algebraic. □

Prop.(7.1.5.6)[Characterizing Monomorphisms]. For a homomorphism $\varphi : G \to H$ of algebraic groups over $k$, the following are equivalent:

1. $\varphi$ is a monomorphism.
2. $\ker(\varphi) = e$ (7.1.1.4).
• $\varphi$ is a monomorphism in the category of algebraic groups over $k$.
• $\varphi$ is a monomorphism in the category of algebraic schemes over $k$.

Moreover, a monomorphism is just a closed embedding.

Proof: $1 \to 4 \to 3$ is obvious.
3 $\iff$ 2: the composition of $\ker(\varphi) \to G$ with $\varphi$ is trivial, thus $\ker(\varphi)$ is trivial.
2 $\iff$ 1: This follows from the definition of $\ker(\varphi)(7.1.1.4)$.

For the last assertion, if $\varphi$ is a closed embedding, then, conversely, if $\varphi$ is a monomorphism, consider the quotient space $G \to G/H(7.1.1.21)$, then by(7.1.1.26), $H$ is the fiber over $o \in G/H$, thus a closed subscheme. $\square$

Def.(7.1.5.7)[Embedding]. An embedding of algebraic groups is a closed immersion of algebraic groups.

Isogenies

Def.(7.1.5.8)[Finite Index Subgroups]. An algebraic subgroup $H$ of an algebraic group scheme $G$ is said to have finite index if the quotient $G/H$ is a finite scheme.

Prop.(7.1.5.9). For any algebraic group $G$ over $k$, the identity component $G^0$ is of finite index in $G$.

Proof: Notice an algebraic group $H$ is finite iff $\#H(\overline{k}) < \infty$. And $(G/G^0)(\overline{k}) = G(\overline{k})/G^0(\overline{k})(7.1.4.11)$ is finite as $G$ is compact. $\square$

Def.(7.1.5.10)[Isogeny]. A homomorphism of algebraic groups $G \to H$ is called an isogeny if its kernel is finite and its image is of finite index in $H(7.1.5.8)$.

Def.(7.1.5.11)[Strongly Connected Groups]. An algebraic group $G$ is called a strongly connected group if it has no non-trivial subgroup of finite index.

Def.(7.1.5.12)[Strongly Identity Components]. The strongly identity component $G^{s0}$ of an algebraic group $G$ is defined to be the intersection of the algebraic subgroups of finite index. Thus it is a characteristic subgroup of $G$.

Prop.(7.1.5.13). $G/G^{s0}$ is a a finite scheme. In particular, $G^{s0}$ is the smallest algebraic subgroup having the same dimension as $G$.

Proof: As $G$ is Noetherian, $G^{s0} = H_1 \cap \ldots H_r$ for $G/H_i$ finite schemes. Thus $G/G^{s0} \hookrightarrow H_1 \cap \ldots H_r$ is a finite scheme. $\square$

Prop.(7.1.5.14)[Strongly Identity Components and Identity Components]. $G^{s0}$ is connected, and the converse is true if $G$ is smooth. In fact, if $G$ is smooth, $G^{s0} = G^0$.

In particular, a group variety has no algebraic subgroup of finite index. Thus an isogeny to a group varieties is surjective(thus a quotient map by(7.1.1.31)).

Proof: $G^{s0}$ is connected because the identity component is of finite index(7.1.5.9). Conversely, $G^0/G^{s0}$ is smooth and connected and finite(7.1.5.29), thus it is a group variety of dimension0, which is trivial. $\square$

Prop.(7.1.5.15). Let $G$ be an algebraic group over a perfect field $k$, then $G^{s0}_{\text{red}} = G^{s0}$. 

Def.(7.1.5.16). A central/multiplicative isogeny is an isogeny that the kernel is central/of multiplicative type.

Prop.(7.1.5.17). Any isogeny with kernel order prime to the characteristic has étale kernel by (7.1.2.4), thus it is central, by (7.1.4.10).

Prop.(7.1.5.18). Every multiplicative isogeny from a connected algebraic group is central, by (7.2.3.22).

Def.(7.1.5.19). A composition of multiplicative isogenies is a multiplicative isogeny.

Proof: This is because there is an exact sequence $e \to \ker(\varphi_1) \to \ker(\varphi_2 \circ \varphi_1) \to \ker(\varphi_2) \to e$, thus $\ker(\varphi_2 \circ \varphi_1)$ is central, hence of multiplicative type by (7.2.3.16).

Prop.(7.1.5.20)[Isogenies between Group Varieties]. Let $\varphi: G \to H$ be a surjective homomorphism of group varieties, then $\varphi$ is flat. And if $\dim G = \dim H$, then $\varphi$ is finite, and the rank of $\ker(\varphi)$ equals the separable degree of $K(G)/K(H)$.

Proof: $\varphi$ is flat by (7.2.1.4). By (5.10.3.4), there exists a dense open subscheme $U'$ s.t. $\varphi^{-1}(U') \to U'$ is finite, thus by homogeneity, $\varphi$ is finite, and rank of $\ker(\varphi)$ is $[K(G):K(H)]_s$. □

Subnormal Series

Prop.(7.1.5.21)[Solubility]. Let $G$ be an algebraic group that is either affine of smooth, then $G$ is solvable iff $G^{(n)} = e$ for some $n$ large. In particular, for a field extension $k'/k$, $G$ is solvable iff $G_{k'}$ is solvable.

Prop.(7.1.5.22)[Nilpotency]. Let $G$ be an algebraic group that is either affine of smooth, then $G$ is nilpotent iff $G^n = e$ for some $n$ large. In particular, for a field extension $k'/k$, $G$ is solvable iff $G_{k'}$ is solvable.

In particular, if $G$ is a nilpotent and geo.connected, then it contains a non-trivial geo.connected subgroup scheme in its center, by (7.1.4.27).

Prop.(7.1.5.23). A split solvable algebraic group $G$ is an affine group variety, by (7.1.5.29) and (7.1.5.29).

Lemma(7.1.5.24). If $G = G_0 \triangleright G_1 \triangleright \ldots \triangleright G_s = \{e\}$ is a subnormal series and $\dim G = \dim G_i/G_{i+1}$ for some $i$, then $G \sim G_i/G_{i+1}$.

Proof: The maps $G_i \to G_i/G_{i+1}$ and $G_i \to G_{i-1} \to \ldots \to G_0 = G$ are isogenies (7.1.5.10). □

Def.(7.1.5.25) [Composition Series]. A composition series of $G$ is defined to be a maximal object among the subnormal series

$$G = G_0 \triangleright G_1 \triangleright \ldots \triangleright G_s = \{e\}$$

that satisfies $\dim G_0 > \dim G_1 \ldots > \dim G_s$.

Prop.(7.1.5.26). Any two composition series of an algebraic group $G$ has refinements that the quotients are isogenous.

Cor.(7.1.5.27) [Jordan-Holder].
Maximal Subgroup with Properties

Def. (7.1.5.28) [Good Properties]. A property of algebraic groups is called a good property s.t.
- $e$ has $P$.
- Every extension of groups with property $P$ has $P$.
- Every quotient of a group with property $P$ has $P$.

Prop. (7.1.5.29) [List of Good Properties (Not Complete)].
1. Strongly connectedness.
2. Solvability. Moreover, subgroups of solvable groups are solvable.
3. Smoothness.
4. Unipotency.
5. Affineness.
6. Connectedness.
7. Finiteness. Moreover, subgroups of finite groups are finite.
8. Unipotency. Moreover, subgroups of unipotent groups are unipotent.

Proof:
1. This follows from the isomorphism and correspondence theorems (7.1.1.33)(7.1.1.34).
2. This follows from standard argument and correspondence theorems (7.1.1.33)(7.1.1.34).
3. Let $e \to N \to G \to H \to e$ be an exact sequence of algebraic groups, then if $G$ is smooth, then so is $H$ by (7.2.1.10) and the fact $G/H$ is geo.reduced by (5.1.5.28) and (7.1.5.3). If $N, H$ are smooth, then so is $G$ by the fact smoothness is stalkwise.
4. Quotient case is clear. If $N$ is a normal subgroup of $G$ s.t. $N$ and $G/N$ are both unipotent, then (for) any non-zero linear representation $V$ of $G$, $V^N \neq 0$, and $V^N$ is stable under $G$-actions, thus $G/N$ acts on $V^N$, thus $V^G = (V^N)^{G/N} \neq 0$.
5. Notice by (7.1.1.27) and (5.1.5.29). $G \to Q$ is affine.
7. This follows from (7.1.1.28).

□

Prop. (7.1.5.30) [Maximal Group Variety Exists]. If $P$ is a good property of algebraic groups, then every algebraic group $G$ over $k$ contains a largest normal subgroup variety $H$ with property $P$. And also $G/H$ has contains no non-trivial such subgroups.

Proof: $G$ contains at least one normal subgroup variety, namely $e$. There exists a maximal such one, by taking the one with maximal dimension (because smooth varieties are reduced), then it is the largest, because if $H'$ is another, then $HH'$ is a larger one, by (7.1.5.29) and the fact $NH$ is a quotient of $N \times H$.

And if $G/H$ contains a normal subgroup variety $H'$ that has $P$, then the inverse image of $H'$ in $G$ is also a normal subgroup variety that has $P$, contradiction. □
6 Cohomology and Extensions

7.2 Group Schemes II: Solvable Groups

1 Group Actions

Remark (7.2.1.1). Group action of an group functor on an object is defined in (3.1.1.62).

Prop. (7.2.1.2) [Group Action]. An action of an algebraic group $G$ on an algebraic group $X$ is equivalent to a right $\Gamma(G)$-comodule structure on $\Gamma(X)$ as $\Gamma(G)$-modules. This action will induce a right comodule structure on $\Gamma(X)$.

The action of $G$ on itself is called the regular action of $G$.

Prop. (7.2.1.3). Let $\mu : G \times X \rightarrow X$ be an action of an group scheme $G$ on a scheme $X$, then it is faithfully flat, and it is called a smooth/finite/... action if $\mu$ is smooth/finite/..

Proof: We can see this from the commutative diagram (3.1.1.63). \(\square\)

Prop. (7.2.1.4) [Image of Equivariant Map]. Let $G$ be a group functor and $X, Y$ be non-empty algebraic schemes on which $G$ acts, and $f : X \rightarrow Y$ is an equivariant map.

- If $Y$ is reduced and $G(\overline{k})$ acts transitively on $Y(\overline{k})$, then $f$ is faithfully flat.
- If $G(\overline{k})$ acts transitively on $X(\overline{k})$, then the set $f(|X|)$ is locally closed in $|Y|$, so we can let $f(X)_{\text{red}}$ denote its reduced subscheme structure (5.4.1.14).
- If $X$ is reduced and $G(\overline{k})$ acts transitively on $X(\overline{k})$, then $f$ factors into
  
  \[ X \xrightarrow{\text{faithfully flat}} f(X)_{\text{red}} \xrightarrow{\text{immersion}} Y. \]

Moreover, $f(X)_{\text{red}}$ is stable under the action of $G$.

Proof: Cf. [Mil17] P26. \(?\)

1: 
2: 
3: $f$ factors through $f(X)_{\text{red}}$ because $X$ is reduced (5.4.1.14). Then the first assertion follows from 1 and 2. The last assertion follows from universal property again. \(\square\)

Def. (7.2.1.5) [Orbit Map]. Let $\mu : G \times X \rightarrow X$ be an action of an algebraic group $G$ on an algebraic scheme $X$. For any $x \in X(k)$, the orbit map

\[ \mu_x : G \rightarrow X : g \mapsto gx \]

is defined to be the restriction to $\mu$ to $G \times \{x\} \cong G$. The image of the orbit map is locally closed in $X$ by (7.2.1.4), and then its reduced structure subscheme is called the orbit scheme $O_x$ of $x$.

Prop. (7.2.1.6) [Fixed Subscheme]. Let $\mu : G \times X \rightarrow X$ be an action of a group functor $G$ on a separated algebraic scheme over $k$, then the functor

\[ \tilde{X}^G : R \mapsto \{ x \in X(R) | \mu(g, x_{R'}) = x_{R'}, \forall R - \text{algebra } R', g \in G(R') \} \]

is representable by a closed subscheme $X^G$ of $X$, called the fixed subscheme of this action. Then it can be seen directly that the formation of fixed subscheme commutes with extension of base fields.
Proof: An element $x \in X(R)$ defines two functors
\[ G(R') \to X(R') : g \mapsto gx_{R'} \]
\[ G(R') \to X(R') : g \mapsto x_{R'} \]
which are both natural in $R'$. Thus we get a map $X(R) \to \text{Hom}(G_R, X_R \times X_R)$ which is also natural in $R$, thus induce a map $X \mapsto \text{Hom}(G, X \times X)$.

Then there is a Cartesian diagram
\[ \begin{array}{ccc}
\tilde{X}^G & \longrightarrow & \text{Hom}(G, \Delta_X) \\
\downarrow & & \downarrow \text{closed} \\
\tilde{X} & \longrightarrow & \text{Hom}(G, X \times X)
\end{array} \]

The right vertical map is a closed subfunctor by (7.7.1.10), as $\Delta_X$ is closed in $X \times X$ because $X$ is separated. Hence $\tilde{X}^G$ is a closed subfunctor of $\tilde{X}$, thus represented by a closed subscheme of $X$, by (7.7.1.3).

Def. (7.2.1.7) [Isotropy Group]. Let $G$ be a group scheme acting on an algebraic scheme $X$, and $x \in X(k)$, then the isotropy group scheme $G_x$ is defined to be the fiber of the orbit map $\mu_x : G \to X$ over $x$.

Prop. (7.2.1.8) [Orbit Map is Faithfully Flat]. Let $\mu : G \times X \to X$ be an action of an algebraic group $G$ on an algebraic scheme $X$ and $x \in X(k)$.

- If $X$ is reduced and $G(\overline{k})$ acts transitively on $X(\overline{k})$, then the orbit map $\mu_x : G \to X$ is faithfully flat.
- If $G$ is reduced, then $O_x$ is stable under $G$, and the map $\mu_x : G \to O_x$ is faithfully flat. If $G$ is smooth, then $O_x$ is also smooth.

Proof: 1: this follows from (7.2.1.4).
2: The first statement follows from (7.2.1.4)3, and then $O_{O_x} \to \mu_x^*(O_G)$ is universally injective. Therefore if $G$ is smooth, then $O_{O_x}$ is geometrically reduced. Then $O_x$ is smooth by (7.2.1.10).

Def. (7.2.1.9) [Homogenous Space]. A non-empty algebraic scheme $X$ with an action of a group scheme $G$ is called a homogenous space for $G$ if $G(\overline{k})$ acts transitively on $X(\overline{k})$, and for any (some) $x \in X(\overline{k})$, $\mu_x$ is faithfully flat (thus surjective).

Prop. (7.2.1.10) [Smoothness for Homogenous Spaces]. If $G$ is a group scheme and $X$ is a generically geo.reduced $G$-homogeneous space, then $X$ is smooth.

Proof: By (5.6.4.21), it has an open dense smooth locus. Now smoothness can be checked after base change to alg.closed field (4.4.2.1), but then because $G(\overline{k})$ acts transitively on itself, thus all the geometric points are smooth. But geometric points are dense in $G(5.4.1.26)$, thus $G$ is smooth.
Action of Algebraic Groups

Prop. (7.2.1.11) [Homogenous Space as Quotients]. Let $\mu : G \times X \to X$ be an action of an algebraic group $G$ on a separated algebraic scheme $X$ over $k$ with a rational point $x \in X(k)$, then $(X, x)$ is a quotient of $G$ by $G_x$ iff the orbit map $\mu_x : G \to X$ is faithfully flat.

Proof: If $(X, x)$ is a quotient space, then by (7.1.1.22). Conversely, if it is faithfully flat, then clearly $\mu_x(\overline{G})$ is a fat subfunctor of $\overline{X}$, thus $X$ represents the quotient functor $\overline{G}/\overline{G}_x$. □

Cor. (7.2.1.12). Let $\mu : G \times X \to X$ be an action of a reduced algebraic group $G$ on a separated algebraic scheme $X$ over $k$ with a rational point $x \in X(k)$, then $(O_x, x)$ is a quotient space of $G$ by $G_x$.

Proof: Because $G$ is reduced, $\mu_x : G \to O_x$ is faithfully flat by (7.2.1.8), and $O_x$ is stable under the action of $G$ by (7.2.1.4), thus (7.2.1.11) applies to this case. □

Prop. (7.2.1.13). Let $\mu : G \times X \to X$ be an action of a smooth algebraic group on an algebraic scheme.

- A reduced closed subscheme $Y$ of $X$ is stable under $G$ iff $Y(\overline{k})$ is stable under $G(\overline{k})$.
- Let $Y$ be a locally closed subscheme of $X$, then if $Y$ is stable under $G$, then $(Y)_{\text{red}}$ and $(Y \setminus Y)_{\text{red}}$ is also stable under $G$.

Proof: 1: Because $G$ is geo.reduced and $Y$ is reduced, $G \times Y$ is reduced (5.4.3.2), thus $\mu : G \times Y \to X$ factors through $Y$ iff $\mu(\overline{k})$ factors through $Y(\overline{k})$.

2: $|Y|_{\text{red}}(\overline{k})$ is the closure of $Y(\overline{k})$ in $X(\overline{k})$. So as $G(\overline{k})$ acts continuously on $X(\overline{k})$, if it fixes $Y(\overline{k})$, then it also fixes $(Y)(\overline{k})$ and $(Y \setminus Y)(\overline{k})$, thus we finish by 1. □

Cor. (7.2.1.14). Let $G$ be a smooth algebraic group acting on an algebraic scheme $X$ and let $Y$ be a non-empty locally closed subscheme of $X$ stable under the action of $G$ of the smallest dimension, then it is closed.

Proof: This is because $\dim Y > \dim (Y \setminus Y)_{\text{red}}$ (Because irreducible components of $\overline{Y}$ is not contained in $\overline{Y \setminus Y}$). □

Cor. (7.2.1.15) [Orbit Lemma]. Let $G$ be a smooth algebraic group acting on an algebraic group over an alg.closed field $k$, then every orbit of minimal dimension is closed.

Proof: If $Y$ is an orbit of minimal dimension, then $(Y \setminus Y)_{\text{red}}$ is stable under $G$ and has smaller dimensions. If it is non-zero, then it contains an orbit. □

Prop. (7.2.1.16). A representation $(V, \rho)$ of an algebraic group $G$ induces an action of $G$ on the affine algebraic scheme $V_\alpha$, and also an action of $G$ on the projective algebraic scheme $P(V)$.

Prop. (7.2.1.17). Let $G \times X \to X$ be an action of an affine algebraic group $G$ on an affine algebraic scheme $X$ over $k$, then there exists a f.d. representation $(V, \rho)$ of $G$ and an equivariant closed embedding $X \hookrightarrow V_\alpha$.


Def. (7.2.1.18) [Linear Action]. A linear action of an algebraic group $G$ on an algebraic scheme $X$ is an action $(r, V)$ s.t. there exists a f.d. linear representation $(V, \rho)$ of $G$ and an equivariant non-degenerate immersion $X \hookrightarrow P(V)$. □
Prop. (7.2.1.19). If $G \times X \to X$ is a transitive action of an affine algebraic group $G$ on an algebraic variety $X$ that $X(k)$ is non-empty, then this action is linear.


Def. (7.2.1.20)[Grassmannian Variety]. The Grassmannian variety $\text{Gra}(n,k)$ is a scheme over $\mathbb{Z}$ defined to be the quotient of $GL(n)$ by the algebraic subgroup $B$ fixing a subspace of dimension $k$ (7.1.1.21).

The Grassmannian varieties are projective by (7.7.2.16).

Remark (7.2.1.21). For an explicit construction of $\text{Gra}(n,k)$, Cf. [Sta]089T or [Nit05]P6.

Def. (7.2.1.22)[Flag Varieties]. The flag variety is a scheme over $\mathbb{Z}$ defined to be the quotient of $GL_n$ by the algebraic subgroup $B_F$ fixing a flag (7.1.1.21).

The flag varieties are projective by (7.7.2.19).

Prop. (7.2.1.23)[An Algebraic Theorem]. Let $F$ be a local field and $X$ is an algebraic variety over $F$, then the $F$-topology makes $X(F)$ into a locally profinite space (because varieties are closed, and use (3.6.4.6)). Let $G$ be a linear algebraic group over $F$ and $G \times X \to X$ is a $F$-rational map, then $G(F) \times X(F) \to X(F)$ is a continuous action, and this action is constructible (3.8.1.21).

Proof: Cf. [Bernstein-Zelevinsky, Appendix]. □

Prop. (7.2.1.24)[Projectivity of Quotient Spaces]. How to generally prove that a quotient space is projective?

2 Lie Algebras of Algebraic Groups

In this subsection, all algebraic groups $G$ is affine over a field $k$.

Def. (7.2.2.1)[Lie Algebra of an Algebraic Group]. Let $k$ be a field and $G$ a locally algebraic group, then the tangent space at the unit element $e \subset G$ define by (5.6.4.25) is isomorphic to

$$L(G) = \ker(G(k[\varepsilon]) \to G(k)), \varepsilon^2 = 0.$$ as a vector space. For any homomorphism $f : G \to H$, there is a Lie algebra map

$$\text{Lie}(f) : \text{Lie}(G) \to \text{Lie}(H)$$ induced by $f$.

In particular, if $G$ is affine, it is the set of homomorphisms $\Gamma(G) \to k[\varepsilon]$ that the composition with $k[\varepsilon] \to k$ is the counit map $\varepsilon : \Gamma(G) \to k(7.1.1.2)$.

If $G$ is affine, $\varphi$ maps the augmentation ideal $I_G = \ker(\varepsilon)$ into $(\varepsilon)$, and thus is trivial on $I_G^2$. So $\varphi$ factors through $\Gamma(G)/I_G^2$. Now $\Gamma(G)/I_G^2 \cong k \oplus I_G/I_G^2$ by (2.9.2.11), so

$$L(G) \cong \text{Hom}_k(I_G/I_G^2, k).$$ And we define Lie($G$) to be $L(G)$.

In general, if $R$ is any $k$-algebra, then we define $g(R) = \ker(G(R[\varepsilon]) \to G(R))$, then similarly

$$g(R) = \text{Hom}_R(I_R/I_R^2, R) = \text{Hom}_k(I_G/I_G^2, k) \otimes R = g \otimes R.$$
Now \( G(\mathbb{R}[\varepsilon]) \) acts on \( \mathfrak{g}(\mathbb{R}) \) by inner automorphism, so also does \( G(\mathbb{R}) \). So we get a homomorphism of algebraic groups

\[
\text{Ad} : G \to \text{GL}(\mathfrak{g}).
\]

This homomorphism commutes with Lie algebra homomorphism: If \( f : G \to H \) is a homomorphism of algebraic groups, then there is a commutative diagram

\[
\begin{array}{ccc}
G \times \mathfrak{g} & \xrightarrow{(x,X)\mapsto \text{Ad}(x)X} & \mathfrak{g} \\
\downarrow f & & \downarrow \text{Lie}(f) \\
H \times \mathfrak{h} & \xrightarrow{(y,Y)\mapsto \text{Ad}(y)Y} & \mathfrak{h}
\end{array}
\]

Then we define a Lie bracket on \( \mathfrak{g} \) as follows: \( [X,Y] = \text{ad}(X)(Y) = \text{Lie}(\text{Ad})(X)(Y) \). Then this is a Lie algebra structure on \( \mathfrak{g} \), and it commutes with arbitrary base change.

**Proof:** To verify this is truly a Lie algebra, we take a faithful embedding of \( G \) into some \( GL_V(15.3.1.22) \). Thus it suffices to prove the Lie algebra of \( GL_V \) is a Lie algebra. Now for \( A, B \in M_n(\mathbb{R}) \), pondering the definition shows

\[
(1 + \delta A)(1 + \varepsilon B)(1 - \delta A) = 1 + \varepsilon B + \varepsilon \delta [X,Y] \in k[\varepsilon, \delta]/(\varepsilon^2, \delta^2).
\]

So in fact \( [X,Y] = XY - YX \), so it is truly a Lie algebra.

To show the group structure on \( \text{Lie}(G) \) equals the structure on the tangent space, use the Eckmann-Hilton argument, notice the hypothesis is satisfied because both composition is the morphism \( \text{Spec} k[\varepsilon] \to \text{Spec}(k[\varepsilon] \otimes k[\varepsilon]) \xrightarrow{\varphi} G \times G \xrightarrow{\mu} G \), where \( \varphi = (a,b,c,d) : k[\varepsilon] \otimes k[\varepsilon] \xrightarrow{\varphi} G \times G \).

**Cor.(7.2.2.2)[Exponential Map].** As there are natural isomorphisms \( \mathfrak{g}(\mathbb{R}) \cong \mathfrak{g} \otimes \mathbb{R} \), we can write \( e^{\varepsilon X} \) the element of \( \mathfrak{g}(\mathbb{R}) \subset G(\mathbb{R}[\varepsilon]) \) corresponding to \( X \in \mathfrak{g} \times \mathbb{R} \). Then \( e^{\varepsilon X + \varepsilon Y} = e^{\varepsilon X} e^{\varepsilon Y} \), and by functoriality, for any homomorphism \( f : G \to H \),

\[
f(e^{\varepsilon X}) = e^{\varepsilon \text{Lie}(f)(X)}.
\]

Also

\[
x \cdot e^{\varepsilon Y} x^{-1} = e^{\varepsilon \text{Ad}(x)Y}
\]

and also the commutative diagram in (7.2.2.1) means

\[
f(e^{\varepsilon X}) = e^{\varepsilon \text{Lie}(f)(X)}.
\]

**Cor.(7.2.2.3)[Lie algebra commutes with Limits].** It can be seen from the definition that the Lie algebra construction commutes with limits of algebraic groups. In particular it commutes with kernel map.

**Prop.(7.2.2.4).** Let \( H \subset G \) be algebraic groups s.t. \( \text{Lie}(H) = \text{Lie}(G) \). If \( H \) is smooth and \( G \) is connected, then \( H = G \).

**Proof:** Recall that \( \dim \mathfrak{g} \geq \dim G \), with equality iff \( G \) is smooth(7.1.4.5), so the condition forces \( G \) to be smooth. Now \( G \) is smooth and connected thus irreducible(7.1.4.14) and \( \dim G = \dim H \), so \( H = G \).
Cor. (7.2.2.5). Let $H_1, H_2$ be connected algebraic subgroups of $G$ and $H_1 \cap H_2$ is smooth. If $\text{Lie}(H_1) = \text{Lie}(H_2)$, then $H_1 = H_2$.

Cor. (7.2.2.6). If $G$ is an algebraic group over a field of characteristic 0, then the connected subgroups of $G$ correspond to Lie subalgebras of $\text{Lie}(G)$, because every subgroup is smooth, by (7.1.4.2).

Cor. (7.2.2.7). Let $H_i$ be a family of smooth algebraic subgroups of an algebraic subgroup $G$ over a field $k$. If $\text{Lie}(H_i)$ generate $\text{Lie}(G)$ as a Lie algebra, then $H_i$ generates $G$ (7.1.4.26).

Proof: Let $H$ be the subgroup they generate, then $H$ is smooth (7.1.4.26) and $\text{Lie}(H) = \text{Lie}(G)$, thus $H = G$ by (7.2.2.4).

Stabilizers, Centers and Centralizers

Prop. (7.2.2.8) [Lie Algebra of Stabilizer]. Let $G$ be an algebraic group and $(V, r)$ be a representation of $G$, then it induces an action of $\mathfrak{g}$ on $W$ (7.2.2.1). Let $W \subset V$ be a subspace, then the stabilizer $\text{Stab}_G(W)$ is a subgroup of $G$ (15.3.1.3)

$$\text{Lie}(\text{Stab}_G(W)) = \text{Stab}_\mathfrak{g}(W).$$

In particular, $\dim(\text{Stab}_G(W)) \leq \dim \text{Stab}_\mathfrak{g}(W)$, with equation iff $\text{Stab}_G(W)$ is smooth.

Proof: By (7.2.2.2),

$$X \in \text{Lie}(\text{Stab}_G(W)) \iff r(e^\varepsilon X) W[\varepsilon] \subset W[\varepsilon] \iff e^\varepsilon \text{Lie}(r(X)) W_R[\varepsilon] \subset W_R[\varepsilon] \iff (1 + \varepsilon \text{Lie}(r(X)))(W_R + \varepsilon W_R) \subset (W_R + \varepsilon W_R) \iff \text{Lie}(r(X))(W_R) \subset W_R \iff X \subset \text{Stab}_\mathfrak{g}(W)$$

Prop. (7.2.2.9) [Lie Algebra of Center]. Let $G$ be a smooth connected algebraic group, then

$$\dim z(\mathfrak{g}) \geq \dim Z(G),$$

and if equality holds, then $Z(G)$ is smooth and $\text{Lie}(Z(G)) = z(\mathfrak{g})$.

Proof: There are maps

$$\text{Ad} : G \mapsto GL_\mathfrak{g}, Z(G) \subset \ker(\text{Ad}),$$

$$\text{ad} : \mathfrak{g} \mapsto \mathfrak{gl}_\mathfrak{g}, \ker(\text{ad}) = z(\mathfrak{g}).$$

Because Lie algebra commutes with kernel (7.2.2.3), $\text{Lie}(Z(G)) \subset \text{Lie}(\ker(\text{Ad})) = \ker(\text{ad})$. So

$$\dim z(\mathfrak{g}) = \dim \ker(\text{ad}) = \dim \text{Lie}(\ker(\text{Ad})) \geq \dim \ker(\text{Ad}) \geq \dim Z(G)$$

with equality iff $\ker(\text{Ad})$ is smooth and $\dim \ker(\text{Ad}) = \dim Z(G)$ and thus $\ker(\text{Ad})^0 = Z(G)^0$, so $Z(G)$ is also smooth. Finally, $\text{Lie}(Z(G)) \subset z(\mathfrak{g})$, so they are equal if they have the same dimensions.

□
Prop. (7.2.2.10) [Lie Algebra of Centralizer]. Let $G$ be an algebraic group and $H$ a subgroup, then $H$ acts on $\mathfrak{g}$ by $\text{Ad}$. Then

$$\text{Lie}(C_G(H)) = \mathfrak{g}^H, \quad \text{Lie}(N_G(H))/\text{Lie}(H) = (\text{Lie}(G)/\text{Lie}(H))^H.$$  

Proof: 

$$X \in \text{Lie}(C_G(H)) \iff x(e^{e_x}Sx^{-1} = e^{e_x}, \quad \forall k[\varepsilon] \to S, x \in H(S)$$  

And it can be shown these two are equal. Similarly, there is a natural map $\text{Lie}(N_G(H)) \to \text{Lie}(G)/\text{Lie}(H)$, and the image lies in the fixed subgroup of $H$, because

$$X \in \text{Lie}(N_G(H)) \iff (e^{e_x}Sx(e^{e_x}S)^{-1} \subset H(S) \iff e^{e_{\text{ad}(x)}X}S \in H(S)e^{e_x}S, \quad \forall k[\varepsilon] \to S, x \in H(S)$$  

$$X \in (\text{Lie}(G)/\text{Lie}(H))^H \iff e^{e_{\text{ad}(x)}X}R \subset e^{e_{X}}(R+\text{Lie}(H)(R)) \quad \forall k \to R, x \in H(R)$$

Then it can be shown that $X$ satisfies condition in 1 iff $\overline{X}$ satisfies condition in 2, thus we are done. \qed

3 Groups of Multiplicative Type

Throughout this subsection, $G$ is an affine(linear) algebraic group over a field $k$.

Diagonalizable Groups

Def. (7.2.3.1) [Diagonalizable Groups]. An algebraic group $G$ is called diagonalizable if the group-like elements in $\Gamma(G)$ generate $\Gamma(G)$ as a $k$-vector space.

Prop. (7.2.3.2). An algebraic group $G$ is diagonalizable iff it is isomorphic to the the algebraic group corresponding to a group algebra $D(M)$ for some commutative group $M$.

Proof: For the group algebra $D(M)$, its group-like elements are just $\{m|m \in M\}$ by (2.9.2.21), and they clearly span $D(M)$. Conversely, if the set $M$ of group-like elements in $\Gamma(G)$ spans $\Gamma(G)$, then by(2.9.2.20) they form a basis of $\Gamma(G)$, so there is an isomorphism of vector spaces $D(M) \to \Gamma(G)$. But this is also a homomorphism, because they are on a basis. \qed

Cor. (7.2.3.3) [Diagonalizable Groups].

- The functor $M \mapsto D(M)$ is a contravariant equivalence from $\mathcal{C}\mathbb{A}lg_k^fg$ to the category of diagonalizable algebraic groups, with inverse give by $G \mapsto X(G)$.

- This functor preserves exact sequences.

- Algebraic subgroups and quotient groups of diagonalizable groups are diagonalizable.

Proof: 1: By(7.2.3.2), it suffices to show that $\text{Hom}(M, M') \to \text{Hom}(D(M'), D(M))$ is an isomorphism. Because $D$ sends direct sums to direct products, it suffices to check the case that $M, M'$ is cyclic. This is easy to check, just notice that a group homomorphism maps group-like elements to group-like elements.

2: If $M' \to M$ is injective, then $k[M'] \to k[M]$ is injective, thus faithfully flat by(2.9.2.23), and $D(M) \to D(M')$ is a quotient map. Conversely, $D(M) \to D(M')$ is a quotient map iff $k[M'] \to k[M]$ is faithfully flat thus injective thus $M' \to M$ is injective. Now the kernel of $D(M) \to D(M')$
is represented by $k[M]/I_k[M']$, where $I_k[M']$ is the augmentation ideal. Then it is isomorphic to \( k[M/M'] \).

3: Let $H$ be an algebraic subgroup of $G$, then the map $\Gamma(G) \to \Gamma(H)$ is surjective, and sends group-like elements to group-like elements, thus $\Gamma(H)$ is also spaned by group-like elements, and $H$ is diagonalizable.

if $D(M) \to Q$ is a quotient map, then its kernel is an algebraic subgroup thus equals $D(M'')$ for some quotient $M''$ of $M$. Let $M$ be the kernel of $M \to M''$, then $D(M) \to D(M')$ and $D(M) \to Q$ are quotient maps with the same kernel, so they are isomorphic, by (7.1.1.24).

Prop. (7.2.3.4) [Representation of Diagonalizable Groups]. The following conditions are equivalent for an algebraic group $G$ over a field $k$:

1. $G$ is diagonalizable.
2. Every representation of $G$ is diagonalizable.
3. Every f.d. representation of $G$ is diagonalizable.

Proof:  
1 $\to$ 2: We need to show for any comodule $\rho : V \to V \otimes \Gamma(G)$, $V$ is a sum of 1-dimensional representations, or equivalently, it is spanned by vectors $u$ that $\rho(u) \in ku \otimes \Gamma(G)$. Let $v \in V$, we can write $\rho(v) = \sum u_i \otimes e_i$ where $e_i$ are group-like in $G$.

Applying comodule relations, we get
\[
\sum u_i \otimes e_i \otimes e_i = \sum \rho(u_i) \otimes e_i, \quad v = \sum u_i(2.9.219).
\]
so $\rho(u_i) = u_i \otimes e_i$ and they span $V$.

2 $\to$ 1: The regular representation of $G$ is diagonalizable, so $\Gamma(G)$ is spanned by its eigenvectors, for any eigenvector $f \in \Gamma(G)$, so $\mu(f) = f \otimes e$ where $e$ is group-like. Applying $\varepsilon \otimes \text{id}$ shows $f = \varepsilon(f)e$, so $G$ is diagonalizable.

2 $\to$ 3: trivial.

3 $\to$ 2: Every representation of $G$ is a sum of f.d. representation, so it is a sum of 1-dimensional representations, so it is diagonalizable by (15.3.1.17). \qed

Tori

Def. (7.2.3.5) [Linear Tori]. Let $k$ be a field, then a split torus over $k$ is a linear group scheme of the form $T = G_{m,k}^n$, and a linear torus over $k$ is defined to be a linear algebraic group $T$ over $k$ that $T_k^* \cong \text{split torus over } \bar{k}$.

Prop. (7.2.3.6). By (7.2.3.3), a split torus is just $D(\mathbb{Z}^n)$ for some $n$, and quotient of a split torus is a split torus.

Thus a quotient of a torus is a torus, and an algebraic subgroup of a torus is a torus iff it is a group variety.

Prop. (7.2.3.7). Any torus over a separably closed field is a split torus. in particular, any torus split over a finite separable extension.

Proof: \qed
Def.(7.2.3.8)[Quasi-Split Tori]. Let \( A \) be a f.d. separable \( k \)-algebra, then there is a linear algebraic group \( G \) defined by \( G(B) = G_m(A \otimes_k B) = (A \otimes_k B)^* \), denoted by \( \text{res}_{A/k} G_m \).

This is a linear algebraic group because if we choose a basis \( \{v_1, \ldots, v_r\} \) of \( A \) over \( k \), which induces a ring homomorphism \( \phi : A \to M_r(k) \). Then \( f = \det(\phi(x_1v_1 + \ldots + x_r v_r)) \) is a polynomial in \( x_1, \ldots, x_r \). Thus \( G(B) \) is the set of points in \( A^r \) that \( f(x_1, \ldots, x_r) \) is invertible in \( B \). So \( G \) is a linear algebraic variety. Moreover, as \( A \) is separable, \( A \otimes_k k \cong \bigoplus_{i=1}^r M_{n_i}(k) \), so \( G_k \cong G^r_{n, k} \), so \( G \) is a torus, called a \textbf{quasi-split torus} over \( k \).

Def.(7.2.3.9)[Monoidal Transformation]. For a matrix \( A \in \text{SL}(n, \mathbb{Z}) \) with \( \det A = \pm 1 \), we define an isomorphism of \( G_{n, k} \):

\[
\varphi_A(x) = (x_1^{a_{11}} x_2^{a_{12}} \ldots x_n^{a_{1n}}, \ldots, x_1^{a_{n1}} \ldots x_n^{a_{nn}}).
\]

these isomorphisms \( \varphi_A \) is called the \textbf{monoidal transformations}.

Prop.(7.2.3.10). Let \( G \) be a group variety over \( k \) and \( T \) a central torus, then

- \( T \cap [G, G] \) is finite.
- If \( G/T \) is perfect, then the sequence

\[
e \to T \cap [G, G] \to T \times [G, G] \to G \to e
\]

is exact.

In particular, \( G/[G, G] \) is a torus.

Proof: Cf.[Mil17]P246.

Groups of Multiplicative Type

Def.(7.2.3.11)[Groups of Multiplicative Type]. An algebraic group of multiplicative type over a field \( k \) is an algebraic group \( G \) that \( G_K \) is diagonalizable over \( K \) for some field \( K \) containing \( k \).

Subgroups and quotient groups of groups of multiplicative type are also of multiplicative type, because this is true for diagonalizable groups(7.2.3.3).

Prop.(7.2.3.12)[Characterization of Groups of Multiplicative Type]. The follows are equivalent for an algebraic group \( G \) over \( k \):

- \( G \) is of multiplicative type.
- \( G \) is commutative and \( \text{Hom}(G, G_{a}) = 0 \).
- \( G \) is commutative and \( \Gamma(G) \) is coétale.
- \( G \) becomes diagonalizable over \( k^s \).

Proof: Cf.[?]237.

Cor.(7.2.3.13). An algebraic group over \( k \) becomes diagonalizable over some field extension of \( k \) iff it becomes diagonalizable over some finite separable extension of \( k \).

Cor.(7.2.3.14). If a group of multiplicative type splits over a purely inseparable extension of \( k \), then it splits over \( k \).
\textbf{Cor.(7.2.3.15).} A smooth commutative algebraic group $G$ over $k$ is of multiplicative type iff $G(\overline{k})$ consists of semisimple elements.

\textit{Proof:} We can assume that $k = \overline{k}$, and embed $G$ into $GL_n$ for some $n(15.3.1.22)$. If $G$ is of multiplicative type, then by(7.2.3.4), there is a basis that $G \subset D_n$, so all the elements in $G(k)$ is diagonalizable hence semisimple. Conversely, if $G(k)$ are all semisimple, then they form a commutative family of semisimple elements, so $G(k) \subset D_n(k)$ in some basis. Because $G$ is smooth thus reduced, $G \subset D_n$. \hfill \Box

\textbf{Cor.(7.2.3.16).} An extension of algebraic groups of multiplicative type is of multiplicative type iff it is commutative.

\textit{Proof:} A exact sequence $e \to G' \to G \to G'' \to e$ of commutative group schemes gives rise to an exact sequence

$$0 \to \text{Hom}(G'', G_a) \to \text{Hom}(G, G_a) \to \text{Hom}(G', G_a)$$

of Abelian groups by(7.1.1.24), thus we can use characterization(7.2.3.12). \hfill \Box

\textbf{Prop.(7.2.3.17)[Largest Subtorus].} Cf.[Mil17]P241.

\textbf{Prop.(7.2.3.18)[Representation of Groups of Multiplicative Type].} Let $G$ be an algebraic group over $k$, then Rep($G$) is a semisimple Abelian category, and the isomorphism classes of simple objects in Rep($G$) are classified by the orbits of $G(k^s/k)$ acting on $X^*(G)$.

Let $(V, r)$ be a representation corresponding to an orbit $\Sigma$, and let $\chi \in \Sigma$, then $\text{End}(V, r) \cong k_\chi$, where $k_\chi$ is the subfield of $k^s$ fixed by the subgroup of $G(k^s/k)$ fixing $\chi$.

\textit{Proof:} The group $G$ is split by a finite Galois extension $K/k$ by(7.2.3.13). Let $\Gamma = G(K/k)$, then $\Gamma$ acts on $\Gamma(G_K)$ through its action on $K$. Let $(V, r)$ be a representation of $G_K$ and let $\rho$ be the corresponding co-action, then by(5.1.5.24), the functor $V \mapsto V \otimes_k K$ induces an equivalence between Rep($G$) and Rep($G_K$) with a semi-linear action of $\Gamma$ fixing $\rho$.

Let $V$ be a representation of $G$ over $k$, then $K \otimes V$ decomposes as a representation of $G_K$ into

$$K \otimes V = \oplus_{\chi \in X(G_K)} V_\chi.$$ 

and an element $\gamma \in \Gamma$ maps $V_\chi$ isomorphically onto $V_{\sigma \chi}$. Thus the set of $\chi$ occurring in $K \otimes V$ is stable under the action of $\Gamma$.

Conversely, if $\Sigma$ is an orbit of $\Gamma$ in $X(G_K)$ and $V$ is a 1-dimensional $K$ vector space, then $\oplus_{\chi \in \Sigma} V_\chi$ has a natural semi-linear action of $\Gamma$, so it arises from a simple representation of $G$ over $k$. \hfill \Box

\textbf{Prop.(7.2.3.19)[Density Theorem for Groups of Multiplicative Type].} Let $G$ be a smooth algebraic group of multiplicative type, thus $G$ is commutative. Let $G_n$ be the kernel of multiplication by $n$ on $G$.

- The only closed subscheme containing every $G_n$ is $G$ itself.

- If $G$ is smooth, then the only closed subscheme containing $G_n$ for $n$ prime to characteristic of $k$, is $G$ itself.

\textit{Proof:} 1: 2: Cf.[Mil17]P242. \hfill \Box
Cor. (7.2.3.20). Let \( G \) be an algebraic group of multiplicative type. If two homomorphisms from \( G \) to another algebraic group \( H \) coincides on \( G_n \) for all \( n \geq 1 \), then they are equal.

Proof: This is because the equalizer is a closed subscheme of \( G \), as \( H \) is separated (7.1.1.12). □

Prop. (7.2.3.21) [Rigidity Theorem for Groups of Multiplicative Type]. Let \( G, H \) be diagonalizable groups over \( k \), and let \( X \) be a connected group scheme over \( k \). Let \( \varphi : X \times G \to H \) be a morphism that for all \( k \)-algebra \( R \) and \( x \in X(R) \), the map \( g \mapsto \varphi(x, g) : G(R) \to H(R) \) is a homomorphism. Then for any \( x_0 \in X(k) \), we have \( \varphi(x, g) = \varphi(x_0, g) \) for any \( k \)-algebra \( R \) and \( (x, g) \in X(R) \times G(R) \).


Cor. (7.2.3.22). Every action of a connected algebraic group \( G \) on an algebraic group \( H \) of multiplicative type by group homomorphisms is trivial.

Cor. (7.2.3.23). Every normal algebraic subgroup of multiplicative type of a connected algebraic group \( G \) is contained in the center of \( G \).

Proof: The action of \( G \) on \( N \) by inner automorphism is trivial. □

Cor. (7.2.3.24). Let \( H \) be a subgroup of multiplicative type of an algebraic group \( G \), then \( N_G(H)^0 = C_G(H) \), i.e. \( C_G(H) \) is an open subgroup of \( N_G(H) \).

Proof: The inner action of \( N_G(H)^0 \) on \( H \) by inner automorphism is trivial. □

Cor. (7.2.3.25). If \( N \) is a normal subgroup of an algebraic group \( H \) that \( N \) and \( H/N \) are of multiplicative type, then every action of a connected algebraic group \( G \) on \( H \) by group homomorphisms preserving \( N \) is trivial.

Proof: The action of \( G \) on \( N \) is trivial, thus the action factors through \( G \times H/N \to H \), thus also factors through \( G \times H/N \to N \). Now the action is trivial, by (7.2.3.21). □

Cor. (7.2.3.26). An extension of algebraic groups of multiplicative type is of multiplicative type if it is connected.

Proof: The adjoint action of \( G \) is trivial, by (7.2.3.25), thus \( G \) is commutative. Thus it is of multiplicative type by (7.2.3.16). □

4 Actions of Tori

Prop. (7.2.4.1) [Białyńcki-Birula Decomposition]. Cf. [Mil17]P272.

5 Solvable Groups

All group schemes \( G \) in this subsection are affine and algebraic over a field \( k \).

Prop. (7.2.5.1). Let \( H \) be an algebraic group of a solvable group variety \( G \), then \( G/H \) doesn’t contain a proper subscheme of dimension \( > 0 \). In particular, \( G = H \) if \( G/H \) is proper.

Cor. (7.2.5.2). If $G$ is a solvable group variety acting on a separated algebraic scheme $X$ over $k$, then no orbits of $X$ contains a proper subscheme of dimension $> 0$.

Proof: By (7.2.1.12), the orbits are quotients of $G$. □

Cor. (7.2.5.3) [Borel Fixed Point Theorem]. If $G$ is a solvable group variety acting on a proper algebraic scheme $X$ over $k$, then $X^G \neq \emptyset$, in particular, $X^G(\overline{k}) \neq \emptyset$.

Proof: It suffices to change to $\overline{k}$, then by (7.2.1.15) $X$ has a closed orbit, which is then proper, thus must be a point. □

Triangularizable Algebraic Groups

Def. (7.2.5.4) [Triangularizable Algebraic Groups]. A triangularizable algebraic group is an algebraic group s.t. every simple representation has dimension 1. Equivalently, for any f.d. linear representation $V$ of $G$, there exists a basis that $G$ is mapped into $B(n)$.

Prop. (7.2.5.5) [Lie-Kolchin]. Let $G$ be a solvable group variety over an alg.closed field $k$, then $G$ is triangularizable. In particular, any solvable group variety over $k$ is a triangularizable after a finite field extension.

Proof: Let $(V, r)$ be any linear representation of $G$, then $G$ acts on the maximal flag variety of $V$. Thus by Borel's fixed point theorem (7.2.5.3), there is a flag in $V$ that is fixed by $G$, which means $G$ is mapped into $U(V)$. □

Nilpotent Algebraic Groups
7.3  Group Theory III: Reductive Groups

All group schemes $G$ in this section are assumed to be linear algebraic over a base scheme $S$. Main references are [Mil17]. For relative reductive group schemes, Cf.[reductive group schemes, Conrad].

1  Borel Subgroups

Def.(7.3.1.1)[Borel Subgroups]. A Borel subgroup of a group variety $G$ is a maximal solvable subgroup variety of $G$. A Borel pair is a pair $(B, T)$ where $B$ is a Borel subgroup of $G$ and $T$ is a maximal torus of $G$ contained in $B$.

Def.(7.3.1.2)[Parabolic Subgroups]. A parabolic subgroup $P$ of a group variety $G$ is a subgroup variety s.t. $G\lhd P$ is proper.

Prop.(7.3.1.3) [Parabolic and Borel]. Parabolic subgroups are exactly those containing a Borel subgroup. In particular, if $B$ be a Borel subgroup of $G$, then $G\lhd B$ is proper.


Prop.(7.3.1.4) [Characterizing Borel Subgroups]. Let $G$ be a group variety over $k$, then a subgroup $B$ is Borel iff it is solvable and $G/B$ is proper.

Prop.(7.3.1.5) [Borel Pairs are Conjugate]. Let $G$ be a group variety over $k$, then

- Any two Borel subgroups of $G$ are conjugate by an element of $G(k)$.
- Any two maximal tori of $G$ are conjugate by an element of $G(k)$.
- Any two Borel pairs are conjugate by an element of $G(k)$.

Proof: Cf.[Mil17]P354.? 3: This follows from the first two(by applying item2 on a Borel subgroup $B$). □

Def.(7.3.1.6)[Split Group Variety]. A split group variety is a group variety whose Borel subgroup is split solvable.

Def.(7.3.1.7)[Cartan Subgroup]. A Cartan subgroup of a group variety is the centralizer of a maximal tori.

2  Geometric Aspects

Def.(7.3.2.1)[Simply Connected Groups]. A simply-connected group variety is a group variety $G$ that every multiplicative isogeny(7.1.5.16) from a group variety $G' \to G$ is an isomorphism.

Prop.(7.3.2.2)[Lifting]. Let $G$ be a simply connected group variety over $k$ and $\varphi : G' \to G$ is a multiplicative isogeny, then $\varphi$ admits a section if $k$ is perfect or $G$ is a perfect group.

Proof: Cf.[Mil17]P388. □

Def.(7.3.2.3)[Universal Covering]. A universal covering of a group variety $G$ is a multiplicative isogeny $\pi : G' \to G$ from a simply connected group variety $G'$. If such a covering exists, ker $\pi$ is called the fundamental group $\pi_1(G)$ of $G$. 
Prop. (7.3.2.4) [Galois Theory]. Let \( \tilde{G} \to G \) be a universal covering of a group variety over \( k \). If \( k \) is perfect or \( G \) is perfect, then \( \pi \) factors uniquely through any other multiplicative isogeny of group varieties \( G' \to G \).

\textbf{Proof}: As \( \tilde{G} \) is a group variety, it admits no finite quotient (7.1.5.14), thus if \( [G, G] = G \), then \( [\tilde{G}, \tilde{G}] \) \( \ker \pi = \tilde{G} \), thus \( G/[G, G] \) is finite, thus trivial, so \( \tilde{G} \) is also perfect.

The map \( G' \times \tilde{G} \) is surjective with finite kernel of multiplicative type, thus it has a section by (7.3.2.2), and the composite of this section with projection to \( G' \) is the desired lifting. If \( \alpha, \beta \) are two liftings, then \( \alpha \subset \beta \) is a map from \( \tilde{G} \) to \( \ker(\varphi) \), which is finite, thus \( \alpha = \beta \). \( \square \)

Prop. (7.3.2.5). Every semisimple algebraic group admits an essentially unique isogeny \( \tilde{G} \to G \) that \( \tilde{G} \) is simply connected.

\textbf{Proof}: \( \square \)

3 Reductive Groups

In this subsection, \( k \) is a field.

Linearly Reductive Groups

Def. (7.3.3.1) [Linearly Reductive Groups]. An algebraic group over a field is called \textbf{linearly reductive} if every f.d. representation of \( G \) is semisimple.

Prop. (7.3.3.2). Let \( G \) be an algebraic group over \( k \), and \( k' \) a field containing \( k \). If \( G_{k'} \) is linearly reductive, then so is \( G \). Conversely, if \( G \) is linearly reductive and \( k' \) is separable over \( k \), then \( G_{k'} \) is linearly reductive.

\textbf{Proof}: Cf. [Mil17]P248. \( \square \)

Prop. (7.3.3.3). A commutative algebraic group is linearly reductive iff it is of multiplicative type.

\textbf{Proof}: Cf. [Mil17]P248. \( \square \)

Prop. (7.3.3.4) [Hilbert]. Let \( G \) be a linearly reductive group of \( GL(n) \) and let \( A = k[T_1, \ldots, T_n] \), then \( A^G \) is f.g. as a \( k \)-algebra.

\textbf{Proof}: Cf. [Mil17]P249. \( \square \)

Semisimple Groups

Def. (7.3.3.5) [Radicals]. The \textbf{radical} \( R(G) \) of an algebraic group \( G \) over a field \( k \) is the largest smooth connected solvable normal subgroup of \( G \), which exists by (7.1.5.29) and (7.1.5.30).

\( G \) is called a \textbf{semisimple algebraic group} iff it is an affine group variety and \( R(G_{\overline{k}}) = e \).

Prop. (7.3.3.6). Let \( k'/k \) be a field extension, then an algebraic group \( G \) over \( k \) is semisimple iff \( G_{k'} \) is semisimple.

\textbf{Proof}: Affineness, Smoothness and geo.connectedness satisfies field descent by (5.1.5.26), so it suffices to prove for \( k'/k \) alg.closed. But if \( N \) is non-trivial normal solvable subgroup variety of \( G_{k'} \), it is defined on a f.g. field extension \( K = k(x_1, \ldots, x_n) \) of \( k \), thus \( N_K \) is a normal solvable subgroup variety of \( G_K \), and they extends to smooth group varieties \( \tilde{G} \) and \( N' \) on some open subscheme \( Spec A \subset Spec k[x_1, \ldots, x_n] \). But on some maximal ideal \( \mathfrak{m} \), \( N_{k(\mathfrak{m})} \) is non-zero (4.2.6.11) normal open subgroup of \( \tilde{G}_{k(\mathfrak{m})} \), and \( k(\mathfrak{m}) \cong k = \mathfrak{F} \), contradiction. \( \square \)
Prop. (7.3.3.7). If \( k'/k \) is a separable algebraic extension, then \( R(G_{k'}) = R(G)_{k'} \).

Proof: \( R(G)_{k'} \subset R(G_{k'}) \) by definition, and it suffices to prove they are the same when \( k'/k \) is Galois. But then this follows from Galois descent (5.1.5.19) and the fact connectedness, smoothness, normality and solvability is reflexive (7.1.5.21).

□

Cor. (7.3.3.8). Let \( G \) be a group variety over a perfect field \( k \), then \( G \) is semisimple iff \( R(G) = e \). In particular, \( G/R(G) \) is semisimple, by (7.1.5.30).

Cor. (7.3.3.9). Let \( G \) be a group variety over a perfect field \( k \), then \( G \) is semisimple iff it contains no non-trivial commutative normal subgroup varieties.

Def. (7.3.3.10) [Simple Groups]. A simple algebraic group is a semisimple non-commutative group with no non-trivial normal algebraic subgroups.

An almost-simple algebraic group is a semisimple non-commutative group s.t. every non-trivial normal algebraic subgroup is finite.

A geometrically (almost-)simple algebraic group is an algebraic group \( G \) s.t. \( G_{\overline{k}} \) is (almost-)simple.

A(n) (almost-)pseudo simple algebraic group is a non-commutative group variety \( G \) s.t. every non-trivial normal algebraic subgroup is trivial (finite). (May not by semisimple).

Reductive Groups

Def. (7.3.3.11) [Unipotent Radicals]. By (7.1.5.29) and (7.1.5.30), any algebraic group \( G \) has a maximal connected smooth normal unipotent subgroup \( R_u(G) \), which is called the unipotent radical of \( G \), denoted by \( R_u(G) \).

Let \( G \) be an affine group variety over \( k \), then \( G \) is called a reductive group iff \( R_u(G_{\overline{k}}) = e \).

\( G \) is called a pseudo-reductive group if \( R_u(G) = e \).

Prop. (7.3.3.12). Let \( k'/k \) be a field extension, then an algebraic group \( G \) over \( k \) is reductive iff \( G_{k'} \) is reductive.

Proof: The proof is verbatim as that of (7.3.3.6).

□

Prop. (7.3.3.13). If \( k'/k \) is a separable algebraic extension, then \( R_u(G_{k'}) = R_u(G)_{k'} \).

Proof: \( R(G)_{k'} \subset R(G_{k'}) \) by definition, and it suffices to prove they are the same when \( k'/k \) is Galois. But then this follows from Galois descent (5.1.5.19) and the fact connectedness, smoothness, normality and unipotency is reflexive (15.3.3.2).

□

Cor. (7.3.3.14). Let \( G \) be a group variety over a perfect field \( k \), then \( G \) is reductive iff \( R_u(G) = e \). In particular, \( G/R_u(G) \) is reductive, by (7.1.5.30).

Prop. (7.3.3.15). Let \( G \) be a reductive group, then

- the center \( Z(G) \) is of multiplicative type.
- \( R(G) \) is the largest subtorus of \( Z(G) \).
- \( R(G_{k'}) = R(G)_{k'} \) for any field extension \( k'/k \).
- \( G/R(G) \) is semisimple.
- \( G/Z(G) \) has trivial center.
• $Z(G) \cap [G,G]$ is finite.


4: This is because $(G/R(G))_{k'} = G_{k'}/R(G)_{k'} = G_{k'}/R(G_{k'})$ is semisimple.


Cor. (7.3.3.16). Central and multiplicative isogenies from a group variety are the same thing, by (7.1.5.18).

Prop. (7.3.3.17) [Reductive Groups and Semisimple Groups]. A semisimple group is reductive, because $R_u(G) \subset R(G)$ as a unipotent group is solvable. Conversely, if $G$ is a reductive group, then the following are equivalent:

• $G$ is semisimple.
• $R(G) = e$.
• $Z(G)$ is finite.
• $G/[G,G]$ is finite.

Proof: 1 $\iff$ 2 follows from (7.3.3.15).

2 $\iff$ 3: As $R(G)$ is the maximal torus of the group $Z(G)$ of multiplicative type, $Z(G)/R(G)$ is finite (7.2.3.17). So if $R(G) = e$, $Z(G)$ is finite. And if $Z(G)$ is finite, $R(G) = e$ because it is a torus. □

Prop. (7.3.3.18). Let $G$ be a group variety over a field $k$, then if $G$ is reductive, then every commutative normal subgroup variety of $G$ is a torus, and the converse is also true if $k$ is perfect.

Proof: If $N$ is a commutative normal subgroup variety of $G$, then $N \subset R(G)$, which is a torus by (7.3.3.15) and (7.2.3.6). The converse follows from the fact $R_u(G) = e$ because $U(n)$ has no non-zero subtorus by (7.3.5.4). □

Prop. (7.3.3.19). If $G$ is reductive, then $[G,G]$ is semisimple of rank equal to the semisimple rank of $G$.


Prop. (7.3.3.20) [Maximal Central Torus]. If $G$ is a reductive group over a perfect field $k$, then $R(G) = Z(G)^{0 \text{red}}$, which is the maximal central torus by (7.3.3.21). In particular, $G$ is semisimple if and only if $Z(G)$ is finite.

Proof: □

Prop. (7.3.3.21). Any commutative affine group variety $G$ is of the form $U \times T$ where $U$ is unipotent and $T$ is a torus.

Proof: ? □

Prop. (7.3.3.22). Let $\varphi : G' \to G$ be an isogeny of group varieties. If $G$ is reductive or semisimple, then so is $G'$.

Proof: It suffices to assume $k = \overline{k}$. Let $U$ be a normal unipotent/solvable subgroup variety of $G$, then $\varphi(U)$ is also a unipotent/solvable group variety by (7.1.5.29), and it is normal because $\varphi$ is a quotient map (7.1.5.29). Thus $\varphi(U) = e$, which implies $U$ is a finite group variety, thus trivial. □
Prop. (7.3.3.23) [Matsushima’s Criterion]. If $G$ is a reductive group and $H$ a smooth algebraic subgroup, then $G/H$ is affine if $H^0$ is reductive.

Proof: Cf. [Borel, On affine algebraic homogeneous spaces].

Def. (7.3.3.24) [Ranks]. The rank of a group variety $G$ over $k$ is the dimension of the maximal torus in $G_{\mathbb{F}}$. The semisimple rank is the rank of $G_{\mathbb{F}}/R(G_{\mathbb{F}})$.

The $k$-rank is the dimension of a maximal split torus in $G$. The semisimple $k$-rank of $G$ is is the $k$-rank of $G/R(G)$.

These are well-defined by (7.3.1.5).

Prop. (7.3.3.25). Let $G$ be a reductive group, then the semisimple rank of $G$ equals $\dim G - \dim Z(G)$.

Proof: Cf.[Mil17]P402.

Parabolic Subgroups of Reductive Groups

Prop. (7.3.3.26) [Levi Factors]. Let $P$ be a group variety over $k$, a Levi subgroup of $P$ is a subgroup variety $L$ of $P$ s.t. $L_{\mathbb{F}} \to P_{\mathbb{F}}/R_u(P_{\mathbb{F}})$ is an isomorphism. In other words, $L$ is a reductive subgroup of $P$ s.t. $P_{\mathbb{F}} = R_u(P_{\mathbb{F}}) \ltimes L_{\mathbb{F}}$.

Prop. (7.3.3.27). Let $P$ be a parabolic subgroup of a reductive group $G$, then $P$ has Levi subgroups, and any two Levi subgroups of $P$ are conjugate by a unique element of $R_u(P)(k)$.

Proof: Cf.[Mil17]P559.

4 Split Reductive Groups

Def. (7.3.4.1) [Split Reductive Groups]. For $k \in \text{Field}$, a split reductive pair is a pair $(G, T)$ where $G$ is a reductive group over $k$ and $T$ is a split maximal torus. A reductive group is called split reductive if it is contained in some reductive pair. By (7.2.3.7), any reductive group is reductive after a finite separable change of fields.

Def. (7.3.4.2) [Anisotropic Reductive Groups]. For $k \in \text{Field}$, a reductive group is isotropic if it contains a non-central split torus; otherwise, it is anisotropic. Notice for semisimple groups, any split torus is central.

Reductive Groups of Semisimple Rank $\leq 1$

Prop. (7.3.4.3) [Classifying Reductive Groups of Semisimple Rank $\leq 1$]. Any reductive group over $k$ of semisimple rank 1 is isomorphic to exactly one of the groups $G_m^r \times \text{SL}(2), G_m^r \times \text{PGL}(2), G_m^r \times \text{PGL}(2), r \in \mathbb{N}$.

Proof: Cf.[Mil17]P419.
5 Classical Groups

Def.(7.3.5.1)[Examples of Classical Groups].

- the **general linear group** \( GL(n) = \mathbb{Z}[T_{ij}][1/\det] \) representing the group functor \( \mathcal{CAlg}_{\mathbb{Z}} \to \mathcal{S}rp : R \mapsto GL(n, R) \).

- the **multiplicative group** \( \mathbb{G}_m = \text{Spec} \mathbb{Z}[T, T^{-1}] \), which is just \( GL(1) \).

- the **special linear group** \( SL(n) \) is the algebraic subgroup scheme of \( GL(n) \) defined by the ideal \( (\det - 1) \), representing the group functor \( \mathcal{CAlg}_{\mathbb{Z}} \to \mathcal{S}rp : R \mapsto SL(n, R) \).

- the **orthogonal group** \( O(n) \) is the algebraic subgroup of \( GL(2n) \times \mathbb{G}_m \subset GL(2n+1) \) generated by the \( n^2 \) entries of the equation \( (T_{ij})^t C_n(T_{ij}) = TC_n \), where \( C_n = \begin{bmatrix} 0 & I_k & 0 \\ I_k & 0 & 0 \\ 0 & 0 & 1 \end{bmatrix} \) if \( n = 2k + 1 \) and \( \begin{bmatrix} 0 & I_k \\ I_k & 0 \end{bmatrix} \) if \( n = 2k \), representing the functor \( \mathcal{CAlg}_{\mathbb{Z}} \to \mathcal{S}rp : R \mapsto \{ g \in GL(2n, R) \times \mathbb{R}^\times | g^t C_n g = rC_n \} \).

- the **special orthogonal groups** \( SO(n) = O(n) \cap SL(n) \).

- the **symplectic group** \( \text{Sp}(2n) \) is the algebraic subgroup of \( GL(n) \) defined by the ideal generated by the \( n^2 \) entries of the equation \( (T_{ij})^t J_{2n}(T_{ij}) = J_{2n} \), where \( J_{2n} = \begin{bmatrix} 0 & I_n \\ -I_n & 0 \end{bmatrix} \), representing the functor

\[
\mathcal{CAlg}_{\mathbb{Z}} \to \mathcal{S}rp : R \mapsto \{ g \in GL(2n, R) | g^t J_{2n} g = J_{2n} \} = \left\{ \begin{bmatrix} A & B \\ C & D \end{bmatrix} | A^t C = C^t A, A^t D - C^t B = I, B^t D = D^t B \right\}.
\]

- \( \text{PGL}(n) \) is the quotient group of \( GL(n) \) by its center.

- \( \text{PSL}(n) \) is the quotient group of \( SL(n) \) by its center.

- \( \text{PSO}(n) \) is the quotient group of \( SO(n) \) by its center.

- the **general symplectic group** \( \text{GSp}(2n) \) is the algebraic subgroup of \( GL(2n) \times \mathbb{G}_m \subset GL(2n+1) \) generated by the entries of the equation \( (T_{ij})^t J_n(T_{ij}) = T J_n \), representing the functor \( \mathcal{CAlg}_{\mathbb{Z}} \to \mathcal{S}rp : R \mapsto \{ (g, r) \in GL(2n, R) \times \mathbb{R}^\times | g^t J_n g = r J_n \} \).

- the **standard Borel subgroup** \( B(n) \) is the algebraic subgroup of \( GL(n) \) representing the upper-triangular matrices.

- the **standard unipotent subgroup** \( \text{Unip}(n) \) is the algebraic subgroup of \( B(n) \) representing the unipotent matrices.

- the **diagonal group** \( D(n) \) is the algebraic subgroup of \( B(n) \) representing the diagonal matrices.

- **unitary groups**.

- **special unitary groups**.

*Proof:* By(7.1.1.3), it suffices to show \( \text{Hom}( -, G) \) is a group functor when restricted to affine schemes. \( \square \)
Prop. (7.3.5.2) [Amplitude Character]. There is an \textbf{amplitude character} $\text{GSp}_{2n} \to G_m : T \mapsto T$, which represents the natural transformation $R \mapsto ((g, r) \mapsto r)$.

Prop. (7.3.5.3) [Borel Subgroups of $GL(n)$]. If $k = \overline{k}$ and $G = GL(n)$, then by Lie-Kolchin (7.2.5.5), the Borel subgroups of $G$ are exactly the conjugates by $G(k)$ of $B(n)$.

\textit{Proof:} Cf. [Mil17]P354. \hfill \square

Prop. (7.3.5.4). $B(n)$ is split solvable and $\text{Unip}(n)$ is split nilpotent.

Moreover, $\text{Unip}(n)$ has no non-zero subtorus, by successively using (7.1.1.8).

\textit{Proof:} Cf. [Mil17]P137. \hfill \square

Prop. (7.3.5.5). Let $G = \text{SO}(2n), \text{SO}(2n+1)$ or $\text{Sp}(2n)$, then the maximal Borel subgroup of $G$ are the stabilizers of the maximal totally anisotropic flags in $G$(of length $n$).

\textit{Proof:} Cf. [Mil17]P354. \hfill \square

Prop. (7.3.5.6) [Reductive and Semisimple Groups]. $GL(n), SL(n), SO(n), Sp(2n)$ are reductive, as they are connected, and their standard representation is simple, by (15.3.4.1).

$SL(n), SO(n), Sp(2n)$ are semisimple, as they have finite centers (7.3.3.17).

6 Real Reductive Groups

Main references are [Gaitsgory, Real Reductive Groups] and [Mil17b].

Def. (7.3.6.1) [Real Forms]. Let $G$ be a connected complex Lie group, then a \textbf{real form} of $G$ is a connected real Lie subgroup $K \subset G$ that $\mathfrak{k} \otimes \mathbb{C} \cong \mathfrak{g}$.

Prop. (7.3.6.2) [Real Lie Groups and Algebraic Groups]. Let $(H, \mathfrak{h})$ be a connected Lie group in $\text{LieGrp}/\mathbb{C}$, then there needs not be an algebraic group $G$ over $\mathbb{R}$ that $G(\mathbb{R})^0 = H$. For example, the topological fundamental group of $\text{SL}(2, \mathbb{R})$ is $\mathbb{Z}$, so it has many coverings of finite degree, none of which is algebraic, because $\text{SL}_2$ as an algebraic group is simply connected.

However, if $H$ admits a f.d. representation $H \hookrightarrow GL(V)$, then there exists an algebraic group $G \subset GL(V)$ that $\text{Lie}(G) = [\mathfrak{h}, \mathfrak{h}]$. So if $H$ is semisimple, then there exists an algebraic group $G \subset GL(V)$ s.t. $\text{Lie}(G) = [\mathfrak{h}, \mathfrak{h}]$. When $H$ is semisimple, this means $G^0 = H$.

Compact Real Algebraic Groups

Def. (7.3.6.3) [Compact Real Algebraic Groups]. A compact real algebraic group is an algebraic group $G \in \text{AlgGrp}/\mathbb{R}$ s.t. $G(\mathbb{R})$ is a compact Lie group.

Prop. (7.3.6.4) [Compactness and Representations]. Let $G \in \text{AlgGrp}_{\text{cntd}}/\mathbb{R}$. If $G$ is compact, then every f.d. real representation $\rho : G \to GL(V)$ carries a $G(\mathbb{R})$-invariant inner form. Conversely, if a faithful f.d. real representation carries such a form, then $G$ is compact.

\textit{Proof:} If $G$ is compact, then $H = \rho_{\mathbb{R}}(G(\mathbb{R}))$ is compact, so we can take an arbitrary inner form on $V$ and take average on $H$. The converse is easy. \hfill \square

Def. (7.3.6.5) [Relevant Groups]. A compact real algebraic group is called \textbf{relevant} iff the map $\pi_0(G(\mathbb{R})) \to \pi_0(G(\mathbb{R}))/\mathbb{R}$ is surjective.
Lemma (7.3.6.6). Let $Z$ be an affine variety over $\mathbb{R}$, let $X$ be a subset of $Z(\mathbb{R})$, and let $I_X$ be the ideal of regular functions on $Z$ that vanishes at $X$, then $X' = V(I_X)$ satisfies $X \subset X'(\mathbb{R})$. Also by construction, $X'$ is relevant and $X$ intersects real points of every connected components of $X'$.

Now if $Z$ is acted on by a compact Lie group $K$ and $X$ is a single $K$-orbit, then $X \cong X'(\mathbb{R})$.

Proof: Cf. [Gaitsgory P17]. $\square$

Prop. (7.3.6.7) [Compact Relevant Groups and Compact Real Lie Groups]. The functor $G \mapsto G(\mathbb{R})$ is an equivalence of categories from the category of relevant real compact algebraic groups to the category of compact real Lie groups.

Proof: For the fully faithfulness: given a map $\varphi : G_1(\mathbb{R}) \to G_2(\mathbb{R})$, we need to show it comes from a unique algebraic group homomorphism. Let $K \subset G_1(\mathbb{R}) \times G_2(\mathbb{R})$ be the graph of $\varphi$, then let $\Gamma$ be the subgroup of $G_1 \times G_2$ corresponding to $K$ in (7.3.6.6), then it suffices to prove that the map $\Gamma \to G_1$ is an isomorphism. It is an isomorphism after passing to real points, so isomorphism on the level of Lie algebras. And then it is an isomorphism, because both groups are relevant.$^?$. $\square$

Cor. (7.3.6.8). The proof actually works only if $G_1$ is relevant compact real group. So if we choose $G_2 = GL(n, \mathbb{C})_\mathbb{R}$, then by adjointness there is a bijection

$$\text{Hom}_{\text{AlgGrp}/\mathbb{C}}(G_\mathbb{C}, GL(n)_\mathbb{C}) \cong \text{Hom}_{\text{LieGrp}}(G(\mathbb{R}), GL_n(\mathbb{C})).$$

That is, their complex representations correspond.

Complex Reductive Algebraic Groups

Prop. (7.3.6.9). If $G$ is a real reductive group, then its complexification $G_\mathbb{C}$ is complex reductive.

Proof: It suffices to show that $\text{Rep}(G_\mathbb{C})$ is semisimple. For this, notice $\text{Rep}(G)$ is semisimple by definition, so it suffices to show for any representation $V$ of $G_\mathbb{C}$, if $W$ is a $G$-invariant subspace, then $W$ is also $W$ is $G_\mathbb{C}$-invariant. But the invariance condition is a vanishing of some matrix coefficients, they vanish on $G$ so also vanish on $G_\mathbb{C}$. $\square$

Def. (7.3.6.10) [Real Form]. A real form on a complex reductive algebraic group is an anti-linear group isomorphism $\sigma : G \to G$ that $\sigma^2 = 1$. It is called relevant iff $G^\sigma$ is compact real, and it is called relevant iff $G^\sigma$ is relevant compact (7.3.6.5).

Prop. (7.3.6.11) [Polar Decomposition]. If $G$ is a complex algebraic group and $K \in G(\mathbb{C})$ is a compact Lie subgroup. Assume that

- $\mathfrak{g} \cong \mathfrak{k} \otimes \mathbb{R} \oplus \mathfrak{c}$.
- $K$ intersects non-trivially every connected components of $G(\mathbb{C})$.

Then the group $G$ contains a unique real structure $\sigma$ that $K = G(\mathbb{C})^\sigma$. And if $\mathfrak{p} \subset \mathfrak{g}$ be the subspace $\{\xi \in \mathfrak{g} | \sigma(\xi) = -\xi\}$, then the map

$$k \times \mathfrak{p} \to G(\mathbb{C}) : (k, p) \mapsto k \cdot \exp(p)$$

is a diffeomorphism.

Proof: Cf. [Gaitsgory P18]. $\square$
Cor. (7.3.6.12). If we denote $P = \exp(p)$, then $P \subset \tilde{P} = \{g \in G(\mathbb{C})|\sigma(g) = g^{-1}\}$, and there is a diffeomorphism:

$$\prod_{k \in K, k^{2} = 1} \{k\} \times P \cong \tilde{P}.$$

Cor. (7.3.6.13). In the situation of $(7.3.6.11)$, $G$ is reductive, by $(7.3.6.9)$.

Cor. (7.3.6.14). $K \to G(\mathbb{C})$ is a homotopy equivalence.

**Cartan Involutions**

Def. (7.3.6.15) [Cartan Involutions]. Let $G \in \mathfrak{Alg}\mathfrak{Grp}_{\text{cntd}} / \mathbb{R}$, an involution on $G$ is an isomorphism $\theta : G \cong G$ s.t. $\theta^{2} = \text{id}$.

A Cartan involution is an involution s.t. $G^{(\theta)}(\mathbb{R}) = \{g \in G(\mathbb{C})|g = \theta(\overline{g})\}$ is compact.

Prop. (7.3.6.16). Cartan involution and compactness.

Example (7.3.6.17). Let $G = \text{SL}(2)_{\mathbb{R}}$ and $\theta = \text{ad}\left(\begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}\right)$, then $\text{SL}(2)^{(\theta)}(\mathbb{R}) = \text{SU}(2)$ is compact, so this is a Cartan involution on $G$.

Thm. (7.3.6.18) [Satake]. Let $G \in \mathfrak{Alg}\mathfrak{Grp}_{\text{cntd}} / \mathbb{R}$, then $G$ admits a Cartan involution iff $G$ is reductive. And in this case, any two Cartan involutions differ by a conjugation by elements in $G(\mathbb{R})$, i.e. $(\tau = \text{ad}(g_{0})^{-1} \circ \theta \circ \text{ad}(g_{0}))$.


Cor. (7.3.6.19) [Satake].

- $G$ is a connected algebraic group, then $G$ is compact iff id is a Cartan involution on $G$. And in this case, this is the only Cartan involution of $G$. In particular, a compact connected algebraic group is reductive.

- If $V$ is a f.d. real vector space and $G = \text{GL}(V)$, then the choice of a basis for $V$ determines a Cartan involution $M \mapsto M^{t}$, and by (7.3.6.18), any Cartan involution is of this form.

- If $G \subset \text{GL}(V)$, then $G$ is reductive iff $g$ is stable under a Cartan involution of $\text{GL}(V)$. And any Cartan involutions of $G$ is of this form.


Prop. (7.3.6.20) [c-Polarizations]. Let $G \in \mathfrak{Alg}\mathfrak{Grp} / \mathbb{R}$ and $c \in G(\mathbb{R})$ (equivalently $c^{2} \in Z(G(\mathbb{R}))$, and $\text{ad}(c)^{-1} = \text{ad}(c^{-1})$). Then for a real representation $V$ of $G$, a $c$-polarization is a $G(\mathbb{R})$-invariant bilinear form $\varphi$ s.t. the form $(u, v) \mapsto \varphi(u, cv)$ is symmetric and positive-definite.

Then for such $c$, if $\text{ad}(c)$ is a Cartan involution, then any f.d. real representation of $G$ admits a $c$-polarization. Conversely, if a faithful real representation of $G$ admits a $c$-involution, then $\text{ad}(c)$ is a Cartan involution.

Maximal Compact Subgroup

Cor. (7.3.6.21). For any compact subgroup $K' \subset G(\mathbb{R})$, there exists an element $g \in P^\tau$ s.t. $Ad_g(K') \in K^\tau$.

Proof: Cf.[Gaitsgory P25].

Complex Reductive Lie Groups

Def. (7.3.6.22)[Complex Reductive Lie Groups]. A connected complex reductive Lie group is a connected complex Lie group $G$ of the form $((\mathbb{C}^*)^r \times G_{ss})/Z$ where $G_{ss}$ is semisimple and $Z$ is a finite central subgroup. A complex reductive Lie group is a complex Lie group $G$ that $G^0$ is connected reductive and $G/G^0$ is finite.

Def. (7.3.6.23)[Compact Part]. If $G = ((\mathbb{C}^*)^r \times G_{ss})/Z$ is a connected complex reductive Lie group, then $Z \subset (S^1)^r \times G^c_{ss}$ (the compact part), then we denote $G^c = (S^1)^r \times G^c_{ss}/Z$ the compact subgroup of $G$. Then the restriction of f.d. representations of $G$ to $G^c$ is an equivalence by (11.6.7.3).

Example (7.3.6.24). $GL(n, \mathbb{C}) = (\mathbb{C}^* \times SL(n, \mathbb{C}))/\mu_n$ is a complex reductive Lie group.

Prop. (7.3.6.25) [Abstract Jordan Decomposition]. Let $G$ be a connected reductive complex Lie group. A semisimple/unipotent element of $G$ is an element that acts on every f.d. representation of $G$ by a semisimple/reductive operator. By (11.6.5.5), it suffices to check for one faithful representation of $G$ by (11.6.5.5) and (7.3.6.23)(faithful representations exist by (7.3.6.23) and (11.6.5.4)).

Then every element $g \in G$ has a decomposition $g = g_s g_u$ where $g_s$ is semisimple, $g_u$ is unipotent, and $g_s g_u = g_u g_s$.

Proof: Cf.[Etingof, P210].

7 Reductive Group Schemes
7.4 Topics in Group Schemes

Thm.(7.4.0.1) [Lang-Steinberg]. Let $k \in \text{Field}, k = \overline{k}, G \in \text{AlgGrp}\text{cntd}/k, F \in \text{End}(G) \in \text{AlgGrp}/k$ s.t. the fixed point of $F(\overline{k})$ is finite, then the **Lang map**

$$\mathcal{L} : G \to G : g \mapsto g^{-1}F(g)$$

is surjective.

**Proof:** Cf.[Steinberg, Endomorphisms of Linear Algebraic Groups, P67].

We only prove for the case $\# k < \infty$ and some Power of $F$ is given by a standard Frobenius of $G$.

By(7.1.4.3), we can assume $G$ is smooth. $G$ acts on itself as $g(x) = gxF(g)^{-1}$. By(7.2.1.15), it has a closed orbit $\Omega$. Thus it suffices to show that $\dim \Omega = \dim G$. Take $x \in \Omega(k)$, by(7.2.1.12) and(7.1.1.28), it suffices to show there exists only f.m. $g \in G(k)$ s.t. $gxF(g)^{-1} = x$. Let $F^m(x) = x, f : G \to G : f(g) = xF(g)x^{-1}$. Notice $xF(x) \cdot F^2(x) \cdot \ldots \cdot F^{m-1}(x)$ is contained in $\ker(F^m)$, so it is of finite order, let’s say $r$. Then $f^{mr} = F^{mr}$, which has only f.m. solutions, thus there are only f.m. $g$ s.t. $gxF(g)^{-1} = x$. □

1 over Finite Fields

Main references are [Representations of Finite Groups of Lie Type, Digne and Michel].

Notations(7.4.1.1).

- $p \in \mathbb{P}, r \in \mathbb{Z}_+, q = p^r, k \in \text{Field}^p, \# k = q$.

Prop.(7.4.1.2)[Orbits Contains a Rational Point]. Let $V \in \text{Sch}/k, G \in \text{AlgGrp}\text{cntd}/k, G$ acts on $V$, then any $G$-orbits $O$ contains a rational point.

**Proof:** Let $v \in O(\overline{k})$, then $F(v) = gv$ for some $g \in G(\overline{k})$. Then by Lang’s theorem(7.4.0.1), $g = F(h)^{-1}h$ for some $h \in G(\overline{k})$. Then $F(h(v)) = h(v)$, so $h(v) \in O$ is a rational point. □

Cor.(7.4.1.3). If $G \in \text{AlgGrp}/k, H \leq G$ is a connected subgroup, then $G(k)/H(k) = G/H(k)$. 

7.5 Formal Groups and $p$-Divisible Groups

Main References are [Zin84].

1 Formal Power Series

Def.(7.5.1.1)[Notations]. Let $X = \{X_1, \ldots, X_n\}$, $Y = \{Y_1, \ldots, Y_n\}$.

Let $R$ be a commutative unital ring, $R[[X]]$ be the power series ring. It is a local ring with the maximal ideal $(X)$.

Let $i_1 : R[[X]] \to R[[X, Y]]$ and $i_2 : R[[Y]] \to R[[X, Y]]$ be the natural embeddings.

Let $\Omega^1_{R[[X]]/R}$ be the free $R[[X]]$-module with basis given by $dX_1, \ldots, dX_n$. And there is a universal derivative $D : R[[X]] \to \Omega^1_{R[[X]]/R}$ given by $D(f) = \sum_i \frac{\partial f}{\partial X_i} dX_i$. It satisfies the usual universal property of Kähler differentials, but with morphisms changed to continuous morphisms.

Prop.(7.5.1.2)[Formal Sums and Products].

• Let $f_n \in R[[X]]$ for any $n \in \mathbb{N}$ s.t. for any $m \in \mathbb{N}$, there exists a $N(m) \in \mathbb{N}$ s.t. $f_n \in (X)_m$ for any $n \geq N(m)$, then define the formal sum

$$\sum_n f_n = \lim_{n \to \infty} \sum_{k=0}^n f_k.$$ 

In this case, we say $\sum_n f_n$ is well-defined.

• Let $g_n \in R[[X]]$ for any $n \in \mathbb{N}$ s.t. for any $m \in \mathbb{N}$, there exists a $N(m) \in \mathbb{N}$ s.t. $g_n \in 1 + (X)_m$ for any $n \geq N(m)$, then define the formal product

$$\prod_n g_n = \lim_{n \to \infty} \prod_{k=0}^n g_k.$$ 

In this case, we say $\prod_n g_n$ is well-defined.

Prop.(7.5.1.3)[Automorphisms]. If $F_i$ are power series without constant terms that the matrix degree 1 terms of $(F_i)$ (the Jacobi matrix) is invertible in $R$, then there are unique power series $G_i$ without constant terms that $G_i \circ F_i = \text{id}$ and $F_i \circ G_i = \text{id}$.

Proof: It $F_i$ induces a map $F : R[[X_1, \ldots, X_n]] \to R[[X_1, \ldots, X_n]]$ which in turn induces a graded map $K[X_1, \ldots, X_n] \to K[X_1, \ldots, X_n]$. It is clear that $(\frac{\partial F_i}{\partial X_j})_{ij}$ is invertible iff the induced graded ring map is an isomorphism, and because $K[[X_1, \ldots, X_n]]$, a map is an isomorphism iff its induced graded map is an isomorphism. □

Prop.(7.5.1.4). If $R$ be a torsion-free algebra, and let

$$f(T) = \sum_{n \geq 1} \frac{a_n}{n!} T^n \in (R \otimes \mathbb{Q})[[T]], \quad a_1 \in R^*.$$ 

Then the unique $g(T)$ s.t. $f(g(T)) = T$ is of the form

$$g(T) = \sum_{n \geq 1} \frac{b_n}{n!} T^n \in (R \otimes \mathbb{Q})[[T]], \quad b_1 \in R^*.$$
Proof: Repeatedly differentiating the equation \( f(g(T)) = T \), we get that \( f(t(g(T))g^{(n)}(T) \) can be expressed as integral polynomials in the variables
\[
f^{(i)}(g(T)), 1 \leq i \leq n, \quad g^{(j)}(T), 1 \leq j \leq n - 1.
\]
Then evaluating at \( T = 0 \), we get that \( b_n \in R \) and \( b_1 \in R^* \), as \( a_1 \in R^* \).

1-Dimensional Formal Power Series

Def.(7.5.1.5)[Formal Exponential and Logarithm]. The formal exponential and formal logarithm is defined to be elements in \( Q[[x]] \):
\[
\exp(x) = \sum_{n \geq 0} \frac{x^n}{n!}, \quad \log(1 + x) = -\sum_{n > 0} \frac{(-x)^n}{n}.
\]
They satisfies \( \exp(\log(1 + x)) = 1 + x \), \( \log(\exp(x)) = x \).

Remark(7.5.1.6). WARNING: It should be made clear that \( \log(1 + f) \) is defined only for \( f \in xK[[x]] \), and \( \log(1 + x) \) is a symbol for the function \( \Log(x) = \log(1 + x) \). \( \log(x) \) is not defined.

Proof: It suffices to prove \( \Exp(x) = \exp(x) - 1 \) and \( \Log(x) = \log(1 + x) \) are inverse to each other. It suffices to show \( \log(\exp(x)) = x \), because then by (7.5.1.3) the inverse of \( \Log \) must be just \( \Exp \) by (7.5.1.3).

We notice \( \Exp \) are the unique formal power series without constant term that satisfied \( d(\Exp) = \Exp + 1 \), and \( \Log \) is the unique formal power series that satisfies \( d(\Log(x)) = \frac{1}{1+x} \). Thus
\[
d(\log(\exp(x))) = \frac{\exp(x)}{\exp(x)} = 1,
\]
so \( \log(\exp(x)) = x \), because it has no constant term.

Prop.(7.5.1.7)[Multiplicative Properties]. Suppose \( Q \subset R \), then
- for any \( f, g \in R[[X]] \), \( \exp(f + g) = \exp(f) \exp(g) \).
- If \( \sum_n f_n \) is well-defined(7.5.1.2), then \( \prod_n \exp(f_n) \) is well-defined and
\[
\exp(\sum_n f_n) = \prod_n \exp(f_n).
\]
- for any \( f, g \in 1 + (X) \), \( \log(f) + \log(g) = \log(fg) \).
- If \( g_n \in 1 + (X) \) and \( \prod_n g_n \) is well-defined(7.5.1.2), then \( \sum_n \log(f_n) \) is well-defined and
\[
\log(\sum_n f_n) = \prod_n \log(f_n).
\]

Proof: Brutal force calculation.

Def.(7.5.1.8)[Formal Powers]. Let \( f \in 1 + xR[[x]] \), \( g \in R[[x]] \), \( f^g \) is defined to be
\[
\exp(g \log(f)).
\]
In particular, \( \log(f^g) = g \log(f) \) by (7.5.1.5).
**Prop. (7.5.1.9).** In $\mathbb{Q}[x]$, if $p \in \mathbb{P}$, $m, n \in \mathbb{Z}$, $(n, p) = 1$, and $f(x) \in 1 + x\mathbb{Z}_p[[x]]$, then $f(x)^{m/n} \in 1 + x\mathbb{Z}_p[[x]]$.

**Proof:** If $g(x) = f(x)^{m/n}$, it is easy to see $g(x)^n = f(x)^m$ and $g(x) \in 1 + x\mathbb{Q}[[x]]$. Let

$$f(x)^m = 1 + \sum_{m \geq 1} a_m x^m, \quad g(x) = 1 + \sum_{m \geq 1} b_m x^m,$$

Then it is easy to use induction to show $b_m \in \mathbb{Z}_p$ for any $m \in \mathbb{Z}_+$.

**Prop. (7.5.1.10).** In $\mathbb{Q}[x]$, $$\exp(x) = \prod_{d > 0} \left( \frac{1}{1 - x^d} \right)^{\mu(d)/d}.$$  

**Proof:** Taking log, we prove its convergence and equality at once:

$$\sum_{d > 0} \log((1 - x^d)^{\mu(d)/d}) = \sum_{d > 0} \frac{\mu(d)}{d} \log(1 - x^d) = \sum_{d > 0} \frac{\mu(d)}{d} \sum_{d' > 0} x^{dd'} = \sum_{n > 0} x^n \sum_{d | n} \mu(d) = x(20.1.2.19).$$

**Prop. (7.5.1.11) [Artin-Hasse Exponential].** For $p \in \mathbb{P}$, the Artin-Hasse exponential is the power series $\text{hexp}(x)$ defined to be

$$\text{hexp}(x) = \exp(x + \frac{x^p}{p} + \frac{x^{p^2}}{p^2} + \ldots) \in \mathbb{Q}[x].$$

Then it satisfies

$$\text{hexp}(x) = \prod_{d > 0, p \nmid d} \left( 1 - x^d \right)^{\mu(d)/d},$$

and in fact $\text{hexp}(x) \in \mathbb{Z}_p[[x]]$.

**Proof:** Taking log, we prove its convergence and equality at once:

$$\sum_{d > 0, p \nmid d} \log((1 - x^d)^{\mu(d)/d}) = \sum_{d > 0, p \nmid d} \frac{\mu(d)}{d} \log(1 - x^d) = \sum_{d > 0, p \nmid d} \frac{\mu(d)}{d} \sum_{d' > 0} x^{dd'} = \sum_{n > 0} x^n \sum_{d | n, p \nmid d} \mu(d) = \sum_{k \in \mathbb{N}} x^{pk}(20.1.2.19).$$

Then the last assertion follows from (7.5.1.9).

**Def. (7.5.1.12) [Hankel Determinants].** Let $K$ be a field and $f = \sum a_i T^i \in K[[T]]$, then for $k, M > 0$, define the Hankel determinants to be

$$H_k = \det(a_{i+j+k}), 1 \leq i, j \leq M$$

**Prop. (7.5.1.13) [Characterizing Rational Functions].** Let $f \in K[[T]]$, then $f \in K[T]$ iff the Hankel determinants $H_k$ of $f$ vanishes for $k, M$ large.

**Proof:**

**Cor. (7.5.1.14).** If $K \subset L$ are fields, then $K[[T]] \cap L[T] = K[T]$. 

7.5. FORMAL GROUPS AND P-DIVISIBLE GROUPS

Geometric Objects

**Def. (7.5.1.15) [Differential Operators].** A continuous $R$-linear mapping $D : R[[X]] \to R[[X]]$ is called a formal differential operator of order $N \geq -1$ iff

$$L_D : R[[X, Z]] \to R[[X]] : \sum p_\alpha(X)Z^\alpha \to \sum p_\alpha(X)D(X^\alpha)$$

vanish on $J^{N+1}$, where $J = (X_i - Z_i)$.

Then $D$ is an operator of order $N$ if $f D - D f$ has order $N - 1$ for any $f \in R[[X]]$.

**Proof:** Let $D$ be a differential operator of order $N$, since $f(X) - f(Z) \in J$, for all $g(X, Z) \in J^N$, we have $L_D((f(X) - f(Z))g(X, Z)) = 0$, which is equivalent to $L_{D(f - f \circ D)}(g) = 0$, so $D \circ f - f \circ D$ is an operator of order $N - 1$. Conversely, if $D \circ f - f \circ D$ is an operator of degree $N - 1$, then $L_D((f(X) - f(Z))g) = 0$ for all $g \in J^N$, then $D$ is an operator of order $N$.

**Cor. (7.5.1.16).** A differential operator $D : R[[X]] \to R[[X]]$ of order 1 is a linear map that satisfies $D(fg) = D(f)g + fD(g)$, which is just a derivative on $R[[X]]$. Equivalently, $D = \sum_i u_i(Z) \frac{\partial}{\partial Z^i}$.

**Prop. (7.5.1.17) [Graded Module of Differential Operators].** Let $D_1, D_2$ be differential forms of order $N_1, N_2$, then $D_1 \circ D_2$ is a differential form of order $N_1 + N_2$, and $[D_1, D_2]$ is a differential form of order $N_1 + N_2 - 1$. The $R$-algebra of differential operators on $R[[X]]$ is denoted by $\mathcal{DO}$.

In particular, the graded module of differential operators

$$\text{gr } \mathcal{DO} = \oplus \mathcal{DO}_N / \mathcal{DO}_{N-1}$$

is a commutative graded ring.

**Proof:**

**Prop. (7.5.1.18) [Basis of Differential Operators].** There is a representation $g(X + Y) = \sum_\alpha D_\alpha g(X)Y^\alpha$ for any $g \in R[[X, Y]]$, where $D_\alpha$ is a differential operator of degree $|\alpha|$. And \{D_\alpha\} form a free $K[[X]]$-basis for the module of differential operators (7.5.1.17).

In fact, $D_\alpha$ is just mimicking $\frac{\partial^\alpha}{\partial X^\alpha}$ in all fields.

**Proof:** $g(Z) = \sum_\alpha D_\alpha g(X)(Z - X)^\alpha$, thus if $D$ is a differential operator of order $N$, then

$$D(g)(X) = L_D(g(Z)) = \sum_{|\alpha| \leq N} L((Z - X)^\alpha)D_\alpha g(X),$$

which means $D = \sum_{|\alpha| \leq N} a_\alpha(X)D_\alpha$, where $a_\alpha = L((Z - X)^\alpha)$.

**Def. (7.5.1.19) [Tangent Space].** The tangent space of $K[[X]]$ is the $K$-module $\text{Hom}_K((X)/(X)^2, K)$.

**Def. (7.5.1.20) [Formal Curves].** A formal curve in $K[[X]]$ is an $n$-tuple $(\gamma_1(T), \ldots, \gamma_n(T))$ of elements in $K[[T]]$. The tangent space of formal curve is the map $\text{Hom}_K((X)/(X)^2, K)$ given by $X_i \mapsto \gamma_i(T) \in (T)/(T^2) \cong K$.

**Prop. (7.5.1.21) [Integral Curves].** For any
2 Formal Identities

Prop.(7.5.2.1). In $\mathbb{Z}[[T]]$,
\[
\frac{1}{(1-T)^2} = \sum_{n \geq 0} (n+1)z^n
\]

Proof:
\[
(1-T)^2 \sum_{n \geq 0} (n+1)z^n = (1-T) \sum_{n \geq 0} z^n = 1.
\]

Prop.(7.5.2.2). In $\mathbb{Z}[[T]]$,
\[
\sum_{n \geq 1} \frac{nT^n}{1-T^n} = \sum_{n \geq 1} \frac{T^n}{(1-T^n)^2}
\]

Proof:

Prop.(7.5.2.3). In $\mathbb{R}[[z]]$, if
\[
\infty \sum_{r=0} A(r)z^r = \frac{1}{(1-\alpha_1 z)(1-\alpha_2 z)}, \quad \infty \sum_{r=0} B(r)z^r = \frac{1}{(1-\beta_1 z)(1-\beta_2 z)},
\]
then
\[
\infty \sum_{r=0} A(r)B(r)z^r = (1-\alpha_1 \alpha_2 \beta_1 \beta_2 z^2)^2 \prod_{i=1}^2 \prod_{j=1}^2 \frac{1}{1-\alpha_i \beta_j z}.
\]

Proof: \( A(n)B(n) = \sum_{0 \leq k,j \leq n} \alpha_i^k \alpha_2^{n-k} \beta_1^j \beta_2^{n-j} \), and the coefficients in the $z^n$ term of \( \prod_{i=1}^2 \prod_{j=1}^2 \frac{1}{1-\alpha_i \beta_j z} \)

\[
\sum_{0 \leq k,j \leq n} \sum_{0 \leq k,j \leq n} \{ (r_1, r_2, r_3, r_4) | 0 \leq r_i \leq n, r_1 + r_2 = a, r_1 + r_3 = b, r_1 + r_2 + r_3 + r_4 = n \} \alpha_i^k \alpha_2^{n-k} \beta_1^j \beta_2^{n-j}.
\]

Notice
\[
\sum_{0 \leq k,j \leq n} \{ (r_1, r_2, r_3, r_4) | 0 \leq r_i \leq n, r_1 + r_2 = a, r_1 + r_3 = b, r_1 + r_2 + r_3 + r_4 = n \} = \min(a,n) - (a + n).
\]

Thus the effect of multiplying \( (1-\alpha_1 \alpha_2 \beta_1 \beta_2 z^2)^2 \) reduces the coefficients of \( \alpha_i^k \alpha_2^{n-k} \beta_1^j \beta_2^{n-j} \) to 1. So the assertion follows.

Prop.(7.5.2.4)[Euler Identities].

- In $\mathbb{Z}[x][[q]]$,
\[
\prod_{n \geq 0} (1 + xq^n) = \sum_{n=0}^{\infty} \frac{q^{n(n-1)/2} x^n}{(1-q) \ldots (1-q^n)}.
\]

- In $\mathbb{Z}[[x, q]]$,
\[
\prod_{n \geq 0} (1 - xq^n)^{-1} = \sum_{n=0}^{\infty} \frac{x^n}{(1-q) \ldots (1-q^n)}.
\]

Proof: These follow from interesting combinatorial identities.
Def. (7.5.3.1) [Formal Group Laws]. A formal group law $G$ of dimension $n$ over $R \in \mathcal{C}_{\text{Alg}}$ is a continuous local map $\mu_G : K[[X]] \to K[[X,Y]]$ given by an $n$-tuple of power series $G = (G_1, \ldots, G_n)$ in $R[[X,Y]]$ such that

$$G(X,Y) \equiv X + Y \mod (X,Y)^2, \quad G(G(X,Y),Z) = G(X,G(Y,Z)).$$

A formal $R$-module is a formal group law $G$ over $R$ together with a ring homomorphism $R \to \text{End}_R(G)$ that $[a](X) = aX + \ldots$.

Prop. (7.5.2.5) [Jacobi’s Triple Product Formula, [And65]]. In $\mathbb{Z}[x][[x^{-1}q]]$,

$$\sum_{n=-\infty}^{\infty} x^n q^{2n} = \prod_{n=1}^{\infty} (1 - q^{2n})(1 + xq^{2n-1})(1 + x^{-1}q^{2n+1}).$$

**Proof:** By substituting $q = q^2$, $x = xq$ in Euler identities (7.5.2.4), in $\mathbb{Z}[x][[x^{-1}q]]$,

$$\prod_{n \geq 0} (1 + xq^{2n+1}) = \sum_{n=0}^{\infty} \frac{q^n x^n}{(1 - q^2)(1 - q^4) \cdots (1 - q^{2n})}$$

$$= \left( \prod_{j \geq 0} (1 - q^{2j+2}) \right)^{-1} \sum_{n=-\infty}^{\infty} q^n x^n \prod_{j=0}^{\infty} (1 - q^{2n+2+j})$$

$$= \left( \prod_{j \geq 0} (1 - q^{2j+2}) \right)^{-1} \sum_{n=-\infty}^{\infty} q^n x^n \prod_{j=0}^{\infty} (1 - q^{2n+2+j})$$

$$= \left( \prod_{j \geq 0} (1 - q^{2j+2}) \right)^{-1} \sum_{n=-\infty}^{\infty} q^n x^n \prod_{j=0}^{\infty} (1 - q^{2n+2+j})$$

$$= \left( \prod_{j \geq 0} (1 - q^{2j+2}) \right)^{-1} \sum_{m=0}^{\infty} \frac{(-1)^m q^{m^2 + m + 2nm}}{(1 - q^2)(1 - q^4) \cdots (1 - q^{2n})} \sum_{n=-\infty}^{\infty} q^{(m+n)^2} x^{m+n}$$

$$= \left( \prod_{j \geq 0} (1 - q^{2j+2}) \right)^{-1} \sum_{j=0}^{\infty} (1 + x^{-1}q^{2j+1})^{-1} \sum_{n=-\infty}^{\infty} q^n x^n.$$

\[\square\]

Cor. (7.5.2.6) [Dedekind Eta Function]. Substitute $q = q^{3/2}$ and $x = q^{-1/2}$, we get:

$$\sum_{n=-\infty}^{\infty} (-1)^n q^{(3n^2 + n)/2} = \prod_{n=1}^{\infty} (1 - q^{3n})(1 - q^{3n-1})(1 - q^{3n+1}) = \prod_{n=1}^{\infty} (1 - q^n) \in \mathbb{Z}[[q]].$$

By completing the square,

$$\sum_{n=-\infty}^{\infty} (-1)^n q^{(6n+1)^2/24} = q^{1/24} \prod_{n=1}^{\infty} (1 - q^n) \in \mathbb{Z}[[q^{1/24}]].$$

the last term is known as the Dedekind eta function $\eta(q) = q^{1/24} \prod_{n=1}^{\infty} (1 - q^n) \in \mathbb{Z}[[q^{1/24}]].$

3 Formal Group Law

In this subsection, the local structure of an algebraic group scheme at the origin is studied.
A morphism of formal groups laws $G \to H$ is a continuous local map $\varphi^* : R[[X]] \to R[[X]]$ given by an $n'$-tuple of power series $\varphi = (\varphi_1, \ldots, \varphi_{n'})$ in $R[[X]]$ that satisfies

$$\mu_G \circ \varphi^* = (\varphi^* \circ \varphi^*) \circ \mu_H.$$ 

Or equivalently, $\varphi(G(X, Y)) = H(\varphi(X), \varphi(Y))$.

**Prop.(7.5.3.2).** For a formal group Law $G$,
- $G(0, Y) = Y, G(X, 0) = X$.
- There exists a unique inverse $i(X)$ that $G(X, i(X)) = 0$. And this $i(X)$ satisfies $G(i(X), X) = 0$, and $i^2 = \text{id}$.

**Proof:**

**Cor.(7.5.3.3) [Formal Group Laws and Group Schemes].** WARNING: A formal group law of dimension $n$ is not equivalent to a group scheme structure on Spec $\mathbb{Z}[[X_1, \ldots, X_n]](7.1.1.1)$, as here we are taking a completion.

**Def.(7.5.3.4)[Multiplication Map].** Let $G$ be a commutative formal group law over $R$ and $m \in \mathbb{Z}$, then we can define a group homomorphism $[m] : G \to G$ inductively as follows:

$$[0](X) = 0, \quad [m+1](X) = G([m](X), X), \quad [m-1](X) = G([m](X), i(X)).$$

Then it can be verified that this is well-defined and $[m]$ is a group homomorphism.

**Prop.(7.5.3.5) [Multiplications as Automorphisms].** Let $G$ be a commutative formal group law over $R$ and $m \in \mathbb{Z}$, then $[m](X) = mX + o(X)$. In particular, if $m$ is invertible in $R$, then $[m]$ is an automorphism of $G$, by (7.5.1.3).

**Prop.(7.5.3.6).** $G_a$ is the one-dimensional formal group with $G_a(X, Y) = X + Y$, $G_m$ is the one-dimensional formal group with $G_m(X, Y) = X + Y + XY$. Over a $\mathbb{Q}$-algebra $K$, there is an isomorphism between $G_a$ and $G_m$ giving by $X \mapsto \exp(X) - 1$.

**Def.(7.5.3.7)[Invariant Differential Forms].** An invariant differential form on a formal group law $G$ over $R$ is an element $\omega = \sum a_i(X)dX_i \in \Omega^1_{R[[X]]/R}$ that satisfies $(Y \mapsto G(X, Y))_* \omega = \omega$, i.e.

$$\sum_j a_j(Y)dY_j = \sum_i a_i(G(X, Y)) \frac{\partial G_i}{\partial Y_j}(X, Y)dY_j.$$ 

If $G$ is commutative, then this is equivalent to $\mu_* \omega = i_1 \omega + i_2 \omega$.

**Prop.(7.5.3.8).** The mapping $\omega \mapsto (u_1(0), \ldots, u_n(0))$ is an isomorphism of the $R$-module of invariant differential forms and $R^n$.

**Proof:** Cf.[Zin84]P14.

**Prop.(7.5.3.9)[Pullback of Invariant Differential Forms].** Let $\varphi : G \to H$ be a homomorphism of formal group laws, then for any invariant differential form $\omega = \sum a_i(X)dX_i$ on $H$, $\varphi^* \omega$ is a differential form on $G$, given by expanding $\sum a_i(\varphi(X))d(\varphi_i(X))$. 

**Proof:**
7.5. FORMAL GROUPS AND P-DIVISIBLE GROUPS

Proof:

\[(Y \mapsto G(X,Y))^* \phi^* \omega = \sum a_i(\phi(G(X,Y)))d(\phi(G(X,Y))) \]
\[= \sum a_i(H(\varphi(X),\varphi(Y)))d(H(\varphi(X),\varphi(Y))) \]
\[= \sum a_i(\varphi(Y))d(\varphi(Y)) \]
\[= \varphi^* \omega \]

\[\square\]

Def. (7.5.3.10) [Invariant Differential Operators]. An invariant differential operator on a formal group \(G\) of dimension \(n\) is a differential operator \(D\) s.t.

\[\mu \circ D = (1 \otimes D) \circ \mu.\]

Equivalently, if \(D = \sum_i u_i(Z) \frac{\partial}{\partial Z_i}\), it satisfies

\[\sum_j u_j(Y) \frac{\partial G_i}{\partial Y_j} = u_i(G(X,Y)).\]

The space of invariant operators is stable under composition. The \(R\)-algebra of invariant differential operators on \(G\) is denoted by \(DO_G\).

Prop. (7.5.3.11). The space of invariant differential operators on \(G\) of order \(\leq N\) are in bijection with the space of \(K\)-linear maps \(l: K[[X]] \to K\) s.t. \(l((X)^{N+1}) = 0\) via

\[Df(X) = (1 \otimes l)f(G(X,Y)).\]


\[\square\]

Cor. (7.5.3.12) [Basis of Invariant Differential Operators]. For any \(f \in K[[X]]\), write \(f(G(X,Y)) = \sum_\alpha (H_\alpha f)(X)Y^\alpha\).

Then \(H_\alpha\) are differential operators of order \(|\alpha|\), and the space of invariant differential operators of order \(N\) form a free \(R\)-module with basis \(H_\alpha\). In particular, the space of invariant derivatives is isomorphic to \(R^n\).

Proof: By (7.5.3.11),

\[Df(X) = (1 \otimes l)f(G(X,Y)) = (1 \otimes l)(\sum_\alpha (H_\alpha f)(X)Y^\alpha) = \sum_\alpha l(Y^\alpha)(H_\alpha f)(X).\]

\[\square\]

Cor. (7.5.3.13) [Composition of Invariant Differential Operators]. Let \(D_1, D_2 \in DO_G\), then

\[(D_1 \circ D_2)f(Z) = (1 \otimes l_1 \otimes l_2)f(G(Z, G(X,Y))),(\]

in particular,

\[l_{D_1 \circ D_2}(f) = (l_1 \otimes l_2)f(G(X,Y)).\]
Proof:
\[(D_1 \circ D_2) f(Z) = D_1(1 \otimes l_1) f(G(Z, Y)) = (1 \otimes l_2 \otimes 1)(1 \otimes 1 \otimes l_1) f(G(G(Z, X), Y)) = (1 \otimes l_1 \otimes l_2) f(G(Z, G(X, Y))).\]

\[\square\]

Prop. (7.5.3.14) [Pushforward of Invariant Differential Operators]. A homomorphism \( \varphi \) of formal groups \( G \to H \) induces a map from the linear maps \( l : K[[X]] \to K \) to linear maps \( l \circ \varphi^* : K[[\lambda]] \to K \), which induces a \( K \)-homomorphism of algebras \( \varphi_* : \mathcal{D}_H \to \mathcal{D}_G \).

\[\text{Proof:}\] To show preserves algebra structure, notice for any \( f \in R[[\lambda]] \), by (7.5.3.13),
\[\varphi_*(D) \circ \varphi_*(D') f(0) = (l \circ \varphi^*) \circ (l' \circ \varphi^*) f(H(X, Y)) = (l \otimes l') f(H(\varphi(X), \varphi(Y))) = [(l \otimes l') \circ \varphi^*] f(G(X, Y)) = \varphi_*(D \circ D') f(0).\]

Thus \( \varphi_*(D) \circ \varphi_*(D') = \varphi_*(D \circ D') \), by (7.5.3.11).

\[\square\]

Prop. (7.5.3.15) [Q-Theorem]. Any commutative connected formal group over a \( \mathbb{Q} \)-algebra \( R \) is a direct sum of \( \mathbb{G}_a \).


1-dimensional Formal Groups

Def. (7.5.3.16) [Normalized Invariant Differential Form]. For a 1-dimensional formal group \( G \) over \( R[[X]] \), the module of invariant differentials is isomorphic to \( R(7.5.3.10) \). An invariant differential form \( \omega = P(T)dT \) is called normalized if \( P(0) = 1 \).

Then the unique normalized invariant differential form on \( G \) is given by \( \omega_G = G_X(0, T)^{-1}dT \).

\[\text{Proof:}\] We need to check \( G_X(0, G(T, S))^{-1}G_X(T, S) = G_X(0, T)^{-1} \), and this is just \( G(U, G(T, S)) = G(G(U, T), S) \) differentiated at \( U \) and let \( U = 0 \).

\[\square\]

Prop. (7.5.3.17). For a morphism \( \varphi : \mathcal{F} \to \mathcal{G} \) of 1-dimensional formal groups laws over \( R \), \( \varphi^* \omega_\mathcal{G} = \varphi'(0) \omega_\mathcal{F} \).

\[\text{Proof:}\] By (7.5.3.9), \( \varphi^* \omega_\mathcal{G} \) is an invariant differential form, and compare their constant coefficients.

\[\square\]

Cor. (7.5.3.18). Let \( p \) be a prime, then for any formal group law of dimension 1,
\[ [p](T) = pf(T) + g(T^p) \]
for some \( f(0) = g(0) = 0 \).

\[\text{Proof:}\] If suffices to show that \( [p]'(T) \subset pR[[T]] \). But by (7.5.3.17) and (7.5.3.5),
\[ p^* \omega(T) = [p]^* \omega(T) = G_X(0, [p](T))^{-1}[p]'(T)dT \]
so this is true.

\[\square\]
Def. (7.5.3.19) [Formal Logarithm]. When \( R \) is torsion-free, the formal logarithm \( \log_F \) for a 1-dimensional formal group is the integration of invariant differential

\[
\int_0^T \omega_F = T + \frac{c_1}{2} T^2 + \cdots \in (R \otimes \mathbb{Q})[[T]].
\]

Then the formal power exponential is the the unique power series \( \exp_F \) that is the inverse of \( \log_F \). It exists uniquely by (7.5.1.3), and by (7.5.1.4), it is of the form

\[
\exp_F = \sum_{n \geq 1} b_n T^n \in (R \otimes \mathbb{Q})[[T]], b_n \in R.
\]

Prop. (7.5.3.20). For \( R \) is torsion-free and an 1 dimensional formal group \( F \) over \( R \),

\[
\log_F : F \to \mathbb{G}_a
\]

is an isomorphism of formal groups laws over \( R \otimes_{\mathbb{Z}} \mathbb{Q} \).

And if \( F \) is a formal \( R \)-module, then it is an isomorphism of \( R \)-modules, because from (7.5.3.17) that \( \omega_F \circ [a] = a \omega_F \), thus \( \log_F \circ [a] = a \cdot \log_F \).

Proof: From \( \omega_F(F(T, S)) = \omega_F(T) \), we get that \( \log_F(F(T, S)) = \log_F(S) + \log_F(T) \). So it is a homomorphism. Now the inverse \( \exp_F \) is already given, so it is an isomorphism.

\[ \square \]

Cor. (7.5.3.21) [1-Dimensional Formal Group Law is Commutative]. Any 1-dimensional formal group over a ring \( R \) that has no torsion nilpotents is commutative.

Proof: We only prove for \( R \) torsion free. \( F(T, S) = \exp_F(\log_F(T) + \log_F(S)) \).

\[ \square \]

Lubin-Tate Formal Group Law

Def. (7.5.3.22) [Lubin-Tate Formal Group Law]. For a \( p \)-adic number field \( K \) with a uniformizer \( \pi_K \) with residue field \( \mathbb{F}_q \), a Lubin-Tate power series for \( \pi_K \) is a \( \varphi(X) \in \mathcal{O}_K[[X]] \) that \( \varphi(X) \equiv \pi_K X \mod X^2 \) and \( \varphi(X) \equiv X^q \mod \pi_K \).

A Lubin-Tate module \( G \) over \( \mathcal{O}_K \) is a formal \( \mathcal{O}_K \)-module that \( [\pi_K](X) \) is a Lubin-Tate power series.

Prop. (7.5.3.23). Given a \( p \)-adic number field \( K \) with residue field \( \mathbb{F}_q \), we consider the set \( \xi_\pi \) of all Lubin-Tate power series for \( \pi \).

If \( f, g \in \xi_\pi \) and \( L(X) = \sum a_i X_i \) be a linear form, then there exists a unique power series \( F(X) \) that \( F(X) \equiv L(X) \mod (X)^2 \) and \( f(F(X)) = f(g(X)) \).

Proof: Choose \( F \) consecutively, if \( F_{r+1} = F_r + \Delta_r \), then must

\[
\Delta \equiv \frac{f(F_r(X)) - F_r(g(X))}{\pi^{r+1} - \pi} \mod \text{degree } (r + 2).
\]

This has coefficient in \( \mathcal{O} \) because \( f \equiv g \equiv Z^q \mod \pi \).

\[ \square \]

Cor. (7.5.3.24). If we let \( f = g, L = X + Y \) to get \( F_f \) and \( f, g, L = aX \) to get \( a_{f,g} \), then

- \( F_f(X, Y) = F_f(Y, X) \).
- \( F_f(F_f(X, Y), Z) = F_f(X, F_f(Y, Z)) \).
• \(a_f g(F_g(X, Y)) = F_f(a_f g(X), a_f g(Y))\).
• \(a_f b_f(Z) = (ab)_f(Z)\).
• \((a + b)_f(Z) = F_f(a_f(Z), b_f(Z))\).
• \(\pi_f(Z) = f(Z)\).

all follow from the unicity of the last proposition.

**Cor. (7.5.3.25) [Existence of Lubin-Tate Module]**. We get a commutative formal \(O\)-module \(F_f\) for every \(f\). And this group can act on \(\mathfrak{p}_L\) for an alg.ext \(L/K\). The set of zeros \(\Lambda_{f,n}\) of \(f^n\) in \(L\), as the elements annihilated by \(\pi^n\), is a submodule of \(\mathfrak{p}_L^{(f)}\).

And \(u_{g,f}\) for any unit \(u \in O\) defines an isomorphism between \(F_f\) and \(F_g\), thus this formal group only depends on \(\pi\), called \(F_{\pi}\). Hence \(L_{f,n} = K(\Lambda_{f,n})\) only depends on \(\pi\), with Galois group \(G_{\pi,n}\).

**Prop. (7.5.3.26) [Different Uniformizers]**. Now consider different \(\pi\), it is proven that \(F_{\pi}\) and \(F_{\pi'}\) are isomorphic, but the coefficient in \(O_{\pi}\) is \(T\) the maximal unramified extension.

Thus \(L_{\pi,n}\) and \(L_{\pi',n}\) may not be isomorphic, but \(T.L_{\pi,n} = T.L_{\pi',n}\) since \(\hat{T}.L_{\pi,n} = \hat{T}.L_{\pi',n}\) and both of them is the algebraic closure of \(K\) in it.

**Proof**: Cf.[Neukirch CFT P105].

**Lemma (7.5.3.27)**. The Newton polygon of \([\pi^n]\) has vertices

\[(1, 0), (q, -1/e_K), (q^2, -2/e_K), \ldots.\]

**Proof**: Notice \([\pi^n]\) has no infinite edge of negative slope because all its coefficient are in \(O_K\). Now look at its roots, it has a root 0, and \(q - 1\) roots of valuation \(v_p(\pi_K)/(q - 1)\), \(q(q - 1)\) roots of valuation \(v_p(\pi_K)/q(q - 1)\), and so on. So by factor out these roots, \([\pi^n]/\pi_K^n\) is left with a power series whose Newton polygon is a single line, which shows the desired result.

**Prop. (7.5.3.28)**. The formal logarithm of the Lubin-Tate formal group \(F_{\pi}\) satisfies:

\[\log_{F_{\pi}}(T) = \lim_{n \to \infty} [\pi^n]/\pi^n.\]

**Proof**: By(7.5.3.20) we have

\[\log_{F}(T) = \log_{F}([\pi^n]) = ([\pi_k^n] + a_2/2[\pi_k^n]^2 + \ldots)/\pi^n_k\]

and for any degree \(n\), the coefficient of \([\pi^{2n}_K]/\pi^{2n}_K\) is bounded below by a \(c(n)\), so \([\pi^{2n}_K]/\pi^{2n}_K\) converges to 0, thus the result.

**Cor. (7.5.3.29)**. The Newton polygon of \(\log_{F}(T)\) has vertices \((1, 0), (q, -1/e_K), (q^2, -2/e_K), \ldots.\)

The discussion is continued at 2.

4 Formal Groups

**Prop. (7.5.4.1) [Formal Group Law as Functors]**. Let \(\text{Nil}_R\) be the Abelian category of nilpotent commutative (non-unital) \(R\)-algebras, then the category of commutative formal group law are equivalent to Abelian functors on \(\text{Nil}\) whose underlying set-theoretic functor if \(N \mapsto N^n\).
Proposition (7.5.4.5). Let $G$ be a commutative formal group law defined over a complete local ring $(R, m)$, then

- For each $n$, $G(m^n)/G(m^{n+1}) \cong m^n/m^{n+1}$ as groups.
- Let $p$ be the characteristic of the residue field $k$ ($p$ may be 0), then $\mathcal{F}(m)_{\text{tor}} = \mathcal{F}(m)[p^\infty]$.

Proof: 1: This is because $F(x, y) \equiv x + y \mod m^n$.
2: This is because $[m]$ is an automorphism by (7.5.3.5) as $m$ is invertible in $R$.

1-Dimensional Commutative Formal Groups over DVR

Proposition (7.5.4.6). Let $(R, m)$ be a CDVR with residue field $k$ of characteristic $p$, $\mathcal{F}$ a formal group law over $R$. Then $\mathcal{F}(m)_{\text{tor}} = \mathcal{F}[p^\infty]$, and if $x \in \mathcal{F}(m)$ has exact order $p^n$, then $v(x) \leq \frac{v(p)}{p^n - p^{n-1}}$.

Proof: 1: Then $\mathcal{F}(m)[m] = 0$ by (7.5.3.5).

By (7.5.3.18), $[p](x) = pf(x) + g(x^p)$, where $f(0) = 1$. Thus it is possible only if $pv(x) \geq v(p^x)$, which means $v(x) \leq v(p)/(p-1)$.

Now if this is true for $n \geq 1$, let $x \in \mathcal{F}(m)$ with order $p^{n+1}$, then $v([p](x)) = v(pf(x) + g(x^p)) \geq \min(v(px), pv(x))$. But $[p](x)$ has order $p^n$, thus $\frac{v(p)}{p^n - p^{n-1}} \geq \min(v(px), pv(x))$. But $n \geq 1$ and $v(x) > 0$, it is impossible that $\frac{v(p)}{p^n - p^{n-1}} \geq v(px)$, thus we have $\frac{v(p)}{p^n - p^{n-1}} \geq v(px)$.

Proposition (7.5.4.7). Let $(R, m)$ be a complete DVR of characteristic $p$ with residue field $k$ of characteristic $p$, $\mathcal{F}$ a formal group law over $K$, then

- the formal logarithm (7.5.3.19) induces an homomorphism $\log_\mathcal{F} : \mathcal{F}(m) \to K$.
- For $r > \frac{v(p)}{p - 1}$, $\log_\mathcal{F}$ is an isomorphism $\log_\mathcal{F} : \mathcal{F}(m^r) \cong m^r$.

Proof: 1: This follows from determining the convergence of $\log_\mathcal{F}$ and $\exp_\mathcal{F}$ by (12.1.3.22), after which it is a homomorphism by (7.5.3.20).
Prop. (7.5.4.9) [Zp-Multiplication]. Let \((R, m)\) be a CDVR with residue field \(k\) of characteristic \(p\), \(F\) a formal group law over \(R\), then for any \(x \in F(m)\), \(\lim_{n \to \infty} [p^n](x) \to 0\).

In particular, we can define \([α](x)\) for any \(α \in \mathbb{Z}_p\).

Proof: By (7.5.3.18), \(v([p](x)) = v(pf(x) + g(x^p)) \geq \min(v(x) + v(p), pv(x))\). □

5 Cartier Theory

Main References are [Zin84].

Isogenies of Formal Groups

Def. (7.5.5.1) [Heights over Positive Characteristic]. Let \(R\) be a ring of characteristic \(p > 0\), \(φ : F \to G\) be a homomorphism of formal group laws over \(R\) of dimension 1, the **height of homomorphism** \(ht(φ)\) is the largest integer \(h\) s.t. \(φ(T) = g(T^h)\) for some \(h\).

For a formal group law \(F\) over \(R\), the **height of formal group law** \(ht(F)\) is \(ht([p]F)\). By (7.5.3.18), the height is always positive.

Prop. (7.5.5.2). Let \(R\) be a ring of characteristic \(p > 0\), \(f : F \to G\) be a homomorphism of formal group laws over \(R\) of dimension 1, then

- If \(f'(0) \neq 0\), then \(ht(f) > 0\).
- If \(f = g(T^h)\) with \(h = ht(f)\), then \(g'(0) \neq 0\).

In particular, the first non-zero term of \(f(T)\) is \(T^h\), where \(h\) is the height of \(f\).

Proof: 1: Let \(ω_F, ω_G\) be the normalized invariant differential forms of \(F\) and \(G\), then

\[
0 = f'(0)ω_F(T) = ω_G(f(T)) = G_X(0, T)^{-1}f'(T)dT,
\]

thus \(f'(T) = 0\), which means \(ht(f) > 0\).

2: Let \(q = p^h\) and \(F(q)(T) = F(X^{1/q}, Y^{1/q})^q\). Then it is easy to see \(F(q)\) is another formal group law, and \(g\) is a homomorphism from \(F(q)\) to \(F\):

\[
g(F(q)(X^q, Y^q)) = g(F(X, Y)^q) = f(F(X, Y)) = F(f(X), f(Y)) = F(g(X^q), g(Y^q)).
\]

Which means \(g(F(q)(X, Y)) = F(g(X), g(Y))\). Thus if \(g'(T) = 0\), by item1, \(g(T) = g_1(T^p)\), contradicting \(h = ht(f)\). □

Prop. (7.5.5.3). Let \(F \xrightarrow{f} G \xrightarrow{g} H\) be homomorphisms of formal group laws over ring \(R\) of characteristic \(p > 0\), then \(ht(g \circ f) = ht(f) + ht(g)\).

Proof: Let \(f(T) = f_1(T^{ht(f)})\), \(g(T) = g_1(T^{ht(g)})\), where \(f_1(0) \neq 0, g_1(0) \neq 0\) by (7.5.5.2), then

\[
g \circ f(T) = g_1(f_1(T^{ht(f)})^{ht(g)}) = g_1(\tilde{f}_1(T^{ht(f)+ht(g)}))
\]

where \(g_1(0)\tilde{f}_1(0) \neq 0\), thus by (7.5.5.2) again, \(ht(g \circ f) = ht(f) + ht(g)\). □
6 $p$-divisible Groups

Def.(7.5.6.1) [$\Lambda$-Formal Schemes]. Let $\Lambda$ be a local complete Noetherian ring and $A^f_\Lambda$ be the category of finite length(Artinian) $\Lambda$-algebra,

Then a $\Lambda$-formal functor is a functor $A^f_\Lambda \to \text{Set}$.

The formal completion of a functor $A_\Lambda \to \text{Set}$ is its restriction on $A^f_\Lambda$. We denote the formal completion of $\text{Spec } A$ by $\text{Spf } A$.

Then a $\Lambda$-formal scheme is a filtered colimits of functors $\lim \to \text{Spf } A_i$, or equivalently a profinite $\Lambda$-algebra $A = \lim \leftarrow A_i$ with profinite topology.

Def.(7.5.6.2) [$\Lambda$-Formal Group Schemes]. A $\Lambda$-formal group is a $\Lambda$-formal scheme with values in groups.

Def.(7.5.6.3) [$p$-Divisible Formal Lie Group Schemes]. A formal Lie group $\mathcal{G}$ over $\Lambda$ is a connected formally smooth $\Lambda$-formal group. It is necessarily isomorphic to $\mathcal{G} = \text{Spf } \Lambda[[X_1, \ldots, X_n]]$ where $n = \dim \mathcal{G}$. The number $n$ is called the dimension of $\mathcal{G}$.

A $p$-divisible formal Lie group is a commutative formal Lie group $\mathcal{G} = \text{Spf } \Lambda[[X_1, \ldots, X_n]]$ that multiplication by $p : [p]^* : \mathcal{G} \to \mathcal{G}$ is a finite flat morphism on $\Lambda[[X_1, \ldots, X_n]]$.

Def.(7.5.6.4) [$p$-Divisible Groups]. Let $p$ be a prime and $S$ a scheme, a $p$-divisible group is a commutative group functor on $\text{Sch}_{fppf}/S$ that

- $G$ is $p$-divisible: $[p]_G$ is an epimorphism.
- $G$ is $p$-torsion: $G = \lim \to G(n)$, where $G(n) = \ker([p]_G : G \to G)$.
- $G(n)$ are representable as sheaves on $\text{Sch}_{fppf}/S$.

The category of $p$-divisible groups over $S$ is denoted by $p\text{div}(S)$.

Prop.(7.5.6.5)[Equivalent Definitions of $p$-Divisible Groups]. Let $p$ be a prime and $S$ a scheme, then a $p$-divisible group over $S$ is an ind system $(G_v, i_v)$ of finite commutative groups schemes over $S$ s.t.

- $0 \to G_v \xrightarrow{i_v} G_{v+1} \xrightarrow{p^v} G_{v+1}$ is an exact sequence of group schemes over $S$.
- the rank of fiber of $G(n)$ at $s \in S$ is $p^{nh(s)}$ where $h$ is a locally constant function on $S$.
- $(G_v, i_v)$ is called a $p$-divisible group of height $h$ over $S$.

Proof: Cf.[Shatz, P61], [P-Divisible Groups, Haoran Wang].

Prop.(7.5.6.6)[Connected $p$-Divisible Groups and Formal Lie Groups]. Cf.[Shatz, P62].

Def.(7.5.6.7) [Tate Module]. Let $G$ be a $p$-divisible group over an integral domain $O$ with fraction field $K$ of characteristic 0, then the Tate module of $G$ is defined to be

$$T_p(G) = \lim \to G_n(K),$$

and the Tate comodule of $G$ is defined to be

$$\Phi_p(G) = \lim \to G_n(K).$$
Hodge-Tate Decomposition

Prop. (7.5.6.8) [Hodge-Tate Decomposition]. If $\mathcal{O}$ is a CDVR of mixed characteristic with perfect residue field $k$ and fraction field $K$, then there is an isomorphism of f.d. $\mathbb{Q}_p$-representation of $G_K$:

$$T_p(G) \otimes_{\mathbb{Z}_p} \mathbb{Q}_p \cong \text{tangent} \oplus \text{cotangent spaces of } G.$$ 

Proof: Cf. [p-divisible Groups, Morrow]. \qed
7.6 Geometric Invariant Theory
7.7 Moduli Problems

1 Schemes as Functors

Prop. (7.7.1.1) [Strong Yoneda Lemma]. For any $S \in \text{Sch}$, the functor

$$\text{Sch}_S \to \text{Sh}_{\text{fpqc}} / S \to \text{Sh}^{\text{set}}(\text{Aff}_{\text{fpqc}} / S) \to \text{Psh}^{\text{set}}(\text{Aff}_S) : X \mapsto (\tilde{X} : \text{Spec} R \mapsto \text{Mor}_S(\text{Spec} R, X))$$

is a fully faithful embedding of the categories.

Proof: (5.1.2.24) applied to $\text{Aff}_{\text{fpqc}} / S \to \text{Sch}_{\text{fpqc}} / S$ implies the restriction map $\text{Sh}_{\text{fpqc}} / S \to \text{Sh}(\text{Aff}_{\text{fpqc}} / S)$ is an equivalence, thus the assertion follows from Yoneda lemma and the fact $\text{Sh}^{\text{set}}(\text{Aff}_{\text{fpqc}} / S) \to \text{Psh}^{\text{set}}(\text{Aff}_S)$ is fully faithful. □

Def. (7.7.1.2) [Closed Subfunctors]. Let $S \in \text{Sch}$ and $Z$ be a subfunctor of $X \in \text{Psh}^{\text{set}}(\text{Aff}_S)$. $Z$ is called a closed subfunctor of $X$ if for any $T \in \text{Aff}_S$, $f \in \text{Mor}(h_T, X)$, the functor $Z \times_X h_T$ is represented by a closed subscheme of $T$.

Prop. (7.7.1.3) [Closed Subfunctor of Schemes]. Let $S \in \text{Sch}$ and $X \in \text{Sch}_S$, then the closed subfunctors of $\tilde{X}$ (7.7.1.2) are exactly of the form $\tilde{Z}$ for a closed subscheme $Z$ of $X$.

Proof: If $Z$ is a closed subscheme of $X$, then for any $f : h^A \to X$, $f^{-1}(Z)$ is the pullback of $Z$ along $\text{Spec} A \to X$, so it is a closed subscheme of $\text{Spec} A$. Conversely, if $Z$ is a closed subfunctor of $X$, then for each affine open subset $U$ of $X$, $Z \cap h_U$ is represented by a quotient of $\mathcal{O}(U)$ by some ideal $\mathcal{I}(U)$. Because of the uniqueness, $\mathcal{I}(U)$ and $\mathcal{I}(U')$ coincide on the intersection $U \cap U'$, thus $U \mapsto \mathcal{I}(U)$ defines a sheaf of ideals $\mathcal{I}$ on $X$.

Now $Z = h_{Z'}$, where $Z'$ is the closed subscheme of $X$ defined by $\mathcal{I}$, because for any $\text{Spec} R \to X$, the pullback of $Z$ and $Z'$ to $R$ are the same, because they are all closed subschemes of $\text{Spec} R$ and they are equal on an open covering of $\text{Spec} R$. (The pullback of the open coverings of $X$). Now if $\text{Spec} R \to X$ is represented by an element $\alpha \in X(R)$, $Z \times_X h^R(R)$ is the set $\{ \varphi \in \text{Hom}(R, R) | X(\varphi)(\alpha) \in Z(R) \}$. So $\text{id}_R \in Z \times_X h^R(R) \iff \alpha \in Z(R)$. From this we see that $Z(R) = Z'(R)$ for any $R$. □

Def. (7.7.1.4) [Open Subfunctors]. Let $S \in \text{Sch}$ and $Z$ be a subfunctor of $X \in \text{Psh}^{\text{set}}(\text{Aff}_S)$. $Z$ is called an open subfunctor of $X$ if for any $T \in \text{Aff}_S$, $f \in \text{Mor}(h_T, X)$, the functor $U \times_X h_T$ is represented by an open subscheme of $T$.

Prop. (7.7.1.5) [Open Subfunctor of Schemes]. Let $S \in \text{Sch}$ and $X \in \text{Sch}_S$, then closed subfunctors of $\tilde{X}$ (7.7.1.2) are exactly of the form $\tilde{U}$ for an open subscheme $U$ of $X$.

Proof: The proof is exactly the same as that of (7.7.1.3). □

Def. (7.7.1.6) [Open Coverings by Functors]. Let $S \in \text{Sch}$, an open covering of a functor $X \in \text{Psh}^{\text{set}}(\text{Sch}_S)$ is a family of open subfunctors $\{ U_i \}$ that for any $T \in \text{Aff}_S$, $h_T \times_X U_i$ is an open covering of $T$.

Prop. (7.7.1.7) [Open Coverings of Schemes]. Let $S \in \text{Sch}$ and $X \in \text{Sch}_S$, then open coverings of the functor $\tilde{X}$ are exactly open coverings of $X$.

Proof: The proof is exactly the same as that of (7.7.1.3). □

Prop. (7.7.1.8). The pullback of a closed subfunctor is also a closed subfunctor. The intersection of closed subfunctors is a closed subfunctor.
Lemma (7.7.1.9). Let $k$ be a field and $B \in \mathcal{C}\text{Alg}_k$, $X \in \mathcal{P}sh^\text{SET} (\mathcal{C}\text{Alg}_B)$, define
\[ X_* \in \mathcal{P}sh^\text{SET} (\mathcal{C}\text{Alg}_k) : X_*(R) = X(R \otimes_k B). \]
Then if $Z$ is a closed subfunctor of $X$, $Z_*$ is also a closed subfunctor of $X_*$. 

Proof: Let $A$ be a $k$-algebra, and $\alpha \in X_*(A)$. To prove $Z_*$ is closed in $X_*$, we need to show there exists an ideal $\alpha \subset A$ that for any homomorphism $\varphi : A \to R$,
\[ X_*(\varphi)(\alpha) \in Z_*(R) \iff \varphi(\alpha) = 0. \]
Because $Z$ is closed in $X$, there exists an ideal $b$ of $A \otimes_k B$ that for any $\varphi : A \to R$,
\[ X(\varphi \otimes B)(\alpha) \in Z_*(R) \iff (\varphi \otimes B)(b) = 0. \]
Now by (4.1.1.26), there is an ideal $a \subset A$ that an ideal $I$ of $A$ satisfies $b \subset I \otimes B \iff a \subset I$, thus we are done. \qed

Prop. (7.7.1.10). Let $S \in \text{Sch}$, $X \in \mathcal{P}sh^\text{SET} (\text{Aff}/S)$ and $Z$ a closed subfunctor of $X$. If $Y \in \text{Sch}_R$, then $\text{Mor}(h_Y, Z)$ is a closed subfunctor of $\text{Mor}(h_Y, X)$. 

Proof: If $Y = h^B$, then $\text{Mor}(Y, X)(R) = X(B \otimes R)$, thus the conclusion follows from (7.7.1.9). For a general $Y$, let $Y_i$ be an affine open covering of $Y$, then there are maps $\rho_i : \text{Hom}(Y, X) \to \text{Hom}(Y_i, X)$. Now $\text{Hom}(Y, Z)$ is closed subfunctor of $\text{Hom}(Y_i, X)$, thus we are done if we can show that $\text{Hom}(Y, Z) = \cap_i \rho_i^{-1}(\text{Hom}(Y_i, Z))$. But this is equivalent to any map $Y_R \to X_R$ that maps $(Y_i)_R$ into $Z_R$ maps $Y_R$ into $Z_R$, which is clear. \qed

Def. (7.7.1.11) [Fat Subfunctors]. Let $S \in \text{Sch}$ and $\mathcal{F} \in \mathcal{S}h^{\text{SET}} (\text{Aff}_{\text{fppf}}/S)$, then a subfunctor $D$ of $\mathcal{F}$ is called a fat subfunctor if the shifification of $D$ w.r.t. the fppf topology is just $\mathcal{F}$. 

Prop. (7.7.1.12) [Extending Group Structures]. Let $S \in \text{Sch}$, $\mathcal{F} \in \mathcal{S}h^{\text{SET}} (\text{Aff}_{\text{fppf}}/S)$ and $D$ a fat subfunctor of $\mathcal{F}$, then every group structure on $D$ extends uniquely to a group structure on $\mathcal{F}$ by shifification.

Representability

Prop. (7.7.1.13) [A Representability Criterion]. Let $\mathcal{F} \in \mathcal{S}h^{\text{SET}} (\text{Sch}_{\text{Zar}})$ and there is a covering $\mathcal{F} = \cup F_i$ by open subfunctors (7.7.1.4)(7.7.1.6) that are representable by schemes, then $\mathcal{F}$ is representable by a scheme. 

Proof: Let $(X_i, \xi_i)$ represents $F_i$, where $\xi_i \in F_i(X_i)$. Because $F_j \subset F$ is representable by open immersion, there are open subsets $U_{ij} \subset X_i$ that $T \to X_i$ factors through $U_{ij}$ iff $\xi_j | T \in F_j(T)$. In particular, $\xi_i | U_{ij} \subset F_j(U_{ij})$, and therefore there is a canonical map $\varphi_{ij} : U_{ij} \to X_j$ that $\varphi_{ij}^* \xi_j = \xi_i | U_{ij}$. By definition of $U_{ij}$ this map factors through $U_{ji}$. 

For the rest, Cf. [Sta]01JJ. \qed

Cor. (7.7.1.14) [Representing Group Functors]. Let $S \in \text{Sch}$ and $\mathcal{G} \in \mathcal{S}h^{\text{SET}} (\text{Aff}_{\text{Zar}}/S)$ and there is an open subfunctor $\mathcal{F} \subset \mathcal{G}$ s.t. for any Spec $K \in \text{Aff}_S$ where $K$ is a field and $g \in \mathcal{G}(K)$, there exists a $g' \in G(k)$ s.t. $gg' \in \mathcal{F}(K)$, then $\mathcal{G}$ is representable.
Prop. (7.7.2.15) [Hom(\mathcal{E}, \mathcal{F}) for Coherent Sheaves]. Let $S$ be a locally Noetherian scheme and $X$ a projective scheme over $S$. Let $\mathcal{E}, \mathcal{F}$ be coherent sheaves on $X$ and $\mathcal{F}$ is flat, then the functor

$$\text{Hom}(\mathcal{E}, \mathcal{F}) : \text{Sch}_S \to \text{Set} : T \mapsto \text{Hom}_T(\mathcal{E}_T, \mathcal{F}_T)$$

is representable by a vector bundle $V$ over $S(5.5.2.21)$.

Proof: Cf. [Kle05]P16.

Cor. (7.7.1.16). For any $f \in \text{Hom}(\mathcal{E}, \mathcal{F})$, $f$ corresponds to a morphism $X \to Y$, then the inverse image of $V \subset Y$ in $X$ is the closed subscheme $X'$ with the universal property that for any $\varphi : T \to X$, $\varphi^*f = 0$ iff $\varphi$ factors through $X'$.

2 Hilbert & Quot Schemes

References are [Nit05]. For simplicity, we restrict to the category of locally Noetherian schemes over $S$, and assume $X/S$ is separated.

Def. (7.7.2.1) [Hilbert Functors]. Let $X \in \text{Sch}_S$, then the Hilbert functor is the functor

$$\text{Hilb}_{X/S} : \text{Sch}_S \to \text{Set} : T \mapsto \text{closed subschemes of } X_T \text{ that is flat over } Z \}.$$

Def. (7.7.2.2) [Quot Functors]. Let $S$ be a locally Noetherian scheme and $f : X \to S$ be a f.t. scheme over $S$ and $\mathcal{E} \in \text{Coh}(X)$, then for any $T \in \text{Sch}_S$, define a family of quotients of $\mathcal{E}$ parametrized by $T$ to be a pair $(\mathcal{F}, q)$ where

- $\mathcal{F} \in \text{Coh}(X_T)$ s.t. $\text{Supp}(\mathcal{F})$ is proper over $T$.
- A surjective homomorphism of sheaves $q : \mathcal{F}_T \to \mathcal{F}$.

Then the Quot functor is the functor

$$\text{Quot}_{\mathcal{E}/X/S} : \text{Sch}_S \to \text{Set} : T \mapsto \{ \text{isomorphism classes of family of quotients of } \mathcal{E} \text{ parametrized by } T \}.$$

Cor. (7.7.2.3) [Hilbert Functors as Quot Functors]. $\text{Hilb}_{X/S} = \text{Quot}_{\text{Coh}/X/S}$

Prop. (7.7.2.4) [Quot_{\mathcal{F}/X/S} are Fpqc Sheaves]. $\text{Quot}_{\mathcal{F}/X/S}$ are fpqc sheaves.

Proof: This follows from the fact $\text{Coh}/\text{Sch}$ is a fpqc sheaf $(5.1.5.12)$.

Prop. (7.7.2.5) [Stratification by Hilbert Polynomials]. Let $\mathcal{L}$ be a line bundle on $X_T$, then for any line bundle $\mathcal{L}$ on $X_T$, then for any $t \in T$, the Hilbert polynomial of $\mathcal{F}_t$ w.r.t. the line bundle $\mathcal{L}_t$ on $X_t$ is locally constant on $T$, and is stable under extension of residue fields, thus we can define $\text{Quot}^{\Phi, \mathcal{L}}_{\mathcal{E}/X/S}$ to represent the subfunctor of $\text{Quot}_{\mathcal{E}/X/S}$ consisting of pairs $(\mathcal{F}, q)$ s.t. $\mathcal{F}_t$ has Hilbert polynomial $\Phi$ w.r.t. $\mathcal{L}_t$ for all $t \in T$.

Then if each $\text{Quot}^{\Phi, \mathcal{L}}_{\mathcal{E}/X/S}$ is representable, $\text{Quot}_{\mathcal{E}/X/S}$ is also representable, and there is a decomposition

$$\text{Quot}_{\mathcal{E}/X/S} = \coprod_{\Phi \in \mathbb{Q}[\lambda]} \text{Quot}^{\Phi, \mathcal{L}}_{\mathcal{E}/X/S}.$$
Prop. (7.7.2.6) [Valuation Criterion]. Let \( X \to S \) be proper, then the morphism of functors \( \text{Quot}_{\mathcal{E}|s/X/S}^\Phi,\mathcal{L} \to h_S \) satisfies the discrete valuation criterion for properness.

Proof: The valuation criterion says if \( R \) is a valuation ring with fraction field \( K \) with a morphism \( \text{Spec} \, R \to S \), then any pairs \((\mathcal{F}_K, q_K)\) where \( \mathcal{F}_K \in \text{Coh}(X_K) \) and \( q_K : \mathcal{E}_K \to \mathcal{F}_K \) a surjection can extends uniquely to a surjective map \( q_R : \mathcal{E}_R \to \mathcal{F}_R \in \text{Coh}(X_R) \) s.t. \( \mathcal{F}_R \) is flat over \( R \).

For this, let \( j : X_K \to X_R \) be the open immersion, take \( \mathcal{F}_R \) to be the image of the map \( \mathcal{E}_R \to i_*\mathcal{E}_K \xrightarrow{i*q_K} i_*\mathcal{F}_K \), then \( i^*\mathcal{F}_R = \mathcal{F}_K \), and \( \mathcal{F}_R \) is flat over \( R \) because it is torsion-free (4.4.1.12). Notice the properness of \( X/S \) is used to show that \( \text{Supp}(\mathcal{F}) \subset X_R \) is proper over \( R \).

\( \square \)

Lemma (7.7.2.7) [Preliminary Reductions]. Situation as in (7.7.2.2), then

- Let \( \nu \in \mathbb{Z} \), then tensoring \( \mathcal{L}' \) gives an isomorphism of functors \( \text{Quot}_{\mathcal{E}|s/X/S}^\Phi,\mathcal{L} \cong \text{Quot}_{\mathcal{E}(\nu)|s/X/S}^\Phi,\mathcal{L} \), where \( \Psi(\lambda) = \Phi(\lambda + \nu) \).

- Let \( \varphi : \mathcal{E} \to \mathcal{G} \) be a surjective homomorphism in \( \text{Coh}(X) \), then the corresponding natural transformation \( \text{Quot}_{\mathcal{G}|s/X/S}^\Phi,\mathcal{L} \to \text{Quot}_{\mathcal{E}|s/X/S}^\Phi,\mathcal{L} \) is a closed subfunctor.

- If \( X/S \) is proper, let \( i : U \to X \) be an open subscheme, then \( \text{Quot}_{i^*\mathcal{E}|s/U/S}^\Phi,\mathcal{L} \) is an open subfunctor of \( \text{Quot}_{\mathcal{E}|s/X/S}^\Phi,\mathcal{L} \).

Proof: 1 is obvious.

2: It suffices to show for any locally Noetherian scheme \( T \in \text{Sch}_S \) and a pair \((\mathcal{F}, q) \in \text{Quot}_{\mathcal{E}|s/X/S}(T)\), there exists a closed subscheme \( T' \) of \( T \) s.t. for any locally Noetherian scheme \( U \) and \( f : U \to T \), \( q_U : \mathcal{E}_U \to \mathcal{F}_U \) factors through \( \mathcal{G}_U \) iff \( f \) factors through \( T' \). For this, just take \( T' \) to be the vanishing scheme of \( \ker(\varphi_T) \to \mathcal{E}_T \to T = F_T(7.7.1.16) \) (or by direct verification).

3: Firstly the natural transformation \( \text{Quot}_{i^*\mathcal{E}|s/U/S}^\Phi,\mathcal{L} \to \text{Quot}_{\mathcal{E}|s/X/S}^\Phi,\mathcal{L} \) is given by

\[ \eta_T : (\mathcal{F}, i^*\mathcal{E}_T \to \mathcal{F}) \mapsto (\text{Im}(\mathcal{E}_T \to i_*\mathcal{F}), \text{adjunction}) \]

Notice restriction is a left inverse to this transformation. Then by inspection, this is an open subfunctor iff for any locally Noetherian scheme \( T \in \text{Sch}_S \) and a pair \((\mathcal{F}, q) \in \text{Quot}_{\mathcal{E}|s/X/S}(T)\), for any locally Noetherian scheme \( Q \) and \( f : Q \to T \), the restriction of \((\mathcal{F}, q)\) to \( Q \) is in \( \text{Quot}_{i^*\mathcal{E}|s/U/S}(Q) \) iff \( \mathcal{F}_Q \to i_Q^*\mathcal{E}_Q \) is injective.

\( \square \)

Thm. (7.7.2.8) [Grothendieck]. Let \( S \) be a Noetherian scheme and \( f : X \to S \) a (quasi-)projective morphism, \( \mathcal{L} \) an \( f \)-very ample line bundle on \( X \), then for any coherent \( \mathcal{O}_X \)-module \( \mathcal{E} \) and any polynomial \( \Phi \in \mathbb{Q}[\lambda] \), the functor \( \text{Quot}_{\mathcal{E}|s/X/S}^\Phi,\mathcal{L} \) is representable by a (quasi-)projective \( S \)-scheme.


For the quasi-projective case, use (7.7.2.7) and the fact any coherent sheaf can be extended.

Remark (7.7.2.9). Cf. [Hartshorne Appendix B, 3.4.1] has an example of a 3-dimensional smooth proper scheme over \( \mathbb{C} \) with a free \( G = \mathbb{Z}/(2) \)-action for which the quotient \( X/G \) is not a scheme. Which means that \( \text{Hilb}_{X/C} \) is not representable by a scheme.

Cor. (7.7.2.10). Let \( S \) be a locally Noetherian scheme and \( f : X \to S \) be \( H \)-projective, \( \mathcal{L} = \mathcal{O}_{P^2(1)}(1)|X_\mathcal{E} \), \( \mathcal{E} \) a coherent quotient sheaf of \( \mathcal{O}_{P^2(1)}(\nu) \) where \( p > 0, \nu \in \mathbb{Z} \), and \( \Phi \in \mathbb{Q}[\lambda] \), then he functor \( \text{Quot}_{\mathcal{E}|s/X/S}^\Phi,\mathcal{L} \) is representable by an \( H \)-projective \( S \)-scheme.
Lemma (7.7.2.11) [Altman-Kleinman]. Let $S$ be a locally Noetherian scheme and $f : X \to S$ be a closed subscheme of some $\mathbb{P}_S(V)$ where $V$ is a finite locally free sheaf on $S$, $\mathcal{L} = \mathcal{O}_{\mathbb{P}_S(V)(1)}|_X$, $\mathcal{E}$ a coherent quotient sheaf of $f^*(W)(\nu)$ where $W$ is a finite locally free sheaf on $S$ and $\nu \in \mathbb{Z}$, and $\Phi \in \mathbb{Q}[\lambda]$, then the functor $\text{Quot}_{\mathcal{E}/X/S}^{\Phi,\mathcal{L}}$ is representable by a projective $S$-scheme that can be embedded in $\mathbb{P}_S(F)$ for some finite locally free sheaf $F$ on $S$ that is an exterior power of $W$ with a symmetric power of $V$.

Proof: Cf.[Nit05]P24. □

Lemma (7.7.2.12). Let $S$ be a locally Noetherian scheme and $f : X = \mathbb{P}_S(V) \to S$ where $V$ is a finite locally free sheaf on $S$, $\mathcal{L} = \mathcal{O}_{\mathbb{P}_S(V)(1)}$, $\mathcal{E} = f^*(W)(\nu)$ where $W$ is a finite locally free sheaf on $S$ and $\nu \in \mathbb{Z}$, and $\Phi \in \mathbb{Q}[\lambda]$, then the functor $\text{Quot}_{\mathcal{E}/X/S}^{\Phi,\mathcal{L}}$ is representable by a projective $S$-scheme that can be embedded in $\mathbb{P}_S(F)$ for some finite locally free sheaf $F$ on $S$ that is an exterior power of $W$ with a symmetric power of $V$.

Proof: Cf.[Nit05]P24. □

Examples of Quot Schemes

Prop. (7.7.2.13) [Projective Spaces]. $\text{Quot}_{\mathcal{E}/\mathbb{Z}}^{\mathcal{O}_{\mathbb{Z}}} \cong \mathbb{P}^n_{\mathbb{Z}}$, with the universal element the tautological quotient $\mathbb{Z}^{n+1} \mathcal{O}_{\mathbb{P}^n} \to \mathcal{O}_{\mathbb{P}^n}(1)$.

Moreover, if $\mathcal{E} \in \mathbb{Coh}(S)$, then $\text{Quot}_{\mathcal{E}/S/S}^{\mathcal{O}_S} \cong \mathbb{P}(\mathcal{E})$, with the universal element the tautological quotient $\pi^*(\mathcal{E}) \to \mathcal{O}_{\mathbb{P}(\mathcal{E})}(1)$.

Proof: For any surjective map $\mathcal{E}_T \to \mathcal{L}$ where $\mathcal{L}$ is a line bundle, locally $H^0(\mathcal{L}) \cong H^0(\mathcal{E}_T)$ is of dimension $n$ and thus $\mathcal{L}$ is basepoint-free. Now the associated map $\varphi_{\mathcal{L}} : T \to \mathcal{O}_{\mathbb{P}(\mathcal{E})}(1)$ pulls $\mathcal{O}_{\mathbb{P}(\mathcal{E})}(1)$ to $\mathcal{L}$. □

Def. (7.7.2.14) [Relative Grassmannian of a Coherent Sheaf]. Let $\mathcal{E} \in \mathbb{Coh}(S)$, define the relative Grassmannian of $\mathcal{E}$ to be $\text{Gra}(\mathcal{E},k) = \text{Quot}_{\mathcal{E}/S/S}^{k,\mathcal{O}_S}$.

Then if $\mathcal{E}$ is finite locally free, it is a quotient of the group scheme $\text{GL}(n)_S$, and when $\mathcal{E} \cong \mathcal{O}^n_S$ and $S = \mathbb{Z}$, this is just the Grassmannian variety $\text{Gra}(n,k)$ defined in(7.2.1.20).

In particular, $\text{Gra}(n+1,1) \cong \mathbb{P}^n_{\mathbb{Z}}$ by(7.7.2.13).

Proof: First we prove for $\mathcal{E}$ finite locally free: There is a natural action of $\text{GL}(n)$ on $\text{Quot}_{\mathcal{E}/S/S}^{k,\mathcal{O}_S}$, it is a clearly a quotient map, and the kernel is a closed subgroup of $\text{GL}(n)_S$ by(15.3.1.4). Thus $\text{Gra}(\mathcal{E},k)$ is a quotient of $\text{GL}(n)$ by definition(7.1.1.21).

In general, $\mathcal{E}$ is a locally a quotient of a finite locally free sheaf, thus $\text{Gra}(\mathcal{E},k)$ is locally projective by(7.7.2.7). □

Prop. (7.7.2.15) [Quotient by Flat Projective Equivalence Relations].

Proof: Cf.[Nit05]P31. □

Prop. (7.7.2.16) [Grassmannian Varieties are projective]. The Grassmannian variety $\text{Gra}(\mathcal{E},k)$ is locally projective, and when $\mathcal{E}$ is locally free, it is projective, and if $\mathcal{E}$ is trivial, it is $H$-projective.
7.7. MODULI PROBLEMS 841

Proof: It injects into \( \mathbb{P}(\land^k \mathcal{E}) \) by the natural transformation

\[
T_S : (\mathcal{O}_T^n \to \mathcal{Q}) \mapsto (\land^k (\mathcal{O}_T^n) \to \land^k \mathcal{Q}).
\]

In particular, the corresponding very ample line bundle is just \( \land^k \mathcal{F} \), where \( f^* \mathcal{E} \to \mathcal{F} \) is the universal element and \( f : \text{Gra}(\mathcal{E}, k) \to S \), by (7.7.2.13).

\[\square\]

Cor. (7.7.2.17) [Grassmannian Varieties and Projective Space]. There is a canonical isomorphism \( G(n, n-1) \cong \mathbb{P}^{n-1} \) identifying sections with surjections from \( \mathcal{O}_X^n \).

Prop. (7.7.2.18) [Flag Varieties]. The flag variety (7.2.1.22) represents the functor \( T \mapsto \{ \text{the isomorphism classes of flags in } \mathcal{O}_T \text{ of the given dimensions} \} \).

Cor. (7.7.2.19) [Flag Varieties are Projective]. The flag varieties are projective as they are closed subsets of a product of Grassmannian varieties.

3 Picard Schemes

Main references are [Kle05]. For simplicity, we assume \( S \) is locally Noetherian and restrict to the category of locally Noetherian schemes over \( S \), and \( X/S \) is separated.

Notice a morphism \( X \to S \) is said to have integral geometric fibers if for any alg.closed field \( k \) and a morphism \( \text{Spec} k \to S \), \( X_k \) is integral.

Def. (7.7.3.1) [Picard Functor]. Let \( X \in \text{Sch}_S \), the Picard functor is the functor

\[
\text{Pic}^X : \text{Sch}_S \to \mathfrak{Sr} : T \mapsto \text{Pic}(X_T) = H^1(X_T, \mathcal{O}_{X_T}^*).
\]

The problem of this functor is that it is not a Zariski sheaf.

Define the relative Picard functor \( \text{Pic}^X_{/S} : \text{Sch}_S \to \mathfrak{Sr} : T \mapsto \text{Pic}(X_T)/\text{pr}_T^*(\text{Pic}(T)) \). Let the sheffification of this ring in the Zariski/étale/fppf topology denoted by \( \text{Pic}^X_{/S,Zar}, \text{Pic}^X_{/S,ét}, \text{Pic}^X_{/S} \).

Then there are maps of presheaves:

\[
\text{Pic}^X \to \text{Pic}^X_{/S} \to \text{Pic}^X_{/S,Zar} \to \text{Pic}^X_{/S,ét} \to \text{Pic}^X_{/S}.
\]

Remark (7.7.3.2). In the following we will frequently use a technical condition s.t. \( \mathcal{O}_S \to f_*(\mathcal{O}_X) \) is an isomorphism. This is true when \( X \) is a proper variety over \( S \), by (5.10.5.2).

Prop. (7.7.3.3). Assume \( \mathcal{O}_S \cong f_*\mathcal{O}_X \), then the functor \( \mathcal{N} \to f^*\mathcal{N} \) is fully faithful from the category of finite locally free sheaves on \( S \) to the category of finite locally free sheaves on \( S \) s.t. \( f_* \) is a left partial inverse.

Proof: For any finite locally free sheaf \( \mathcal{N} \), there is an isomorphism \( \mathcal{N} \cong f_*f^*\mathcal{N} \) by checking locally, and for any other finite locally free sheaf \( \mathcal{N}' \), \( \text{Hom}(\mathcal{N}, \mathcal{N}') \) is also finite locally free, thus the natural map \( f^*f^*\text{Hom}(\mathcal{N}, \mathcal{N}') \to \text{Hom}(f^*\mathcal{N}, f^*\mathcal{N}') \) is an isomorphism by checking locally. Thus \( \text{Hom}(\mathcal{N}, \mathcal{N}') \cong \text{Hom}(f^*\mathcal{N}, f^*\mathcal{N}') \).

\[\square\]

Def. (7.7.3.4) [Rigidification]. Assume \( f : X \to S \) has a section \( g : S \to X \), then for any \( T \in \text{Sch}_S \) and \( \mathcal{L} \in \text{Pic}(X_T) \), a \( g \)-rigidification of \( \mathcal{L} \) is an isomorphism \( u : \mathcal{O}_T \cong g_T^*\mathcal{L} \).
**Prop. (7.7.3.5)**. Let \( f : X \to S \) be a morphism of schemes with a section \( g \), then for any \( T \in \text{Sch}_S \), the group of isomorphism classes of pairs \((\mathcal{L}, u)\) where \( \mathcal{L} \in \text{Pic}(X_T) \) and \( u \) is a \( g \)-rigidification of \( \mathcal{L} \), is isomorphism to \( \text{Pic}_{X/S}(T) \).

**Proof:** For any \( \mathcal{M} \in \text{Pic}(X_T) \), let \( \mathcal{L} = \mathcal{M} \otimes (f_T^*g_T^*\mathcal{M})^{-1} \), then \( \mathcal{L} = \mathcal{M} \in \text{Pic}(X_T)/\text{pr}_T^*\text{Pic}(T) \), and there is a canonical isomorphism \( g_T^*\mathcal{L} \cong \mathcal{O}_T \).

Conversely, if \( u : \mathcal{O}_T \cong g_T^*\mathcal{L} \) and there exists some \( \mathcal{N} \in \text{Pic}(T) \) s.t. \( v : \mathcal{L} \cong f_T^*\mathcal{N} \), let \( w = g_T^* \circ u : \mathcal{O}_T \cong g_T^*\mathcal{L} \cong \mathcal{N} \), then there are isomorphism of pairs: \( v : (\mathcal{L}, u) \cong (f_T^*\mathcal{N}, w) \), \( f_T^*w : (\mathcal{O}_X, \text{can}) \cong (f_T^*\mathcal{N}, w \circ \text{can}) \), thus \((\mathcal{L}, u) = e \). \( \square \)

**Prop. (7.7.3.6)** [No Automorphisms after Rigidification]. Let \( f : X \to S \) be a morphism of schemes. If for any \( T \in \text{Sch}_S \), \( f_T : X_T \to T \) satisfies \( \mathcal{O}_T \cong (f_T)_*\mathcal{O}_{X_T} \), and \( f \) has a section \( g \), then for any \((\mathcal{L}, u)\) where \( u \) is a \( g \)-rigidification of \( \mathcal{L} \), \( \text{Aut}(\mathcal{L}, u) \) is trivial.

**Proof:** For such an automorphism \( v : \mathcal{L} \to \mathcal{L} \), \( g_T^*(v) = 1 \). Also notice \( \text{Hom}(\mathcal{L}, \mathcal{L}) = H^0(\text{Hom}(\mathcal{L}, \mathcal{L})) = H^0(\mathcal{O}_{X_T}) \cong H^0(\mathcal{O}_T) \), thus \( v \) is tensoring a line bundle \( \mathcal{L} \) from \( \mathcal{O}_T \). Thus \( g_T^*v \) is multiplying \( \mathcal{L} \). So \( \mathcal{L} \cong \mathcal{O}_T \) and \( v \) is trivial. \( \square \)

**Prop. (7.7.3.7)** [Comparison Theorems]. Let \( f : X \to S \) be a morphism of schemes. If for any \( T \in \text{Sch}_S \), \( f_T : X_T \to T \) satisfies \( \mathcal{O}_T \cong (f_T)_*\mathcal{O}_{X_T} \), then

- The morphisms \( \widetilde{\text{Pic}}_{X/S} \hookrightarrow \text{Pic}_{X/S,Zar} \hookrightarrow \text{Pic}_{X/S,\acute{e}t} \hookrightarrow \text{Pic}_{X/S} \) are injections. In particular, \( \widetilde{\text{Pic}}_{X/S} \) is separated in the fppf topology.
- If \( f \) has a section, then \( \widetilde{\text{Pic}}_{X/S} \cong \text{Pic}_{X/S,Zar} \cong \text{Pic}_{X/S,\acute{e}t} \cong \text{Pic}_{X/S} \).
- If \( f \) has a section Zariski locally, then \( \text{Pic}_{X/S,Zar} \cong \text{Pic}_{X/S,\acute{e}t} \cong \text{Pic}_{X/S} \).
- If \( f \) has a section étale locally, then \( \text{Pic}_{X/S,\acute{e}t} \cong \text{Pic}_{X/S} \).

**Proof:**
1. It suffices to show that \( \widetilde{\text{Pic}}_{X/S} \to \text{Pic}_{X/S} \) are injective. For this, notice first \( \text{Pic}_{X/S} \) is also the fppf-sheaf associated to \( \text{Pic}_{X/} \), as any line bundle on \( T \) is Zariski-locally trivial. Then if \( \mathcal{L} \in \text{Pic}(X_T) \) is fppf-locally trivial, then for some fppf covering \( \pi : T' \to T \), \((f_T)_*\pi_*\mathcal{L} \cong \mathcal{O}_{T'} \) by hypothesis. And this equals \( \pi^*(f_T)_*\mathcal{L} \) by flat base change. So \((f_T)_*\mathcal{L} \) is an invertible sheaf(by hypothesis used on \( f_T \)) and \( (f_T)_*(f_T)^*\mathcal{L} \cong \mathcal{L} \) because it is true after f.f. base change to \( T' \) (flat base change used).
2. By item1, it suffices to show \( \widetilde{\text{Pic}}_{X/S} \) satisfies the fppf-descent, but this follows from the fact \( \text{Pic}_{X/S} \) is a rigid fibered category(5.1.3.5), \( \mathcal{Q}\text{Coh} / \text{Sch} \) is a stack(5.1.5.12) and line bundles satisfy the fpqc descent(5.5.3.1).
3,4 follow from 2 by base change. \( \square \)

**Prop. (7.7.3.8)** [Comparison of Points]. Let \( \text{Spec} A \in \text{Sch}_S \) where \( A \) is a local ring, then

- the natural maps \( \text{Pic}_X(A) \cong \text{Pic}_{X/S}(A) \cong \text{Pic}_{X/S,Zar}(A) \) are isomorphisms.
- If \( A \) is Artin local with alg. closed residue field, then \( \text{Pic}_X(A) \cong \text{Pic}_{X/S,\acute{e}t}(A) \).
- If \( A \) is an alg. closed field \( k \), then \( \text{Pic}_X(k) \cong \text{Pic}_{X/S}(k) \)

**Proof:**
1. Since \( A \) is local, \( \text{Pic}(\text{Spec} A) = 0 \), and it has a unique minimal point, thus 1 is clear.
2. Every étale \( A \)-algebra of f.t. is a direct product of copies of \( A \), thus it is clear any fppf local scheme is a scheme.
3. In this case, any fppf covering of \( \text{Spec} k \) has a section, thus this follows from (7.7.3.7). \( \square \)
Prop. (7.7.3.9). If $X/S$ is proper of f.p., then an element in $\text{Pic}_{X/S}(S)$ is trivial iff it is trivial Zariski-locally on $S$.

**Proof:** Cf.[Neron Model, P202].

Relative Effective Divisors

Prop. (7.7.3.10)[Divisor Functor]. The divisor functor $\text{Div}_{X/S} : \text{Sch} \to \text{Sr}$ is given by $T \mapsto \{\text{relative effective divisors on } X_T/T\}$. This is truly a functor by (5.8.1.12).

Thm. (7.7.3.11) [Div$_{X/S}$ is Representable]. If $S$ is a locally Noetherian scheme and $X \to S$ is projective and flat, then $\text{Div}_{X/S}(7.7.3.10)$ is representable by an open subscheme of the Hilbert scheme $\text{Hilb}_{X/S}$.

**Proof:** Let $H = \text{Hilb}_{X/S}$ and $W \subset X \times H$ the universal closed subscheme. Then $\text{pr}_H$ is projective and flat. Let $V$ be the open loci of points of $W$ s.t. $W$ is an effective divisor, $U = H \setminus q(W \setminus V)$, then $U$ is open in $H$ and $q^{-1}U$ is an effective divisor on $X \times U/U$. By definition of Hilbert scheme, for any effective divisor $D$ on some $X_T/T$ is the pullback of $W$ via $g$. Now we show for any $t \in D$, $g(t) \in U$. This follows from (5.8.1.10) and f.f. descent of regularness (5.1.5.28). Thus $g$ factors through $U$, as $U$ is open.

Def. (7.7.3.12) [Relative Abel Map]. The relative Abel map is the functor

$$A_{X/S}(T) : \mapsto \text{Div}_{X/S}(T) \to \text{Pic}_{X/S}(T) : D \mapsto \mathcal{L}_{X_T}(D).$$

Def. (7.7.3.13) [Linear System Functor]. Let $X \in \text{Sch}_S$ and $\mathcal{L} \in \text{Pic}(X)$, the linear system functor $\text{LinSys}_{\mathcal{L}/X/S} : \text{Sch}_S \to \text{Set}$ is defined to be the inverse image of $\mathcal{L} \in \text{Pic}_{X/S}$ in $\text{Div}_{X/S}$ via the Abel map (7.7.3.12).

Thm. (7.7.3.14) [LinSys$_{\mathcal{L}/X/S}$ is Representable]. Let $X$ be a proper variety over $S$ and $\mathcal{L} \in \text{Pic}(X)$, then $\text{LinSys}_{\mathcal{L}/X/S}$ is represented by some projective space $\mathbb{P}(\mathcal{Q})$ over $S$.

**Proof:** Cf.[Kle05]P25.

Prop. (7.7.3.15). Assume $X/S$ is proper and $\mathcal{F} \in \text{Coh}(X)$, then there exists a unique $\mathcal{Q} \in \text{Coh}(S)$ with functorial isomorphism

$$q : \text{Hom}(\mathcal{Q}, \mathcal{N}) \cong f_*(\mathcal{F} \otimes f^*\mathcal{N})$$

for any $\mathcal{N} \in \mathcal{Q}\text{Coh}(S)$.

And the formation of $\mathcal{Q}$ commutes with base change.

**Proof:** Cf.[Kle05]P24.

Prop. (7.7.3.16). Situation as in (7.7.3.15), if $S$ is a local ring with closed point $s$, the following are equivalent:

- The $\mathcal{O}_S$-module $\mathcal{Q}$ is locally free.
- For all $\mathcal{N} \in \mathcal{Q}\text{Coh}(\mathcal{O}_S)$, the functor $\mathcal{N} \mapsto f_*(\mathcal{F} \otimes f^*\mathcal{N})$ is right exact.
- For all $\mathcal{N} \in \mathcal{Q}\text{Coh}(\mathcal{O}_S)$, the natural map $f_*(\mathcal{F}) \otimes \mathcal{N} \to f_*(\mathcal{F} \otimes f^*\mathcal{N})$ is an isomorphism.
- The natural map $H^0(X, \mathcal{F}) \otimes k(s) \to H^0(X_s, \mathcal{F}_s)$ is a surjection.
Proof: Cf.[Kle05]P24.

Prop.(7.7.3.17) If $X$ is a proper variety over $S$ and is representable with the universal sheaf $P$, then $\text{Div}_{X/S}$ with the relative Abel map(7.7.3.12) is isomorphic to $\text{LinSys}_{P/X_{\text{Pic}X/S}/\text{Pic}X/S}$ and also $P(Q)$ over $\text{Pic}X/S$, where $Q$ is the coherent sheaf associated to $P(7.7.3.15)$.

Proof: It follows from definitions(7.7.3.13)(7.7.3.10) and the definition of a universal sheaf. The last assertion follows from(7.7.3.14).

Prop.(7.7.3.18) Let $X/S$ be locally projective flat with integral geometric fibers, then
- $\text{Div}_{X/S} \to \text{Pic}X/S(T)$ is proper.
- If $\text{Pic}X/T \cong \text{Pic}X/T$, then $A_{X/S} : \text{Div}_{X/S} \to \text{Pic}X/S(T)$ is projective.

Proof: If $\text{Pic}X/T \cong \text{Pic}X/T$, then by(7.7.3.17), it is projective. For general case, notice proper satisfies fpqc descent, so we can base change to $X \times_S X \to X$, then it has a section, i.e. the diagonal section. Thus by(7.7.3.7), $\text{Pic}X/T \cong \text{Pic}X/T$ and $A_{X \times_S X}$ is projective, thus $A_{X/S}$ is proper.

Picard Schemes

Def.(7.7.3.19) For the 5 different presheaves on $\text{Sch}_S$ in(7.7.3.1), if one of them is representable, then all the sheaves after it are all isomorphic to it and representable, because fpqc sites are subcanonical. So it will make no confusion to call the representing scheme the Picard scheme.

Prop.(7.7.3.20) If $\text{Pic}X/S$ is representable, then it is locally of f.t. over $S$.

Proof: Because $S$ is locally Noetherian, by(5.8.4.2), it suffices to show that for any directed inverse system $(T_i, f_i) \in \text{Aff}_S$,
$$\lim_{\to} \text{Pic}X/S(T_i) \cong \text{Pic}X/S(\lim_{\to} T_i).$$

For the rest, Cf.[Kle05]P33.

Prop.(7.7.3.21) If $\text{Pic}X/S$ exists, then schematic points of $\text{Pic}X/S$ corresponds to line bundles on the geometric fibers of $X/S$.

Proof: This follows from the definition of schematic points and(7.7.3.8)item3.

Thm.(7.7.3.22) Let $f : X \to S$ be locally projective, flat with integral geometric fibers, then
- $\text{Pic}X/S_{\text{et}}$ is representable by a scheme separated and locally of f.p. over $S$.
- If moreover $S$ is Noetherian and $X/S$ is projective, then $\text{Pic}X/S_{\text{et}}$ is a disjoint union of open subschemes, each an increasing union of open quasi-projective $S$-schemes.

Proof: Cf.[Kle05]P27.

Cor.(7.7.3.23) If $S$ is Noetherian and $X/S$ is projective flat with integral geometric fibers, then any qc locally closed subscheme of $\text{Pic}X/S$ is quasi-projective.
**Prop. (7.7.3.24) [Tangent Space of $\text{Pic}_{X/k}$]**. Let $X$ be a scheme over a field. Assume $\text{Pic}_{X/k}$ is representable by a scheme and equals $\text{Pic}_{X/k,\text{ét}}$, then $T_e(\text{Pic}_{X/k}) \cong H^1(X, \mathcal{O}_X)$.

**Proof:** By (7.2.2.1), the tangent space equals $\text{ker}(\text{Pic}_{X/k}(k) \to \text{Pic}_{X/k}(k))$.

Take the first order thickening $X_k \subset X_k[\varepsilon] = X_\varepsilon$, there is an exact sequence $0 \to \mathcal{O}_X \to \mathcal{O}_{X_\varepsilon} \to \mathcal{O}_X^\ast \to 1$, where $\mathcal{O}_X \to \mathcal{O}_{X_\varepsilon}^\ast : a \mapsto 1 + a\varepsilon$. And it is split. Thus we have a split exact sequence

$$0 \to H^1(\mathcal{O}_X) \to H^1(\mathcal{O}_{X_\varepsilon}) \to H^1(\mathcal{O}_X^\ast) \to 0.$$ 

Now $\text{Pic}_{X/S,\text{ét}}$ is also the shiffification of $\text{Pic}_{X/k} : T \mapsto H^1(X_T, \mathcal{O}_{X_T}^\ast)$, thus there is a natural map

$$H^1(\mathcal{O}_X) \to \text{ker}(\text{Pic}_{X/k}(k[\varepsilon]) \to \text{Pic}_{X/k}(k)) = T_e(\text{Pic}_{X/k}).$$

And it can be shown that this is a $k$-homomorphism.

To show this map is an isomorphism, by flat base change we can assume $k$ is alg. closed. Then by (7.7.3.8), the maps $H^1(\mathcal{O}_{X_\varepsilon}^\ast) \to \text{Pic}_{X/k}(k)$ and $H^1(\mathcal{O}_{X_\varepsilon}^\ast) \to \text{Pic}_{X/k}(k[\varepsilon])$ are isomorphisms, thus $H^1(\mathcal{O}_X) \to T_e(\text{Pic}_{X/k})$ is also an isomorphism by five lemma.

**□**

**Thm. (7.7.3.25) [Grothendieck]**. Assume $X$ is proper over $S$ integral, then there exists a non-empty open subscheme $V$ of $S$ s.t. $\text{Pic}_{X_V/V}$ is representable, and is a disjoint union of quasi-projective subschemes.

**Proof:** Cf. [Kle05]P34. □

**Cor. (7.7.3.26) [Murre-Oort/Artin]**. Let $X$ be a proper scheme over a field $k$, then $\text{Pic}_{X/k}$ is representable by a disjoint union of quasi-projective subschemes.

**Prop. (7.7.3.27).** Let $X \to Y$ be a surjective morphism of proper schemes over a field $k$, then the dual map $\text{Pic}_{Y/k} \to \text{Pic}_{X/k}$ is affine.

**Proof:** □

**Prop. (7.7.3.28).** If $X/S$ is projective and flat with integral geometric fibers, then any connected component of $\text{Pic}_{X/S}$ is clopen of f.t..

**Proof:** By (7.7.3.22), $\text{Pic}_{X/S}$ is locally Noetherian, so each connected components are clopen (5.4.1.23), and they are of f.t. as $\text{Pic}_{X/S}^\phi$ are (7.7.3.40). □

**Prop. (7.7.3.29) [Projectiveness of Subschemes]**. Let $S$ be Noetherian and $X \to S$ be smooth projective with irreducible geometric fibers, then every quasi-compact closed subscheme of $\text{Pic}_{X/S}$ over $S$ is projective.

**Proof:** By (7.7.3.23), it suffices to show it is universally closed. As $X \to S$ is both proper and flat, it suffices to show for $X \to S$ f.f.. Then we can base change via the f.f. covering $X \to S$, thus we can assume it has a section, so $\text{Pic}_{X/S} \cong \text{Pic}_{X/S}$. Then we use valuation criterion: for any valuation ring $A$ with fraction field $K$, it suffices to extend a line bundle on $X_K$ to a line bundle on $X_A$, because $Z$ is closed and $A$ is reduced. By replacing $L$ with $L(n)$, we can assume $L$ has a global section, which implies $L$ is an effective Cartier divisor $D$, as $X_K$ is integral. Notice $A$ is regular and $X_T/T$ is smooth, so $X_T$ is regular ?? and thus locally factorial. Then the closure of $D$ in $X_T$ is also a divisor?. □
Cor. (7.7.3.30). If $X$ is a smooth projective variety over a field $k$, then all connected components of $\text{Pic}_X/k$ are proper.

Proof: This follows from (7.7.3.29) and (7.1.4.16).

Prop. (7.7.3.31) [Product Varieties]. If $X, Y$ are two complete varieties over a field $k$ with rational points, then $\text{Pic}_X \times_Y \text{Pic}_Y/k \cong \text{Pic}_X/k \times \text{Pic}_Y/k$, with $p_{X \times Y} = p_X^1 \otimes p_Y^2$.

Proof: This follows from see-saw principal (5.10.1.22), the theorem of the cube (5.10.1.23) and (7.7.3.5).

Pic^0_{X/S}

Def. (7.7.3.32) [Pic^0_{X/S}]. If $\text{Pic}_{X/S}$ exists, then its identity component is a subgroup scheme, denoted by $\text{Pic}^0_{X/S}$.

Prop. (7.7.3.33) [Projectiveness of $\text{Pic}^0_{X/S}$]. Let $X$ be a projective variety over a field $k$, then $\text{Pic}^0_{X/S}$ is representable (7.7.3.22) and is quasi-projective. And if $X/k$ is geo.normal, then it is projective.

Proof: Cf. [Kle05] P37.

Cor. (7.7.3.34) [Subfamily and Morphisms Relations]. The Poincaré class $p_X$ in $\text{Pic}(X \times \text{Pic}^0(X))$ is the unique line bundle that satisfies $p_b = b$ for a point $b \in \text{Pic}^0(X)$, and $p_{P_b}$ is trivial.

For a subfamily $c$ of $\text{Pic}^0(X)$ parametrized by an scheme $T$ over $k$, there is a morphism

$$T \rightarrow \text{Pic}^0(X) : t \mapsto c_t \in \text{Pic}^0(X)(k(t))$$

over $k$.

Proof: A point $b \in \text{Pic}^0(X)$ is a morphism $k(b) \rightarrow \text{Pic}^0(X)$, and the restriction of $p$ to $b$ is just $b$, by (7.7.3.22).

The second assertion follows from the first, because this subfamily corresponds to a morphism $T \rightarrow \text{Pic}^0(X)$, and the restriction of $p$ at the image of $t$ in $\text{Pic}^0(X)$ is just the subfamily restricted at $t$, which is $c_t$.

Prop. (7.7.3.35) [Pic^0_{X/k,\text{red}} is an Abelian Variety]. If $X$ is a smooth projective variety over a field $k$, then $\text{Pic}^0_{X/k,\text{red}}$ is an Abelian variety.

Proof: $\text{Pic}^0(X)$ is a group scheme because it represents a group functor. $\text{Pic}^0_{X/S,\text{red}}$ is also a smooth proper connected algebraic group by (7.7.3.30)/(7.7.3.28), thus it is an Abelian variety.

Prop. (7.7.3.36) [Dual Picard Map]. By functoriality, if $X/S, X'/S$ are connected schemes s.t. $\text{Pic}_{X/S}$ and $\text{Pic}_{X'/S}$ are representable, then the pullback along $\varphi$ induces a dual homomorphism of group schemes:

$$\hat{\varphi} : \text{Pic}^0_{X'/S,\text{red}} \rightarrow \text{Pic}^0_{X/S,\text{red}}.$$

In other words, it is the unique morphism $\text{Pic}^0_{X'/S,\text{red}} \rightarrow \text{Pic}^0_{X/S,\text{red}}$ s.t.

$$(\varphi \times \text{id}_{\text{Pic}^0_{X'/S,\text{red}}})^*p_{X'/S} = (\text{id}_X \times \hat{\varphi})^*p_{X/S}.$$
Prop.(7.7.3.37) [Double Picard Map]. Let $X/S$ be a connected scheme s.t. $\overline{\text{Pic}}_{X/S,\text{red}}$ is representable with a Poincaré class $p_X \in \text{Pic}(X \times \overline{\text{Pic}}_{X/S,\text{red}}^0)$, and $\overline{\text{Pic}}_{X/S,\text{red}}^0$ is representable, then $p_X$ satisfies $(p_X)_0 = 0$, thus inducing a map $X \to \overline{\text{Pic}}_{X/S,\text{red}}^0$.

Def.(7.7.3.38) [Néron-Severi Group Scheme]. Let $X$ be a complete $k$-variety, the Néron-Severi group $\text{NS}(X_{\overline{k}})$ of $X_{\overline{k}}$ is defined to be
\[
\text{NS}(X_{\overline{k}}) = \text{Pic}(X_{\overline{k}})/\text{Pic}^0(X_{\overline{k}}) = \pi_0(\text{Pic}_{X/\overline{k}}(\overline{k}))(6.1.12.4)(6.3.1.2),
\]
which in fact equals $\pi_0(\text{Pic}_{X_s/k^s}(k^s))(k^s) = \text{Pic}(X_{k^s})/\text{Pic}^0(X_{k^s}) = \text{NS}(X_{k^s})$.

Also denote
\[
N^1(X_{\overline{k}}) = \text{Pic}(X_{\overline{k}})/\text{Pic}^0(X_{\overline{k}}) = \text{NS}(X_{\overline{k}})/(\text{NS}(X_{\overline{k}})_{\text{tor}}(6.1.12.25) = N^1(X_{k^s}).
\]

Prop.(7.7.3.39) [Theorem of the Base]. $\text{NS}(X_{\overline{k}})$ is f.g. In particular, $N^1(X_{\overline{k}})$ is a finite free $\mathbb{Z}$-module, and its rank $\rho(X)$ is called the Picard number of $X$.

Proof: Cf. [Kleiman, Toward a numerical theory of ampleness, P334].

Prop.(7.7.3.40) $[\text{Pic}^\Phi_{X/S}]$. If $X/S$ is locally projective, flat with integral geometric fibers, $\Phi \in \mathbb{Q}[\lambda]$, let $\text{Pic}^\Phi_{X/S}$ denote the subfunctor of $\text{Pic}_{X/S}$ representing invertible sheaves $L$ with $\chi(L(n)) = \Phi(n)$, then $\text{Pic}^\Phi_{X/S}$ are clopen subschemes of $\text{Pic}_{X/S}$ of f.t. and form a disjoint cover of it, and forming it commutes with base change. Moreover, if $X/S$ is projective and $S$ is Noetherian, then each $\text{Pic}^\Phi_{X/S}$ is quasi-projective over $S$.

Proof: Cf. [Kle05]P60.?

The first assertion follows from the fact Euler character is locally constant so $\text{Pic}^\Phi_{X/S}$ form a clopen disjoint covering of $\text{Pic}_{X/S}$ and use (7.7.1.5) and (7.7.1.7).

Prop.(7.7.3.41) [Quasi-Coherence and Boundedness]. If $\text{Pic}_{X/S}$ is representable and $\Lambda \subset \text{Pic}_{X/S}$ be a subset with corresponding set of line bundles $L$, then $\Lambda$ is qc iff $L$ is bounded (6.1.12.24).

Proof: If $L$ is bounded by $T \in \text{Sch}^{\text{ft}}/S$, then there is a map $\theta : T \to \text{Pic}_{X/S}$ that $\Lambda \subset \theta(T)$. Notice $T$ is a Noetherian space, thus so is $\theta(T)$, and $\Lambda$ is qc.

Conversely, if $\Lambda$ is qc, then it is contained in an open subscheme $U \subset \text{Pic}_{X/S}$ of f.t. over $S$, then $U$ gives out a line bundle on $X_T$ for some fppf covering $T$ of $U$. Such $T$ can be chosen to be f.t. over $S$ as $U$ is f.t., so $L$ is bounded by $T$.

Cor.(7.7.3.42) [Quasi-Coherence and Hilbert Polynomials]. If $S$ is Noetherian and $X/S$ is projective and flat, and $\text{Pic}_{X/S}$ is representable, let $\Lambda \subset \text{Pic}_{X/S}$ be any subset and $\Pi$ the corresponding set of Hilbert polynomials, then $\#\Pi < \infty$ if $\Lambda$ is qc, and $\#\Pi = 1$ if $\Lambda$ is connected.

Proof: If $\Lambda$ is qc, then $L$ is bounded by some $T \in \text{Sch}^{\text{ft}}/S$, and then by locally constancy of Hilbert polynomials, $\#\Pi < \infty$.

If $\Lambda$ is connected, then so is the induced reduced structure on its closure $\overline{\Lambda}$. $\overline{\Lambda}$ gives out a line bundle on $X_T$ for some fppf covering $T$ of $\overline{\Lambda}$. Notice $T \to \overline{\Lambda}$ is open and Hilbert polynomial is locally constant on $T$, so there is only one Hilbert polynomial type.
Torsion Components

Prop. (7.7.3.43). If $X/S$ is projective, flat with integral geometric fibers, then for $n \in \mathbb{Z}_+$, $[n] : \text{Pic}_{X/S} \to \text{Pic}_{X/S}$ is of f.t.

Proof: Cf. [?].

Prop. (7.7.3.44). If $X/S$ is proper and $\text{Pic}_{X/S}$ exists, then $\text{Pic}_{\tau X/S}$ is an open subgroup of f.t.

Proof: Cf. [Kle05] P59.

Prop. (7.7.3.45). If $X$ is a $k$-scheme s.t. $\text{Pic}_{X/k}$ is representable, then $\text{Pic}^\tau_{X/S}$ is an open subgroup, and forming it commutes with change of fields. Moreover, if $X/S$ is projective, then $\text{Pic}^\tau_{X/S}$ is clopen of f.t.

Proof: Using (7.1.4.17) and (7.7.3.20), it suffices to prove $\text{Pic}^\tau_{X/S}$ is of f.t. when $X$ is projective over $S$. For this, it suffices to prove for $k = \overline{k}$. In this case, by (6.1.12.25) and (6.1.12.26), there is an algebraic $k$-scheme $T$ and $\mathcal{M} \in \mathcal{T}$ s.t. the corresponding map $\theta : T \to \text{Pic}_{X/k}$ satisfies $\text{Pic}^\tau_{X/S} \subset \theta(T)$. Notice $T$ is a Noetherian space, thus so is $\theta(T)$, and $\Lambda$ is qc.

Cor. (7.7.3.46). Let $X$ is a projective variety over a field $k$, then $\text{Pic}^\tau_{X/k}$ is quasi-projective. And if $X$ is geo.normal, then it is projective.

Proof: By (7.7.3.45) (7.7.3.23), $\text{Pic}_{X/S}$ is quasi-projective. To show it is proper, it suffices to show for $k = \overline{k}$. In this case, $\text{Pic}^\tau_{X/k}$ is covered by f.m. translates of $\text{Pic}^0_{X/k}$ as it is qc, and $\text{Pic}^0_{X/k}$ is projective by (7.7.3.33), so $\text{Pic}_{X/k}$ is also proper, as it is closed so is the scheme-theoretic image of these copies $\text{Pic}^0_{X/k}$.

Prop. (7.7.3.47). Let $X/S$ be locally projective flat with integral geometric fibers, then $\text{Pic}^\tau_{X/S}$ is a clopen subgroup of $\text{Pic}_{X/S}$ of f.t., and forming it is compatible with base change. Moreover, if $X/S$ is projective with $S$ Noetherian, then $\text{Pic}^\tau_{X/S}$ is quasi-projective.

Proof: Cf. [Kle05] P58.

Cor. (7.7.3.48) [Torsion Components are Projective]. If $X/S$ is smooth projective with integral geometric fibers and $S$ is Noetherian, then $\text{Pic}^\tau_{X/S}$ is projective.

Proof: This follows from (7.7.3.47) and (7.7.3.29).

Prop. (7.7.3.49). If $S$ is Noetherian and $X/S$ is locally projective flat with integral geometric fibers, then for any $s \in S$ with residue field $k(s)$ and an alg.close $\overline{k}(s)$, the group

$$\frac{\text{Pic}^\tau_{X_{\overline{k}(s)}}(\overline{k}(s))}{\text{Pic}^\tau_{X_{\overline{k}(s)}}(\overline{k}(s))}$$

is a finite group, and its order is uniformly bounded.

Proof: It is finite by (7.7.3.47), and the number of connected components of $\text{Pic}^\tau_{X_{\overline{k}(s)}}(\overline{k}(s))$ is constant for a non-empty open subset of $S$ by [EGA 4.3, 9.7.9], so it is bounded by Noetherian induction.
4 Picard Spaces

Thm. (7.7.4.1) [Artin]. If $X \rightarrow S$ is proper flat and f.p. morphism of algebraic spaces s.t. forming $f_*\mathcal{O}_X$ commutes with base change, then $\text{Pic}_{X/S}$ is representable by an algebraic space, and is locally of f.p. over $S$.

Proof:

\[ \square \]

5 Moduli of Curves

Def. (7.7.5.1) [Smooth Curves of Genus $g$]. Given a scheme $S$, there is a category $\mathcal{M}_g$ fibered in sets over $\text{Sch}/S$ where $\mathcal{M}_g(T)$ is the set of smooth and proper morphisms of schemes $C \rightarrow T$ that the fibered are all geometrically connected curves of genus $g$.

Similarly there is a category $Z_g$ fibered in sets over $\text{Sch}/S$ of smooth pointed curves of genus $g$. 
7.8 Algebraic Stacks

Basic references are [Sta], [Ols16], [Vis08] and [Fibered Category to Algebraic Stacks Lamb].

Notations (7.8.0.1).
- Use notations as in Sites, Sheaves and Stacks5.1.
- Fix $S \in \Sch$. A fibered category/stack over $S$ means a fibered category/stack over $\Sch_{fpf} / S$ (obsolete).

1 Algebraic Spaces

Def.(7.8.1.1)[Schematic Morphism]. A schematic morphism of fibered categories $\mathcal{X} \to \mathcal{Y}$ over $S$ is a representable morphism of fibered categories over $S$ (3.1.7.36).

Def.(7.8.1.2)[Properties of Schematic Morphisms]. For a property $P$ of maps of schemes which is stable under base change, we say that $P$ holds for a schematic map $\mathcal{X} \to \mathcal{Y}$ iff for any $S \in \Sch$, $P$ holds for the map $S \times_\mathcal{Y} \mathcal{X} \to S$.

Def.(7.8.1.3)[Algebraic Space]. An algebraic space is a sheaf $\mathcal{F} \in \Sh_{fpf} / S$ that the diagonal is schematic, and there exists some scheme $U \in \Sch / S$ with an étale surjective map $h_U \to \mathcal{F}$ in $\Sch_{fpf} / S$, called an atlas for the algebraic space $\mathcal{F}$.

The category of algebraic spaces is the full subcategory of $\Sh_{fpf} / S$, denoted by $\AlgSp / S$.

Prop.(7.8.1.4)[Schemes is an Algebraic Space]. $\Sch / S$ is a full subcategory of $\AlgSp / S$.

Proof: For $X \in \Sch / S$, $h_X$ is a sheaf because fpf site is subcanonical by (5.1.4.34), its diagonal is representable, and the identity $\id_X : X \to X$ is surjective and étale.

Remark(7.8.1.5). In general, the quotient of a scheme by a finite group action is an algebraic space that is not a scheme. Naively one can think of algebraic spaces as quotients of schemes by finite groups. — Kollar.

Def.(7.8.1.6)[Sites over Algebraic Spaces]. The Zariski/étale/smooth/fppf/... sites over an algebraic scheme is defined verbatim as that of over algebraic schemes.

Prop.(7.8.1.7)[Algebraic Spaces and Étale Equivalence Relations]. Cf.[Sta]02WW.

Proof:

Prop.(7.8.1.8). If $\mathcal{X}$ is an algebraic space over $S$, then the diagonal map $\Delta_{\mathcal{X}/S}$ is locally of finite type, locally quasi-finite, separated and is a monomorphism.

Proof: Cf.[Sta]02X4.

Def.(7.8.1.9)[Underlying Space of Algebraic Spaces]. For $\mathcal{X} \in \AlgSp / S$, the underlying space $|\mathcal{X}|$ is a topological space whose points are the equivalence classes of morphisms $\Spec K \to \mathcal{X} \in \Sh_{fpf} / S$, where $K \in \Field$.

Prop.(7.8.1.10). Let $\mathcal{X} \in \AlgSp / S, T \in \Sch / S, f : T \to \mathcal{X} \in \AlgSp / S$, then $f$ is surjective iff $|f| : |T| \to |\mathcal{X}|$ is surjective.

Proof:
2 Algebraic Stacks

Def. (7.8.2.1) [Representable by Algebraic Spaces]. A morphism of fibered categories $\mathcal{X} \to \mathcal{Y}$ over $S$ is called representable by algebraic spaces if for any $U \in \mathcal{C}$ and a morphism $\mathcal{C}/U \to \mathcal{Y}$, the fibered category $(\mathcal{C}/U) \times_{\mathcal{Y}} \mathcal{X} \to \mathcal{C}/U$ is equivalent to an algebraic space (7.8.1.3). (Notice it is a fibered category by (3.1.7.15) and (3.1.7.16)).

Def. (7.8.2.2) [Properties of Morphisms Representable by Algebraic Spaces]. For a property $P$ of maps of schemes which is stable under base change, we say that $P$ holds for a morphism $\mathcal{X} \to \mathcal{Y}$ representable by algebraic spaces iff for every $U \in \text{Sch}_{fppf}/S$, $P$ holds for the map of algebraic spaces $U \times_{\mathcal{Y}} \mathcal{X} \to S$.

Def. (7.8.2.3) [2-Category of Algebraic Stack]. An algebraic stack is a stack in groupoids $\mathcal{X}$ over $\mathcal{S}ch_{fppf}/S$ that the diagonal is representable by an algebraic space (7.8.2.1), and there exists some scheme $U \in \text{Sch}/S$ with a smooth surjective map $\mathcal{S}ch_{fppf}/U \to X$ in $\text{Sta}_{fppf}/S$, called an atlas for the algebraic stack $X$. It is called a Deligne-Mumford stack if moreover there exists some scheme $U$ with a smooth étale map $\mathcal{S}ch_{fppf}/U \to X$ in $\text{Sta}_{fppf}/S$.

The 2-category of algebraic (Deligne-Mumford) stacks is the full sub-2-category of $\text{Sta}_{fppf}/S$, denoted by $A_{lg} S_{ta}/S (A_{lg} S_{ta}^{DM}/S)$.

Prop. (7.8.2.4). If $\mathcal{X}, \mathcal{Y}$ are categories equivalent in $\mathcal{S}ch/S$ and $\mathcal{X}$ is an algebraic/Deligne-Mumford stack over $S$, then so is $\mathcal{Y}$.

Proof: By (5.1.3.7), $\mathcal{Y}$ is also a stack in groupoid, and Cf. [Sta]03YQ?. □

Prop. (7.8.2.5) [Algebraic Stacks and Étale Groupoid Object]. There is a bijection of étale groupoid objects on a scheme with the category of algebraic stacks.

Proof: Cf. [Lamb, P39]. □

Prop. (7.8.2.6) [Algebraic Spaces and Étale Equivalence Relations]. There is a bijection of étale equivalence relations on a scheme with the category of algebraic spaces.

Proof: This is a corollary of (7.8.2.5). □
7.9 Group Algebraic Spaces

Main references are [Sta] Chap 76.

Notations (7.9.0.1).
- Use notations defined in Algebraic Stacks 7.8.
- Fix $S \in \text{Sch}$ and $B \in \text{AlgSp}/S$. $\text{AlgSp}/B = (\text{AlgSp}/S)/B$.

Def. (7.9.0.2) [Group Algebraic Spaces]. The category $\mathcal{G}_{\text{AlgSp}}/B$ of group algebraic space over $B$ is defined to be

$$\mathcal{G}_{\text{AlgSp}}/B = \mathcal{G}_{\text{fgf}}/B \cap \text{AlgSp}/B \subset \mathcal{G}_{\text{fppf}}/B.$$

1 Quotient of Groupoids

Main references are [Quotient Spaces Modulo Algebraic Groups, Kollar, 1997].

Def. (7.9.1.1) [Quotients of Groupoids]. Let $U \in \text{AlgSp}/B$, $j : R \rightarrow U \times_B U$ be a pre-relation on $U$ over $B$, $\varphi : U \rightarrow X \in \text{AlgSp}/B$, then
- For $u \in |U|$, the $R$-orbit of $u$ is the equivalent class of $u \in |U|$ generated by $|R| \subset |U| \times |U|$.
- For $T \subset |U|$, $T$ is called $R$-invariant if $s^{-1}(T) = t^{-1}(T) \subset |R|$.
- $\varphi$ is said to be $R$-invariant if for it equalizes the two maps $s, t : R(k) \rightarrow U(k)$.
- $\varphi$ is said to be set-theoretically $R$-invariant if for any Spec $k \in \text{Sch}/B$, $k = \overline{k}$, $\varphi(k)$ equalizes the two maps $s, t : R(k) \rightarrow U(k)$.
- $\varphi$ is said to separate $R$-orbits if it is set-theoretically $R$-invariant and for any Spec $k \in \text{Sch}/B$, $k = \overline{k}$ and $u, u' \in U(k)$, $\varphi(u) = \varphi(u') \in X(k)$ implies $u, u'$ are in the same $R$-orbits.
- $\varphi$ is said to be an orbit space for $R$ if it is $R$-invariant and surjective, and separates $R$-orbits.
- $\varphi$ is said to be a course quotient for $R$ if it is a categorical quotient and it is an orbit space for $R$.
- If $S = B, U, R, X \in \text{Sch}$, then $\varphi$ is said to be a course quotient in schemes for $R$ if it is a categorical quotient in schemes and it is an orbit space for $R$.
- If $\varphi$ is $R$-invariant, The sheaf of $R$-invariant functions $(\varphi_*O_U)^R$ as the étale $O_X$-subalgebra of $\varphi_*O_U$ which is the equalizer of two maps induced from $s, t : R \rightarrow X$.

Prop. (7.9.1.2). Situation as in (7.9.1.1), if $R, U$ are locally of f.t. over $B$, $\varphi$ is an orbit space for $R$ iff it is $R$-invariant and for any Spec $k \in \text{Sch}/B$, $k = \overline{k}$,

$$U(k)/(\text{equivalent relations generated by } j(R(k))) \rightarrow X(k)$$

is bijective.

Proof: Cf. [Sta] 04A0. □

Def. (7.9.1.3) [Good Quotients]. Situation as in (7.9.1.1), $\varphi$ is said to be a good quotient if
- $\varphi$ is affine, surjective, $R$-invariant.
- For any base change $\varphi'$ of $\varphi$, $|\varphi'|$ is a closed map, and $|\varphi|(Z_1 \cap Z_2) = |\varphi|(Z_1) \cap |\varphi|(Z_2) \subset |X|$ for any closed subsets $Z_1, Z_2 \subset |U|$.
• $\mathcal{O}_X \to (\varphi_*\mathcal{O}_U)^R$ is an isomorphism.

**Def. (7.9.1.4) [Geometric Quotients].** Situation as in (7.9.1.1), $\varphi$ is said to be a geometric quotient if
- $\varphi$ is an orbit space for $R$,
- $\varphi$ is universally submersive,
- $\mathcal{O}_X \to (\varphi_*\mathcal{O}_U)^R$ is an isomorphism.

**Thm. (7.9.1.5) [Kollar].** Let $S \in \text{Sch}$ be excellent, $G \in \text{AlgGrp}_{\text{Aff}} / S, X \in \text{AlgSp}_{\text{sep,ft}} / S$. Let $m : G \times X \to X$ be a proper $G$-action on $X$, and one of the following holds:
- $G$ is a reductive group scheme over $S$,
- $S = \text{Spec } k$ where $k \in \text{Field}, \text{char } k > 0$.

**Proof:** then a geometric quotient $\varphi : X \to X/G$ exist (7.9.1.4), and $X/G \in \text{AlgSp}_{\text{sep,ft}} / S$. Cf.[Quotient Schemes modulo Algebraic Groups, Kollar]P35.

**2 Quotients of Schemes**

**Prop. (7.9.2.1).** Let $u_0, u_1 : X_1 \to X_0$ be an equivalence relation on the algebraic scheme $X_0$ over $R_0$. Assume that
- $u_0 : X_1 \to X_0$ is locally free of rank $r$.
- For all $x_0 \in X$, $u_0(u_1^{-1}(x))$ is contained in an open affine subscheme of $X_0$.
Then a quotient $u : X_0 \to X$ exists. Moreover, $u$ is locally free of rank $r$.

**Proof:** Cf[Mil17b]P597.
7.10 Higher Dimensional Geometry

1. Bend and Break
2. Cone Theorem
3. Homological Methods

Prop. (7.10.3.1) [Birkar-Cascini-Hacon-Mkernan].

4. Minimal Model Program
8       Algebraic Geometry III: Derived Algebraic Geometry

8.1 Simplicial Commutative Algebras

Main references are [Model Categories and Simplicial Methods, Paul Goerss and Kristen Schemmerhorn], [Simplicial Commutative Rings, Mathew].

1 Simplicial Groups

Prop. (8.1.1.1). A morphism of simplicial groups, when regarded as simplicial set, is a Kan fibration iff

\[ X \to \pi_0 X \otimes_{\pi_0(Y)} Y \]

is surjective. In particular, any simplicial group is a Kan complex.

Proof: Cf.[Simplicial Homology Theory Jardine P12] □

Def. (8.1.1.2) [Simplicial Modules]. A simplicial module over a simplicial ring \( R_\bullet \) is a map of simplicial map \( R_\bullet \times M_\bullet \to M_\bullet \) that is a ring action.

2 Simplicial \( R \)-Modules and Resolutions

Def. (8.1.2.1) [Moore Complex]. Giving a simplicial object in an Abelian category, we can have a Moore chain complex with Čech-like differentials. \( \partial_n = \sum_1^n (-1)^i d_i \). And we have \( \partial^2 = 0 \).

Proof: Should use \( d_i d_j = d_j d_{i - 1} d_i \) for \( i < j \). □

Def. (8.1.2.2) [Normalization of a simplicial \( R \)-Module]. The normalization of a simplicial \( R \)-module \( M \) is the chain complex

\[ NM : \cdots \to NM_n \xrightarrow{(-1)^n d_n} NM_{n-1} \to \cdots \]

where \( NM_n = \bigcap_{i=0}^{n-1} \ker(d_i) \in M_n \). This is a chain complex because \( d_{n-1} d_n = d_{n-1} d_{n-1} \) is 0 on \( NM_n \). In fact \( NM \) is preserved by all injections.

The homotopy groups \( \pi_\ast(M) \) of \( M \) is defined to be the homology of the normalization of \( M \). And it can be shown that as a set \( \pi_n(M) \) is just the \( n \)-th homotopy group of the geometrization of the

The degenerate complex of a Moore complex \( DM \) is the chain complex that \( D_n = \sum_{i=0}^{n-1} s_i M_{n-1} \) is a sub chain complex of \( M \) by the relation of \( d_i, s_j \).
Def. (8.1.2.3). A morphism of simplicial Abelian groups is called a weak equivalence if it induces an isomorphism on the homotopy groups.

Prop. (8.1.2.4) [Differential Graded Structures]. For any simplicial commutative $R$-algebra $A$, the homotopy groups $\pi_\ast(A)$ form a graded commutative $R$-ring.

Proof: The group structure on $\pi_\ast(A)$ is given by smash products. Cf. [Simplicial Commutative Algebras, Mathew, P2].

Cor. (8.1.2.5) [$\pi_0$ is an Algebra]. If $Y$ is a simplicial commutative $R$-algebra, then $\pi_0(Y) = Y_0/(\text{Im}(d_0 - d_1))$, which is an algebra.

Proof: It suffices to show $\text{Im}(d_0 - d_1)$ is an ideal of $Y_0$: If $a \in Y_0$, then

$$(d_0 - d_1)(s_0(a)y) = d_0s_0(a)d_0(y) - d_1s_0(a)d_1(y) = a(d_0 - d_1)(y).$$

Prop. (8.1.2.6). If $R_\ast$ is a simplicial ring and $M_\ast$ is a simplicial $R_\ast$-ring, then $\pi_\ast(M)$ is a graded $\pi_\ast(R)$-module.

Prop. (8.1.2.7). The simplicial homology of the Moore complex of the bar resolution $BG$ of group homology with coefficient in $R$ is just the group homology $H_n(G, R)$ for the trivial module $R$. And it has the same homology with the geometrization $[BG]$.

Lemma (8.1.2.8). $A_\ast \cong NA_\ast \oplus DA_\ast$ as a complex, $NA_\ast$, $A_\ast, (A/DA_\ast)$ are all homotopically equivalent.

Proof: We define similarly $N_kA_\ast$ and $D_kA_\ast$ and induct on $k$, our conclusion is the case $k = n - 1$. When $k = 0$, $\text{Im}d_0 \oplus \ker s_0 A_n = A_n$ because $d_0s_0 = id_{n-1}$ thus $A_{n-1} \xrightarrow{s_0} A_n$ is a split injection.

There are two split exact rows by simplicial relations:

$$
\begin{array}{cccccc}
0 & \longrightarrow & N_{k-1}A_{n-1} & \xrightarrow{s_k} & N_{k-1}A_n & \xrightarrow{1-s_kd_k} & N_kA_n & \longrightarrow & 0 \\
& \downarrow & \downarrow & \downarrow & & \downarrow & & \downarrow & \\
0 & \longrightarrow & A_{n-1}/D_{k-1}A_{n-1} & \xrightarrow{s_k} & A_n/D_{k-1}A_n & \longrightarrow & A_n/D_kA_n & \longrightarrow & 0
\end{array}
$$

The first one split because it has a right section, the second one split because it has a left section. So by induction, $N_kA_n \rightarrow A_n/D_kA_n$ is an isomorphism, thus $N_kA_n \oplus D_kA_n = A_n$ because it splits.

For the homotopy equivalence, Cf. [Jardine P150].

Prop. (8.1.2.9) [Dold-Kan Correspondence]. Let $R$ be a ring, then the normalized Moore complex functor $N$ gives an equivalence of categories:

$$
N : s\text{Mod}_R \cong \text{Ch}_{\geq 0}R.
$$

and the inverse is given by

$$(\sigma C_\ast)_n = \bigoplus_{[n]=[k]} C_k$$

and a morphism $\sigma_n \to \sigma_m$ for a morphism $[m] \to [n]$ is defined as follows: For $[n] \to [k]$, write $[m] \to [n] \to [k]$ as $[m] \to [r] \xrightarrow{\varphi} [k]$ where $\varphi$ is injective, thus maps $a \in C_k$ in $\sigma C_n$ to $\psi^*(a) \in C_r$ in $\sigma C_m$, where $\psi^*$ is zero unless $\psi = d^n : \Delta[n-1] \to \Delta[n]$. And homotopy groups and homology groups correspond via this equivalence, so does weak equivalences.
8.1. SIMPLICIAL COMMUTATIVE ALGEBRAS

Proof: \( \sigma(C) \) defines a simplicial Abelian group because of the uniqueness of the canonical decomposition. There is a natural map from \( \sigma(NA) \) to \( A \).

Now the task is to show that \( \sigma(NA) \cong A \) and \( N(\sigma C) \cong C \). We have \( N(\sigma C)_n = C_n \) because \( d^iC_n \) is 0 for \( i \neq n \) and the other components are all degeneracies thus are not in \( N(\sigma C)_n = C_n \) by (8.1.2.8).

Then we prove \( \sigma(NA) \cong A \). It is a surjection by (8.1.2.8) and induction. For the injectivity, if \( (a_\varphi) \neq 0 \) is mapped to 0, \( a_{id_n} \) is 0 by (8.1.2.8). And we choose an ordering on the \( \varphi : [n] \to [k] \) by dominating, and suppose \( \psi \) is a minimal one. Now choose a section \( \xi \) of \( \psi \) that \( \xi \) is the maximal section, thus \( \varphi \xi \) cannot by id\(_k\) for any other \( \varphi \). Now by induction we have \( a_\psi = 0 \), contradiction. □

Cor. (8.1.2.10)[Trivial Simplicial Algebra]. There is a functor from an \( R \)-algebra \( S \) to a trivial simplicial \( R \)-algebra \( s(S) \), it is a fully faithful embedding and \( \pi_0 \) is left adjoint to it.

Proof: This is the adjointness of (3.4.2.12) under the equivalent \( \sigma(8.1.2.9) \).

Cor. (8.1.2.11)[Model Structure on \( sMod_R \)]. By (3.7.4.2) applied to the equivalence with \( Ch_{\geq 0}R \), \( sMod_R \) has the structure of a model category where a morphism \( X \to Y \) is

- an equivalence if it is a weak equivalence,
- a fibration if \( NX_n \to NY_n \) for any \( n \geq 1 \).
- a cofibration if the maps of the degenerate diagrams is of the form

\[
X_n \to Y_n = X_n \oplus \bigoplus_{\varphi : [n] \to [k]} \varphi^*P_k
\]

compatible with the differential, and \( P_k \) are all projectives.

Prop. (8.1.2.12)[Fibrations]. A fibration of simplicial \( R \)-modules is a fibration iff it is a fibration of simplicial sets. Moreover, by (8.1.1.1), this is equivalent to \( X \to \pi_0X \otimes_{\pi_0(Y)} Y \) is surjective.

Proof: □

Prop. (8.1.2.13)[Simplicial Model Structure]. \( sMod_R \) admits a simplicial model category structure.

Proof: Firstly \( sMod_R \) is a simplicial category tensored and cotensored over \( Set_\Delta(3.1.5.6) \) by (3.12.1.5), then it suffices to show (3.7.6.3)? □

Prop. (8.1.2.14)[Model Structure on \( sCAlg_R \)]. By (3.7.4.2) applied to the forgetful functor to \( Set_\Delta \). Let \( R \) be a commutative algebra, then the category of simplicial commutative algebras \( sCAlg_R \) has a simplicial model category structure where a morphism is

- a weak equivalence if it is a weak equivalence of simplicial sets.
- a fibration if it is fibration of simplicial sets.

Proof: □

Cor. (8.1.2.15). For a ring map \( R \to S \), the tensor product \( S \otimes_R - \) and forgetful functor form a Quillen adjunction between \( sCAlg_R \) and \( sCAlg_S \).

Def. (8.1.2.16) [Free Morphisms]. A morphism of simplicial \( R \)-algebras is called free if it is \( s \)-free(3.12.1.4) on the a set of objects \( P_k \) where \( P_k \) are projective \( R \)-modules.
Prop.(8.1.2.17)[Cofibrations in $sAlg_R$]. A morphism in $sAlg_R$ is a cofibration iff it is a retraction of a free morphism(8.1.2.16). In particular, a cofibrant simplicial $R$-algebra is the symmetrization of a chain of projective $R$-modules.

Proof: This follows from(3.7.4.2)(3.1.6.5) and notice the free morphisms just corresponds free commutative algebra applied to the attaching cell morphism in the category of sets. □

Simplicial Resolutions

Def.(8.1.2.18)[Simplicial Resolutions].

- Let $M \in \text{Mod}_R$, a simplicial resolution of $M$ is a cofibrant replacement of $M$, or equivalently, it is an augmented simplicial $R$-module $X \to M$ that $NX \to M$ is a projective resolution.

- Let $M \in CAlg_R$, a free resolution of $M$ is free cofibrant replacement of $M$, or equivalently, it is an augmented simplicial commutative $R$-algebras $X \to M$ that $NX \to M$ is a resolution of $R$-modules, and $P_n$ are all projective(3.1.1.22) in $Alg_R$. Notice we can always choose a free resolution only only cofibrant resolution by (3.7.8.3) and Dold-Kan complex.

Def.(8.1.2.19)[Bar Resolution]. Let $C$ be a category and $T : C \to C$ a monad, and $X$ is an algebra over $T(3.2.1.2)$, then we can form a simplicial $T$-algebras where $B(T,X) = T_{n+1}X$ where the simplicial operators come from the action of $T$ on itself and the action of $T$ on $X$.

Then there is a simplicial morphism $B(T,X) \to X$, which is a simplicial homotopy.

Remark(8.1.2.20). If $C$ is the category of sets, $R$ is an algebra and $T$ is a functor that sends a set $S$ to $R[S]$, then a $T$-algebra is just an $R$-algebra, and the bar resolution is just the canonical resolution, and it is a cofibrant replacement, by (8.1.2.17).

Prop.(8.1.2.21). If $f, g : A^* \to B^*$ are two homotopic maps of cosimplicial Abelian groups, then $f, g$ induces an isomorphism between their totalizations.

Proof: Cf.[Sta019S]. □

3 Properties

Def.(8.1.3.1). If $A$ is a ring and $f_1, \ldots, f_n \in A$, the Koszul complex is defined to be

$$Kos(A, f_1, \ldots, f_n) = A \otimes_{\mathbb{Z}[X_1, \ldots, X_n]} \mathbb{Z}.$$ 

We want to extend this definition to the case of simplicial commutative rings.

Now if $A$ is a simplicial ring and $f_1, \ldots, f_n \in \pi_0(A)$, let $g_1, \ldots, g_n$ in $A_0$ lifting $f_i$, then we define

$$Kos(A, f_1, \ldots, f_n) = A \otimes_{\mathbb{Z}[X_1, \ldots, X_n]} \mathbb{Z}.$$

Then we need to check that this is independent of the lifting: if there is another set of lifting $h_i$, because we have identities

$$A \otimes_{\mathbb{Z}[X_1, \ldots, X_n]} \mathbb{Z} \cong (A \otimes_{\mathbb{Z}[X_1, \ldots, X_n]} \mathbb{Z}[X_1]) \otimes_{\mathbb{Z}[X]} \mathbb{Z}$$

it suffices to prove for $n = 1$. Then there is a $\gamma \in A_1$ that $d_0(\gamma) = g, d_1(\gamma) = h$. Then we consider the evaluating maps

$$e_0, e_1 : \text{Hom}(\Delta_1, A) \to A$$
are weak equivalences?, and then the maps
\[ e_0 : \text{Hom}(\Delta_1, A) \otimes_{\mathbb{Z}[X]}^L \mathbb{Z} \to A \otimes_{\mathbb{Z}[X]}^L \mathbb{Z} \]
\[ e_1 : \text{Hom}(\Delta_1, A) \otimes_{\mathbb{Z}[X]}^L \mathbb{Z} \to A \otimes_{\mathbb{Z}[X]}^L \mathbb{Z} \]
are also weak equivalences, so we are done.

And if \( M \) is a simplicial \( A \)-module, then we define
\[ \text{Kos}(M, f_1, \ldots, f_n) = M \otimes_A^L \text{Kos}(A, f_1, \ldots, f_n) \]

**Def. (8.1.3.2) [Flatness]** A map \( A \to B \) of simplicial rings is called **(faithfully)flat** if \( \pi_0(B) \) is (faithfully)flat over \( \pi_0(A) \) and \( \pi_i(A) \otimes_{\pi_0(A)} \pi_0(B) \to \pi_i(B) \) is an isomorphism for any \( i \).

**Prop. (8.1.3.3).** Flatness is stable under base change.

**Proof:** Cf. [Emerton note, completely flatness, P12]. \( \square \)

**Prop. (8.1.3.4).** If \( \pi_0(A) \otimes_A^L M \) is (faithfully)flat over \( \pi_0(A) \), then \( M \) is (faithfully)flat over \( A \).

**Proof:** Cf. [Emerton note, completely flatness, P12]. \( \square \)

**Def. (8.1.3.5).** If \( A \) is a simplicial ring and \( M \) is a simplicial \( A \)-module, if \( I = (f_1, \ldots, f_n) \) is an ideal of \( \pi_0(A) \), then \( M \) is called **I-completely flat** over \( A \) if \( \text{Kos}(M, f_1, \ldots, f_n) \) is flat over \( \text{Kos}(A, f_1, \ldots, f_n) \).

Clearly if \( M \) is \( A \)-flat, then it is \( I \)-completely flat.

**Prop. (8.1.3.6) [Flatness and Derived Completion].** If \( A \) is a simplicial ring, \( M \) is a flat simplicial \( A \)-module, and \( I = (f_1, \ldots, f_n) \) is an ideal of \( \pi_0(A) \), then its derived \( I \)-completion \( \tilde{M} = \text{holim}_n \text{Kos}(M, f_1^n, \ldots, f_n^n) \) is \( I \)-completely flat. The proof is similar to that of (4.6.7.4).

**Prop. (8.1.3.7) [Relative Regular Sequence].** If \( A \to B \) is a map of simplicial rings, then \( x_1, x_2, \ldots, x_n \in \pi_0(B) \) is called **regular with respect to** \( A_\bullet \) if
\[ A \to \text{Kos}(B, x_1, \ldots, x_n) \]
is flat. And if \( I = (f_1, \ldots, f_m) \in \pi_0(A) \), then it is called **I-completely regular** if
\[ \text{Kos}(A, f_1, \ldots, f_m) \to \text{Kos}(A, f_1, \ldots, f_m) \otimes_A^L \text{Kos}(B, x_1, \ldots, x_n) = \text{Kos}(B, f_1, \ldots, f_m, x_1, \ldots, x_n) \]
is flat. In particular, regular relative to \( A_\bullet \) implies \( I \)-completely regular relative to \( A_\bullet \).

**Prop. (8.1.3.8).** If \( (f_1, \ldots, f_{r-1}, f) \) is regular w.r.t. \( A \) and \( (f_1, \ldots, f_{r-1}, g) \) is regular w.r.t \( A \), then \( (f_1, \ldots, f_{r-1}, fg) \) is also regular w.r.t \( A \). In particular, for any \( n_i > 0 \), \( f_1^{n_1}, \ldots, f_r^{n_r} \) is also regular w.r.t. \( A \).

**Proof:** Similarly as in (4.4.4.6), we have a distinguished triangle
\[ \text{Kos}(M, f_1, \ldots, f_{r-1}, f) \to \text{Kos}(M, f_1, \ldots, f_{r-1}, fg) \to \text{Kos}(M, f_1, \ldots, g). \]
Then we can use induction. \( \square \)

**Prop. (8.1.3.9) [Regular and Derived Completion].** If \( x_1, \ldots, x_n \in \pi_0(B) \) is regular w.r.t \( A \), then they are \( I \)-completely regular w.r.t. \( A \) in the derived \( I \)-completion \( \tilde{B} \). The proof is similar to that of (8.1.3.6).
4 Non-Abelian Derived Functors

Prop.(8.1.4.1) [Left Derived Functor]. Let $F : Poly_A \to C$ be a functor where $C$ is any $\infty$-category admitting all colimits (e.g. $D(Ab)$), then there exists a left Kan extension $LF$ of $F$ along $Poly_A \subset CAlg_A$ that

- $LF$ commutes with filtered colimit.
- $LF$ commutes with geometric realization of simplicial resolutions: given $B \in CAlg_A$ and a simplicial resolution $P_\bullet \to B$ by $A$-algebras, the geometric realization $|LF(P_\bullet)|$ is equivalent to $LF(B)$.

which is called the left derived functor of $F$.

Proof: Cf.[Bhatt, Prism, 7.1.2]. □
8.2 Andre-Quillen-Cohomology

Basic references are [Andre-Quillen Cohomology of Commutative Algebras Iyenger]. See also [Quillen Cohomology of Commutative Rings] and [Quillen On the (Co-)homology of Commutative Rings]. [Smoothness, Regularity and Complete Intersections] is a must read.

1 Naive Cotangent Complex

This subsection is obsolete.

Prop.(8.2.1.1)[Polynomial Replacement]. For a morphism of ring morphisms \((R \to S) \to (R' \to S')\), let \(\alpha, \alpha'\) be two presentations, then there exists morphism of presentations, and different morphisms induce homotopic maps \(NL_{S/R} \to NL_{S'/R'}\).

Proof: Cf.[Sta00S1]. In fact, any surjective formally smooth representation will give the naive cotangent complex, up to quasi-isomorphism (8.2.1.4).

Cor.(8.2.1.2). If \(A = R[X_i]\) be a polynomial algebras, then \(NL_{A/R}\) is homotopic to \((0 \to \Omega_{B/A})\) because \(A \to A\) is a presentation with zero kernel.

If \(R \to A\) is surjective with kernel \(I\), then \(NL_{A/R}\) is homotopic to \((I/I^2 \to 0)\).

Lemma(8.2.1.3)[Formally Smooth Replacement 1]. If \(A \to B\) is a ring map that has two surjective presentations \(C \to B, D \to B\) with kernels \(I, J\). If there is a map \(C \to D\) commutating these two presentation, \(D\) formally smooth, and \(C \to D\) is surjective or \(C\) is formally smooth, then their corresponding naive cotangent complexes are quasi isomorphic.

Proof: Cf.[Foundations of Perfectoid Geometry P123].

Prop.(8.2.1.4)[Formally Smooth Replacement 2]. If \(B\) is an \(A\)-algebra that has two formally smooth presentation \(C \to B, D \to B\) with kernels \(I, J\). then their corresponding naive cotangent complexes are quasi isomorphic.

Proof: It suffices to prove they are both quasi isomorphic to the canonical cotangent complex.

For this, we first consider the diagram
\[
\begin{array}{c}
D \longrightarrow C \\
\downarrow \quad \downarrow \\
A[B] \longrightarrow B
\end{array}
\]
where \(D = A[S]\) and \(S = C \coprod A[B]\) as sets.

The two map \(D \to A[B]\) and \(D \to A[B]\) can be chosen because \(C \to B\) is surjective. So the results follows from (8.2.1.3).

Prop.(8.2.1.5)[Jacobi-Zariski Sequence]. Let \(A \to B \to C\) be a ring map. Choose a presentation \(\alpha : P \to B\) for \(B/A\) with kernel \(I\), a presentation \(\beta : Q \to C\) for \(C/B\) with kernel \(J\), a presentation \(\gamma : R \to C\) for the induced representation \(C/A\) with kernel \(K\), then there is an exact sequence of complexes:

\[
\begin{array}{c}
I/I^2 \otimes_B C \longrightarrow K/K^2 \\
\downarrow \quad \downarrow \\
0 \longrightarrow \Omega_{P/A} \otimes_B C \longrightarrow \Omega_{R/A} \otimes C \longrightarrow \Omega_{Q/B} \otimes C \longrightarrow 0
\end{array}
\]

Applying snake lemma, we get
\[
H_1(NL_{B/A} \otimes_B C) \to H_1(L_{C/A}) \to H_1(L_{C/B}) \to C \otimes_B \Omega_{B/A} \to \Omega_{C/A} \to \Omega_{C/B} \to 0.
\]
Proof: Cf.\[Sta\][00S2]. □

Prop.(8.2.1.6)[Localization]. Let \(A \to B\) be a ring map, for a multiplicative set \(S\) of \(B\), we have \(N L_{B/A} \otimes_B S^{-1}B\) is quasi-isomorphic to \(N L_{S^{-1}B/A}\).

Proof: Because it commutes with colimit, it suffice to prove for \(S = f\), and this is the content of lemma(8.2.1.7) below. □

Lemma(8.2.1.7). If \(A \to B\) is a ring map and \(\alpha: P \to B\) is a presentation of \(B\) with kernel \(I\), then \(\beta: P[X] \to B_g: X \to 1/g\) is a presentation of \(B_g\) with kernel \(J = I + (gX - 1)\). Then we have

1. \(J/\mathbf{g} = (I/I^2)_g \otimes B_g(fX - 1)\).
2. \(N L(\beta) \cong N L(\alpha) \otimes_B B_g \oplus (B_g \xrightarrow{g} B_g)\).

Hence \(N L_{B/A} \otimes_B B_g \to N L_{B_g/A}\) is a homotopy equivalence.

Proof: Cf.\[Sta\][08JZ]. □

2 Cotangent Complex

Def.(8.2.2.1)[Cotangent Complex]. The adjunction of \(A \otimes - \) and \(A \otimes \Omega_-/R\)(4.4.3.5) extends to an adjunction between \((sCAlg_R)_A\) and \(s\text{Mod}_A\). These categories are model categories by(8.1.2.11)(8.1.2.14) and (3.7.4.1), and \(A \otimes -\) preserves all weak equivalences and fibrations, so it is a Quillen adjunction(3.7.2.1). Then the cotangent complex \(L_{A/R}\) as a simplicial \(A\)-module is defined to be the total left derived functor applied to the trivial simplicial algebra \(A\). Equivalently, it is

\[L_{A/R} = A \otimes_X \Omega_X/R\]

where \(X\) is a cofibrant replacement(3.7.1.12) of \(A\).

Because of the Dold-Kan equivalence, we sometimes also call \(N L_{A/R}\) the cotangent complex.

Def.(8.2.2.2)[André-Quillen Homology and Cohomology]. The André-Quillen homology is defined to be

\[D_q(A/R) = \pi_q(L_{A/R}) = H_qN(L_{A/R})(8.1.2.2)\]

More generally, if \(M\) is an \(A\)-module, then let

\[D_q(A/R, M) = \pi_q(L_{A/R} \otimes_A M)\].

The André-Quillen cohomology is defined to be

\[D^q(A/R, M) = \text{Ext}^n(N L_{A/R}, M)\].

Prop.(8.2.2.3)[Functoriality]. The cotangent complex is functorial in arrows \(R \to A\): If there is a commutative diagram

\[
\begin{array}{ccc}
R & \to & S \\
\downarrow & & \downarrow \\
A & \to & B
\end{array}
\]

then there is a natural morphism \(L_{A/S} \otimes_A B \to L_{B/R}\). This is because if \(X\) is a cofibrant replacement for \(A\), then \(X \otimes_R S\) is also cofibrant object, because \(B \otimes_A -\) is a Quillen adjunction, by(8.1.2.15),
then it factors through $X \otimes_R S \to Y \to B$ where $Y$ is a cofibrant replacement of $B$, thus $Y$ is also cofibrant. Then the functor $L_{A/S} \otimes_A B \to L_{B/R}$ is induced by

$$B \otimes_A (A \otimes_X \Omega_{X/R}) \to B \otimes_Y \Omega_{Y/S}.$$

The formation of Kähler differential commutes with arbitrary colimit as it is a left adjoint, so the formation of cotangent complex commutes with filtered colimits, both in $A$ and $B$. Especially, it commutes with taking stalks, hence the sheaf of cotangent complexes of a map between schemes can be constructed as in the case of Kähler differentials, and it is a Qco sheaf.

**Def.** (8.2.2.4) [Canonical Resolution]. By the Dold-Kan correspondence, we will say that two simplicial $A$-modules are quasi-isomorphic iff their normalized nerves are quasi-isomorphic. Then $P_A(B) \to B$ is a quasi-isomorphic resolution of $B$, where $B$ is the trivial complex.

**Proof:** There is a homotopy $d$ between $\text{id}$ and $0$ for $n \leq 0$, where

$$d_n : (GF)^n G(B) \to (FG)^n \circ GFG(B)$$

using counit map, and on degree $0, -1$, it is $A[A[B]] \xrightarrow{\partial_1 - \partial_2} A[B] \to B \to 0$, which is clearly $0$, so this is a zero map.

Thus $\text{Tot}(P_A(B)) \cong B$, and $N_*(A) \cong \text{Tot}(A)$ by Dold-Kan correspondence, so we are done. □

**Cor.** (8.2.2.5).

$$D_0(L_{B/A}, M) = \Omega_{B/A} \otimes M, \quad D^0(A/R, M) = \text{Der}_R(A, M)$$

by the generator-relation definition of Kähler differential.

**Prop.** (8.2.2.6) [The fundamental Distinguished Triangle]. If $T$ is a site and $A \to B \to C$ are morphisms of sheaves of rings over $T$, then there is a morphism of simplicial $A$-modules that corresponds to distinguished triangles in $D^{\leq 0}(C)$ via Dold-Kan correspondence:

$$L_{B/A} \otimes_B C \to L_{C/A} \to L_{C/B}.$$

In particular, if $M$ is a $B$-module, then there are long exact sequences

$$\ldots \to D_1(A/R, M) \to D_1(B/R, M) \to D_1(B/A, M) \to M \otimes_A \Omega_{A/R} \to M \otimes_A \Omega_{B/A} \to M \otimes_B \Omega_{B/A} \to 0$$

$$\ldots \to D^1(A/R, M) \to D^1(B/R, M) \to D^1(B/A, M) \to \text{Der}_R(A, M) \to \text{Der}_A(B, M) \to \text{Der}_A(B, M) \to 0$$

**Proof:** Choose a simplicial resolution $X \to A$ where $X$ is free, then we factor the morphism $X \to A \to B$ to get a commutative diagram

$$\begin{array}{ccc} X & \xrightarrow{i} & Y \\ \downarrow & & \downarrow \\ A & \longrightarrow & B \end{array}$$

where $i$ is free, then we have an exact sequence (in $Ch_{\geq 0}(R)$ via Dold-Kan) of simplicial modules

$$0 \to B \otimes_X \Omega_{X/R} \to B \otimes_Y \Omega_{Y/R} \to B \otimes_Y \Omega_{Y/X} \to 0$$

because each $X_n \to Y_n = X_n \oplus_{\varphi: [n] \to [k]} \varphi^* P_k$ has a retraction, and use (4.4.3.7).
Notice we have a simplicial map \( A \otimes_X Y \to B \) which is a weak equivalence and \( A \otimes_X Y \) is a free simplicial \( A \)-algebra. Then it suffices to note that \( X_n \to Y_n = X_n \otimes \bigoplus_{[n] \to [k]} \phi^*P_k \) is projective implies
\[
B \otimes_Y \Omega_{Y/X} \cong B \otimes_{A \otimes_X Y} \Omega_{A \otimes_X Y/A},
\], and \( \Omega_{X/R} \) is termwise projective.

Prop. (8.2.2.7) [Properties of Cotangent Complexes].
- If \( B = s(P) \) where \( P \) is a projective \( A \)-module, then \( L_{B/A} \) is weakly equivalent to \( \Omega^1_{P/A}[0] \).
- (Kunneth Formula) If \( B, C \) are Tor independent over \( A \), then
\[
L_{B \otimes C/A} \cong (L_{B/A} \otimes A C) \oplus (L_{C/A} \otimes A B).
\]
- (Flat Base Change) If \( B, C \) are Tor independent over \( A \), \( L_{B \otimes A C} \) \( \cong L_{B \otimes A C/A} \).

Proof:
- \( S_n(P) \) is already cofibrant in \((sCAlg)_{/A}\).
- Let \( X \to B, Y \to C \) be cofibrant replacement of \( A, B \) respectively, then \( X \otimes_R Y \to B \otimes_A C \) is a cofibrant replacement, as \( X \otimes_A Y \) is cofibrant, and Tor independence shows
\[
\pi_*(X \otimes_A Y) = \pi_*(X) \otimes_A \pi_*(Y) = B \otimes_A C.
\]
thus the result follows from (4.4.3.6).
- The same as Künneth formula, noticing that \( X \otimes_A C \to B \otimes_A C \) is a weak equivalence by Tor independence, and \( X \otimes_A C \) is cofibrant.

3 Relations with Algebraic Properties
Cf.[Andre-Quillen Homology].

Prop. (8.2.3.1) [Acyclicity for Smooth Algebras]. If \( A \to B \) is smooth, then \( L_{B/A} \cong \Omega^1_{B/A}[0] \).
In particular, if \( A \to B \) is étale, then \( L_{B/A} = 0 \), and \( L_{C/A} \cong L_{B/A} \otimes_B C \), by distinguished triangle (8.2.2.6).

Proof: The cotangent complex is local, so we may assume it is standard smooth, so it factors as \( A \to A[X_1, \ldots, X_k] \xrightarrow{g} B \), where \( g \) is étale, so using the distinguished triangle and polynomial case, the result follows.

Prop. (8.2.3.2) [Compatibility with \( p \)-adic Completion]. If \( A \) is a \( p \)-adically complete commutative ring with bounded \( p \)-torsion and \( B \) is a flat \( A \)-module, then \( B \) also has bounded \( p^\infty \)-torsion by (4.6.2.4), let \( \hat{B} \) be the \( p \)-adic completion of \( B \), then the cotangent complex \( L_{\hat{B}/B} \) vanishes after derived \( p \)-completion.
In particular, by the distinguished triangle (8.2.2.6), if \( B \) is a smooth algebra, then \( L_{\hat{B}/B} \cong \Omega^1_{\hat{B}/B} \) is a finite projective \( \hat{B} \)-module.

Proof: This is true after base change \( \otimes_A^L A/p \) by flat base change (8.2.2.7), (4.6.7.4) and derived Nakayama (4.6.6.10).
4 Deformations

Prop.(8.2.4.1) [Topological Invariance of Étale Site]. Let $A$ be a ring, consider the following category: $C_A$ of flat $A$-algebras $B$ that $L_{B/A} = 0$, then if $A \to A$ is surjective with locally nilpotent kernel, then the base change defines an isomorphism of categories $C_A \cong C_A$.

The properties characterize the invariance of étale site under infinitesimal thickening.

Proof: ?

Prop.(8.2.4.2) [Relative Perfect Case]. If $A$ is a ring of char $p$ and $B$ is an $A$-algebra which is relatively perfect, i.e. $B^{(1)} = B \otimes A, \text{Frob} A \to B$ is an isomorphism, then $L_{B/A} = 0$.

Proof: Notice for any $A$-algebra $C$, the relative Frobenius induces zero map $L_{C^{(1)}/A} \to L_{C/A}$, because by using the canonical polynomial resolution, $d(x_p) = px^{p-1}xs = 0$. Now the relative Frobenius is an isomorphism $B^{(1)} \to B$, thus induces an isomorphism $L_{B^{(1)}/A} \to L_{B/A}$ by functoriality, thus $L_{B/A} = 0$.

Cor.(8.2.4.3) [Witt Vector Construction]. There is an equivalence of categories of $C_n = \text{flat } \mathbb{Z}/p^n\text{-algebras that } A/p \text{ is perfect and } C_1 = \text{perfect rings over } \mathbb{Z}/p$.

Notice for any $A$, $C_n$ is the usual adjointness of the Witt vector construction.

Proof: It suffices to show that $C_n \subset C_{\mathbb{Z}/p^n}$: By (8.2.4.2) and flat base change (8.2.2.7), $L_{A/(\mathbb{Z}/p^n)} \otimes_{\mathbb{Z}/p^n} \mathbb{Z}/p \cong L_{(A/p)/(\mathbb{Z}/p)} = 0$, so $L_{A/(\mathbb{Z}/p^n)} \otimes_{\mathbb{Z}/p^n} \mathbb{Z}/p^k \cong 0$ by induction, and so $L_{A/(\mathbb{Z}/p^n)} \cong 0$. For the last assertion, it is flat because it is torsion-free, which is because if $p(x_n) = 0$, then by $0 \to p^n \mathbb{Z}/p^{n+1} \to \mathbb{Z}/p^{n+1} \xrightarrow{p} \mathbb{Z}/p^n \to 0$ and the flatness of $A_{n+1}$, $x_{n+1} \in p^n A_{n+1}$, thus $x_n = 0$, and $x = 0$.

Prop.(8.2.4.4) [Adjointness of Witt Vectors]. Using a more careful analysis of cotangent complex (embedded deformation), we can show that if $A \to B \in C_A$ and there is an infinitesimal deformation $C \to C'$ of $A$-algebra, then a map $B \to C'$ can be lifted to an $A$-algebra map $A \to C'$.

In particular, taking inverse image, we get that $\text{Hom}_{\mathbb{F}_p}(A, B/p) \cong \text{Hom}_{\text{Alg}_{\mathbb{F}_p}}(W(A), B)$.

which is the usual adjointness of the Witt vector construction.

5 Algebra Extension

Cf.[Perfectoid Geometry Appendix B].

Def.(8.2.5.1) [Algebra Extensions]. Let $A \to B$ be a ring map and $M$ be a $B$-module, then an $A$-algebra extension of $B$ by $M$ is a short exact sequence of $A$-modules $0 \to M \to B' \to B \to 0$ that $B'$ is an $A$-algebra with $M$ being an ideal of it.

The set of such extensions are denoted by $\text{Exal}_A(B, M)$.

Prop.(8.2.5.2). $\text{Exal}_A(B, M)$ is a group under Baer sum, where the sum of two extension is the extension given by pushout, i.e. $(B_1 \oplus B_2)/\{(m, -m)|m \in M\}$. Moreover, it is a $B$-module, where the multiplication is the pushout along multiplication of $b$ on $M$. 
**Prop. (8.2.5.3).** There is a trivial extension given by $D_B(M) = B \oplus M$ (4.4.3.5), and the automorphism of $D_B(M)$ is isomorphic to $\text{Der}_A(B, M)$ via $d \mapsto \text{id} \oplus d$.

*Proof:* Cf. [Foundations of Perfectoid Spaces Masullo P118]. □

**Prop. (8.2.5.4).** Let $A \to B \to C$ be ring maps, then for any $C$-module $M$, there is an exact sequence

$$0 \to \text{Der}_B(C, M) \to \text{Der}_A(C, M) \to \text{Der}_A(B, M) \xrightarrow{\partial} \text{Exal}_B(C, M) \to \text{Exal}_A(C, M) \to \text{Exal}_A(B, M)$$

functorial in $M$. Where $\partial$ is given by (8.2.5.3).

*Proof:* Cf. [Foundations of Perfectoid Spaces Masullo P119]. □

**Prop. (8.2.5.5).** Let $A \to B$ be a ring map or a map of sheaves of rings, and let $M$ be a $B$-module, then there is an isomorphism of $B$-modules that is natural in $M$:

$$\text{Exal}_A(B, M) = \text{Ext}^1_B(NL_{B/A}, M).$$

*Proof:* Cf. [Foundations of Perfectoid Spaces, P127]. □

**Infinitesimal Deformation**

**Def. (8.2.5.6).** An **infinitesimal deformation** of a f.g. $k$-algebra is defined as an algebra $A'$ flat over $D = k[t]/(t^2)$ that $A' \otimes_D k = A$.

A f.g. $k$-algebra is called **rigid** if it has no infinitesimal deformations.

**Prop. (8.2.5.7).** Let $A$ be a f.g. $k$-algebra, write $A$ as a quotient of a polynomial ring over $k$ with kernel $J$, then there is an exact sequence $J/J^2 \to \Omega_{P/k} \otimes_P A \to \Omega_{A/k} \to 0$ (4.4.3.7), then we apply $\text{Hom}_A(-, A)$ and let $T^1(A) = \text{Coker}(\text{Hom}_A(\Omega_{P/k} \otimes_A A, A) \to \text{Hom}_A(J/J^2, A))$. Then $T^1(A)$ parametrize infinitesimal deformations of $A$. 
8.3 Derived Algebraic Geometry (Lurie)
9 Algebraic K-Theory of Schemes

9.1 K-Theory of Schemes

1 K-Groups of Schemes

Conj. (9.1.1.1) [Berlinson-Parshin]. For $k \in \text{Field}$, $\# k < \infty$, $X \in \text{SmProj} / k, i > 0$, $K_i(X) \otimes \mathbb{Q} = 0$.

Proof: □

Remark (9.1.1.2). In fact, when $\dim X = 0$ this is done by Quillen’s computation of K-groups of fields, Cf. [On the Cohomology and K-theory of the General Linear Groups over a Finite Field, Quillen, 1972].

when $\dim X = 1$, $K_i(X)$ are in fact finite, by [Finite Generation of K-Groups of a Curve over a Finite Field, Don 1982].
9.2 Brauer-Grothendieck Groups

References are [Central Simple Algebras and Galois Cohomology, Gille and Szamuely] and [The Brauer-Grothendieck Group].

1 Brauer Groups

Def.(9.2.1.1) [Brauer Groups]. For $X \in \mathbf{Sch}$, the Brauer group $\text{Br}(X)$ is defined to be $\text{Br}(X) = H^2_{\acute{e}t}(X, \mathbb{G}_m) = H^2_{\text{fppf}}(X, \mathbb{G}_m)(6.4.7.20)$. And for $R \in \mathbb{C}\text{Ring}$, $\text{Br}(R)$ is defined to be $\text{Br}(\text{Spec } R) = \text{Br}(R)$.

Prop.(9.2.1.2). If $X$ is a regular Noetherian scheme that is qc or integral, $\text{Br}(X) \to \text{Br}(\mathcal{O}(X))$ is injective, and $\text{Br}(X)$ is a torsion Abelian group.

Proof: The qc case reduces to the integral case, and this follows from [Brauer-Grothendieck Groups]Chap3.5.

The second assertion follows from the first and the fact $\text{Br}(\mathcal{O}(X))$ is torsion(9.2.2.3).

□

Cor.(9.2.1.3). If $X \to Y$ is a birational morphism of integral regular schemes, then $\text{Br}(Y) \to \text{Br}(X)$ is injective.

Proof: This follows from the fact $\text{Br}(Y) \to \text{Br}(X) \to \text{Br}(\mathcal{O}(X)) = \text{Br}(\mathcal{O}(Y))$ is injective.

□

Azumaya Brauer Groups

Prop.(9.2.1.4)[Azumaya Algebras of Schemes]. For $X \in \mathbf{Sch}$, an Azumaya algebra over $X$ is a coherent $\mathcal{O}_X$-algebra $\mathcal{A}$ s.t. $\mathcal{A}_x \neq 0$ for any $x \in X$, and satisfies the following equivalent definitions:

- There exists an étale covering $\{U_i \to X\}$ s.t. for each $i$, there exists $r_i \in \mathbb{Z}_+$ s.t. $\mathcal{A} \otimes_{\mathcal{O}_X} \mathcal{O}_{U_i} \cong \text{End}(\mathcal{O}_{U_i}^{r_i})$.

- There exists an fppf covering $\{U_i \to X\}$ s.t. for each $i$, there exists $r_i \in \mathbb{Z}_+$ s.t. $\mathcal{A} \otimes_{\mathcal{O}_X} \mathcal{O}_{U_i} \cong \text{End}(\mathcal{O}_{U_i}^{r_i})$.

- $\mathcal{A} \in \text{Vect}_X$, and for any arithmetic point $x \in X$, $\mathcal{A}_x$ is isomorphic to $\text{Mat}(r_x, \kappa(x))$ for some $r_x \in \mathbb{Z}_+$. And this $r_x$ is called the degree of $\mathcal{A}$ at $x$.

- $\mathcal{A} \in \text{Vect}_X$, and the canonical homomorphism $\mathcal{A} \otimes \mathcal{A}^{\text{op}} \to \text{End}_{\mathcal{O}_X}(\mathcal{A})$ is an isomorphism.

In particular, this definition is compatible with the definition of Azumaya algebras over fields in(2.4.3.2), (2.4.3.24).

The category of Azumaya algebras over $X$ is denoted by $\mathbf{Az}_X$. For $n \in \mathbb{Z}_+$, the subset of Azumaya algebras over $X$ of constant degree $n$ is denoted by $\mathbf{Az}^n_X$.

Proof: $1 \to 2 \to 3 \to 4$ is trivial by(2.4.3.24). $4 \to 1$: Cf.[Milne80 Etale Cohomologies]P141.

□

Def.(9.2.1.5)[Azumaya Brauer Groups]. Let $X \in \mathbf{Sch}$, the Azumaya Brauer group $\text{Br}_{\mathbf{Az}}(X)$ is defined to be the set of equivalence class of Azumaya algebras over $X$ under the equivalence relation that $\mathcal{A} \sim \mathcal{A}'$ iff there exists $\mathcal{E}, \mathcal{E}' \in \text{Vect}(X)$ with positive ranks at each point s.t.

\[
\mathcal{A} \otimes_{\mathcal{O}_X} \text{End}(\mathcal{E}) \cong \mathcal{A}' \otimes_{\mathcal{O}_X} \text{End}(\mathcal{E}').
\]

Moreover, $\text{Br}_{\mathbf{Az}}(X)$ is a group under tensor product and the inverse is given by $\mathcal{A} \to \mathcal{A}^{\text{op}}$. 

9.2. BRAUER-GROTHENDIECK GROUPS

Proof: To show this is an equivalence and the group operation is well-defined, use the fact that for \( E, E' \in \text{Vect}(X) \),
\[
\text{End}(E) \otimes_{\mathcal{O}_X} \text{End}(E) \cong \text{End}(E \otimes E').
\]
And the inverse is of the form given, by (9.2.1.4).

Lemma (9.2.1.6). Let \((\mathcal{C}, \mathcal{O})\) be a ringed site and \(F, G \in \text{Vect}(\mathcal{O})\) s.t. \(\text{End}(F) \cong \text{End}(G)\), then there exists an invertible sheaf \(\mathcal{L}\) s.t. \(F \otimes \mathcal{L} \cong G\).

Proof: Let \(\mathcal{L} \subset \text{Hom}(F, G)\) be generated as an \(\mathcal{O}_X\)-module by local isomorphisms \(\varphi: F \cong G\) s.t. the conjugation by \(\varphi\) coincides with the given isomorphism, then local computation and the fact all automorphisms of \(\text{Mat}(n)\) is inner shows that \(\mathcal{L}\) is invertible, and the evaluation map
\[
F \otimes \mathcal{L} \to G
\]
is an isomorphism.

Prop. (9.2.1.7). If \(A \in \text{Az}_X\) has constant degree \(d\), then \([A] \in \text{Br}_\text{Az}(X)\) is annihilated by \(d\).

Proof: Choose an étale covering \(\{U_i \to X\}\) and isomorphisms \(A|_{U_i} \cong \text{Hom}(F_i, F_i)\), where \(F_i \in \text{Vect}^d(X)\), then
\[
A^{\otimes d}|_{U_i} \cong \text{End}(F_i^{\otimes d}).
\]
Consider the maps
\[
p_i: F_i^{\otimes d} \to \Lambda^d F_i \subset F_i^{\otimes d},
\]
then \(p_i^2 = d! p_i\) and \(\text{rank}(p_i) = 1\). We show now that these \(p_i\) glue together to get a global section \(p\) of \(A^{\otimes d}\); by (9.2.1.6), there exist compatible invertible sheaves \(\mathcal{L}_{ij}\) on \(U_i \cap U_j\) s.t.
\[
F_i|_{U_{ij}} \otimes \mathcal{L}_{ij} \cong F_j|_{U_{ij}}.
\]
These isomorphisms can clearly generate isomorphisms to glue \(\{p_i\}\) together.

Then consider \(\mathcal{H} = A^{\otimes d} \circ p \subset A^{\otimes d}\), we claim that
- \(\dim \mathcal{H} = d^d\),
- left multiplication by \(A^{\otimes d}\) induces an isomorphism \(A^{\otimes d} \cong \text{End}(\mathcal{H})\).
Which will imply that \(d[A] = 0 \in \text{Br}_\text{Az}(X)\). To show these claims, it suffices to do local calculations: If \(F \cong \mathcal{O}_X e_1 \oplus \ldots \oplus \mathcal{O}_X e_d\), then \(A \cong \text{End}(\mathcal{O}_X^d)\), and
\[
p: e_{\sigma(1)} \otimes \ldots \otimes e_{\sigma(d)} \mapsto \text{sgn}(\sigma)e_1 \otimes \ldots \otimes e_d, \quad \sigma \in S_d, \quad 0 \text{ on other basis vectors}
\]
So
\[
\mathcal{H} = \{ f: F^{\otimes d} \to F^{\otimes d}: e_{\sigma(1)} \otimes \ldots \otimes e_{\sigma(d)} \mapsto \text{sgn}(\sigma)v_1 \otimes \ldots \otimes v_d, \quad 0 \text{ on other basis vectors}\}
\]
Then \(A \cong \text{End}(\mathcal{O}_X^d)\) is clear.

Cor. (9.2.1.8) [Azumaya Brauer Groups are Torsion]. If \(X \in \text{Sch}\) is qc or connected, then \(\text{Br}_\text{Az}(X)\) is a torsion Abelian group.
Comparison of Two Brauer Groups

Prop.(9.2.1.9)[Azumaya Brauer Groups via Cohomology]. Let $X \in \text{Sch}$, there exists an isomorphism of pointed sets

$$\text{Az}^n_X \cong \check{H}_1^1(X, \text{PGL}(n)).$$

Proof: As $\text{PGL}(n) = \text{Aut}(\text{Mat}(n))$ and any Azumaya algebra is a twist-form for $\text{Mat}(n)_X$, any $\mathcal{A} \in \text{Az}^n_X$ defines a 1-cocycle for $\text{PGL}(n)$. It is clear that if this cocycle is a coboundary, then $\mathcal{A} \cong \text{Mat}(n)_X$. Its left to show that any 1-cocycle comes from these: As $\text{PGL}(n) \subset \text{GL}(n^2)$, and 1-cocycle is a 1-cocycle for $\text{GL}(n^2)$, thus by (5.1.6.1) corresponds to a vector bundle $\mathcal{E}$ of rank $n^2$. By taking a refinement, this means there is a covering $\{U_i \rightarrow X\}$ and isomorphisms $\varphi_i : \text{Mat}(n, \mathcal{O}_{U_i}) \cong \mathcal{E}|_{U_i}$ as modules such that the transformation maps $\varphi_i^{-1} \circ \varphi_j \in \text{PGL}(n, \mathcal{O}_{U_{ij}}) \subset \text{GL}(n^2, \mathcal{O}_{U_{ij}})$, which means exactly $\mathcal{E} \in \text{Az}^n_X$. □

Prop.(9.2.1.10)[Brauer Groups and Azumaya Brauer Groups]. Assume $X \in \text{Sch}$ is qc and every finite subset of $X$ is contained in an affine scheme, by (5.3.2.19), the exact sequence

$$1 \rightarrow \mathbb{G}_m \rightarrow \text{GL}(n) \rightarrow \text{PGL}(n) \rightarrow 1$$

of algebraic groups gives a map

$$\check{H}_1^1(X, \text{GL}(n)) \rightarrow \text{Az}^n(X) = \check{H}_1^1(X, \text{PGL}(n)) \xrightarrow{\delta} \check{H}_2^1(X, \mathbb{G}_m) \rightarrow H^2_{\text{ét}}(X, \mathbb{G}_m) = \text{Br}(X).$$

by (9.2.1.9) and (5.3.2.14). So the kernel of $\delta : \text{Az}^n_X \rightarrow \text{Br}(X)$ is given by Azumaya algebras of the form $\text{End}(\mathcal{E})$ for $\mathcal{E} \in \text{Vect}^n(X)$. These maps for various $n$ give a map

$$\text{Az}(X) \rightarrow \text{Br}(X).$$

Then

- This map is an injective homomorphism, so $\text{Br}_{\text{Az}}(X) \subset \text{Br}(X)$.
- If $X$ has an ample invertible sheaf, then the map induces an isomorphism

$$\text{Br}_{\text{Az}}(X) \cong \text{Br}(X)_{\text{tor}}.$$

In particular, if $X$ is a regular quasi-projective scheme over some $A \in \text{cRing}$, then by (9.2.1.2),

$$\text{Br}_{\text{Az}}(X) \cong \text{Br}(X)_{\text{tor}} = \text{Br}(X).$$

For general $X$, this is also doable, by Gabber and de Jong.

Proof: 1: By taking disjoint union, it suffices to show that for $\mathcal{A} \in \text{Az}^n_X, \mathcal{B} \in \text{Az}^n_X$,

$$\delta_m(\mathcal{A} \otimes \mathcal{B}) = \delta_n(\mathcal{A}) \cdot \delta_m(\mathcal{B}).$$

But this is clear from the description of $\delta_n$: by the hypothesis and [Milne80 Etale Cohomology, Prop4.2.19] and (5.3.2.19), we may take an étale refinement $\{U_i\}$ and assume the cocycle corresponding to $\mathcal{A}$ is given by a cocycle $c_{ij}$ s.t. $c_{ij} \in \Gamma(U_{ij}, \text{GL}(n))$. Then $\delta(\mathcal{A})$ is represented by the 2-cocycle with $a_{ijk} = c_{jk} c_{ik}^{-1} c_{ij} \in \Gamma(U_{ijk}, \mathbb{G}_m)$.

The injectivity follows from the presentation

$$\text{Br}_{\text{Az}}(X) \cong \varprojlim \text{Az}^n_X / \sim = \varprojlim \check{H}_1^1(X, \text{PGL}(n))/\check{H}_1^1(X, \text{GL}(n)).$$
and the fact the image of $\tilde{H}^1_{\text{ét}}(X, \text{GL}(n))$ in $\tilde{H}^1_{\text{ét}}(X, \text{PGL}(n))$ is the class of $\text{End}(n, E)$: a $a \in \tilde{H}^1_{\text{ét}}(X, \text{GL}(n))$ corresponds to a vector bundle $E$ of rank $n$ with trivializations $\varphi_i : \mathcal{O}_{U_i}^n \cong E|_{U_i}$ s.t. $a$ is represented by $(\varphi_i^{-1} \varphi_j)$. Then $A = \text{End}(n, E) \in \text{Az}_n^1(X)$ has trivializations $\psi_i : \text{Mat}(n, \mathcal{O}_{U_i}) \cong \text{End}(n, E)|_{U_i}$, and $A$ corresponds to the 1-cocycle $(\psi_i^{-1} \psi_j)(a) = (\alpha_{ij})$, where $\alpha_{ij}(a) = \varphi_j^{-1} \varphi_i a \varphi_j^{-1} \varphi_i$, $a \in \text{Mat}(n, \mathcal{O}_{U_{ij}})$.

which is exactly the image of the class $a$ under the map $\text{GL}(n) \to \text{PGL}(n) : u \mapsto \text{conj}(u)$.


Prop. (9.2.1.11)[Kummer Exact Sequences]. For $X \in \text{Sch}, n \in \mathbb{Z}_+$, the Kummer exact sequence of algebraic groups

$$1 \to \mu_n \to \mathbb{G}_m \xrightarrow{n} \mathbb{G}_m \to 1$$

gives exact sequences

$$0 \to \text{Pic}(X)/n \text{Pic}(X) \to H^2_{\text{fppf}}(X, \mu_n) \to \text{Br}(X)[n] \to 0,$$

$$0 \to \text{Br}(X)/n \text{Br}(X) \to H^3_{\text{fppf}}(X, \mu_n) \to H^3_{\text{ét}}(X, \mathbb{G}_m)[n] \to 0.$$

by(6.4.7.20).

Prop. (9.2.1.12)[Mayer-Vietoris Exact Sequence]. Let $X \in \text{Sch}$ and $X = U \cup V$ be a Zariski covering with $U \cap V = W$, then by(9.2.1.2) there is an exact sequence

$$0 \to \Gamma(X, \mathcal{O}_X^\times) \to \Gamma(V, \mathcal{O}_X^\times) \oplus \Gamma(V, \mathcal{O}_X^\times) \to \Gamma(W, \mathcal{O}_X^\times)$$

$$\to \text{Pic}(X) \to \text{Pic}(U) \oplus \text{Pic}(V) \to \text{Pic}(W)$$

$$\to \text{Br}(X) \to \text{Br}(U) \oplus \text{Br}(V) \to \text{Br}(W) \to H^3_{\text{ét}}(X, \mathbb{G}_m) \to \ldots$$

And when $U$ is locally factorial, then $\text{Pic}(U) \to \text{Pic}(W)$ is surjective?, so there is an exact sequence

$$0 \to \text{Br}(X) \to \text{Br}(U) \oplus \text{Br}(V) \to \text{Br}(W) \to H^3_{\text{ét}}(X, \mathbb{G}_m).$$

Prop. (9.2.1.13)[Hochschild Spectral Sequence].

Residue Homomorphism

Prop. (9.2.1.14)[Faddeev]. For $k \in \text{Field}$, there is an exact sequence

$$0 \to \text{Br}(k) \to \text{Br}(\mathbb{P}^1_k) \xrightarrow{\text{res}} \bigoplus_{x \in \text{closed}(\mathbb{P}^1_k)} H^2(\kappa(x), \mathbb{Q}/\mathbb{Z}) \to H^1(k, \mathbb{Q}/\mathbb{Z}) \to 0$$

Proof: Cf. [GS06, 6.4.5]?

\[ \square \]
Artin Conjecture

Conj.(9.2.1.15)[Artin]. For $X \in \text{Sch}/\mathbb{Z}$ proper, $\# \text{Br}(X) < \infty$.

Proof: Cf.[Central Simple Algebras and Galois Cohomology, 6.4.5.]. □

Prop.(9.2.1.16)[Artin & Tate Conjecture]. For a proper surface $X/\mathbb{Z}$, the Artin conjecture for $X(9.2.1.15)$ is equivalent to Tate conjecture for divisors of $X$.

Proof: □

Prop.(9.2.1.17)[Artin & Tate-Shafarevich Conjecture]. For $F \in \text{Field}$, for a regular integral scheme $X$ of dimension 2 that is flat proper over $\mathcal{O}_F$ that has a section, the Artin conjecture for $X$ is equivalent to the finiteness of $\text{III}(\text{Jac}(X_F))$.

Proof: □

2 Brauer Groups of Fields

Prop.(9.2.2.1). For $k \in \text{Field}$, any Brauer class in $\text{Br}(k)$ is represented by a unique central division ring.

Proof: The existence of this division ring follows from Wedderburn theorem (2.4.1.22), and to show uniqueness, notice if

$$\text{Mat}(n, D) \cong \text{Mat}(m, D') = A$$

when we can recover $D$ as $D = D' = \text{End}_A(V)$, where $V$ is the unique simple module, by (2.4.1.21). □

Prop.(9.2.2.2)[Brauer Groups and Galois Cohomology]. For any $k \in \text{Field}$, the Brauer group $\text{Br}(k)$ is defined as the profinite cohomology $H^2(\text{Gal}(k_{\text{sep}}/k), (k_{\text{sep}})\times)$. For a Galois extension $L/k$, $\text{Br}(L/k)$ is defined as $H^2(\text{Gal}(L/k), L\times)$. Then by (10.1.2.2) we have

$$\lim_{\rightarrow} \text{Br}(L/k) = \text{Br}(k).$$

And by Hochschild-Serre spectral sequence and by Hilbert’s multiplicative theorem, we have the low term:

$$0 \to \text{Br}(L/k) \overset{\text{inf}}{\to} \text{Br}(k) \overset{\text{res}}{\to} \text{Br}(L)^{\text{Gal}(L/k)} \to H^3(\text{Gal}(L/k), L\times) \to H^3(k, (k_{\text{sep}})\times).$$

So $\text{Br}(L/k)$ is the kernel of $\text{Br}(k) \to \text{Br}(L)$.

Proof: Cf.[Neukirch Cohomology of Number Fields Chap6.3].? □

Cor.(9.2.2.3)[Brauer Groups are Torsion]. For any $k \in \text{Field}$, $\text{Br}(k)$ is a torsion Abelian group, by (10.1.2.3).

Cor.(9.2.2.4). For any $k \in \text{Field}$, $\# k < \infty$, $\text{Br}(F_q) = 0$, because the finite Galois extension is cyclic and unramified.

Prop.(9.2.2.5)[Finite Fields]. Let $k$ be a finite field, then for any $n \in \mathbb{N}$, $H^1(k, \text{PGL}(n)) = 0$, and $\text{Br}(k) = 0$. 

Proof: This follows from (9.2.2.1) and the fact any finite division ring is commutative (2.2.1.8).

Prop. (9.2.2.6) [Valued Fields]. Let \((R, K, k)\) be a complete DVR, then there exists a split exact sequence

\[
0 \to \text{Br}(k) \to \text{Br}_{\text{tame}}(K) \to H^1(k, \mathbb{Q}/\mathbb{Z}) \to 0.
\]

Proof: Cf. [Brauer-Grothendieck Group, P32].

3 Severi-Brauer Varieties

References are [Severi–Brauer varieties: a geometric treatment, Kollar] and [Central Simple Algebras and Galois Cohomology].

Def. (9.2.3.1) [Severi-Brauer Varieties]. For \(k \in \text{Field}\), a Severi-Brauer variety over \(k\) is a \(k\)-variety \(X\) that is a \(k\)-form for \(\mathbb{P}^n_k\) for some \(n \in \mathbb{N}\).

If \(K/k\) is a field extension and \(X_k \cong \mathbb{P}^n_k\), then \(K\) is called a splitting field for \(X\).

Prop. (9.2.3.2). Let \(k \in \text{Field}\) and \(X\) a Severi-Brauer variety over \(k\), then a twisted-linear subvariety of \(X\) is a closed subvariety of \(X\) s.t. the inclusion \(Y_k \subset X_k \cong \mathbb{P}^n_k\) embeds \(Y_k\) as a linear subvariety of \(\mathbb{P}^n_k\).

Prop. (9.2.3.3) [Châtelet]. For \(k \in \text{Field}\) and an \(n\)-dimensional Severi-Brauer variety \(X\) over \(k\), the following are equivalent:

- \(X \cong \mathbb{P}^n_k\).
- \(X \sim \mathbb{P}^n_k\).
- \(X(k) \neq \emptyset\).
- \(X\) contains a twisted-linear subvariety of codimension 1.

Proof: 1 \(\to\) 2 is trivial. If 2 holds, then to show item 3, if \(\#k = \infty\), then any Zariski open subset of \(\mathbb{P}^n_k\) contains a \(k\)-point, and if \(\#k < \infty\), clearly any Severi-Brauer variety over \(k\) splits over a finite Galois field extension of \(k\), so by the proof of (9.2.3.6)? shows that \(SB_n(K) \cong H^1(k, \text{PGL}(n)) = 1(9.2.2.5)\). Thus \(X \cong \mathbb{P}^n_k\) has a rational point.

4 \(\to\) 1: The twisted-linear subvariety is a divisor of \(X\), so it defines a rational map \(\varphi_D\) into some projective variety, and when base changed to \(\overline{k}\), it is the isomorphism of \(X\) with \(\mathbb{P}^n_{\overline{k}}\). Thus it must be an isomorphism.

3 \(\to\) 4: Cf. [Central Simple Algebras] P341.

Cor. (9.2.3.4) [Galois Splitting Fields]. Let \(k \in \text{Field}\) and \(X\) a Severi-Brauer variety over \(k\), then \(X\) has a finite Galois splitting field.

Proof: It suffices to show that \(k^s\) is a splitting field for \(X\). But for this, by the theorem, it suffices to notice \(X_{k^s}\) always has a rational point(5.10.1.10).

Cor. (9.2.3.5). Severi-Brauer groups satisfy the local-global property.


Prop. (9.2.3.6) [Severi-Brauer Varieties and Galois Cohomologies]. For \(k \in \text{Field}\), there is an isomorphism of pointed sets \(H^1(k, \text{PGL}(n)) \cong SB_n(L/K)\), where \(SB_n(L/K)\) is the isomorphism classes of Severi-Brauer varieties of dimension \(n - 1\) that splits in \(L\).

Proof: Cf. [Neukirch Cohomology of Number Fields P348].
4 Norm Residue Isomorphism Theorem

See Voevodsky’s work.
10 | Condensed Mathematics and Analysis

10.1 Profinite Cohomology

Reference are [Neu15] and the giant book [Neukirch Cohomology of Number Fields].

1 Group Cohomology

Let $G$ be a finite group.

Def. (10.1.1.1) [Group Cohomologies]. For $G \in \mathfrak{Grp}^{\text{fin}}$, the group cohomology $H^n(G, A)$ is the derived functor of the left exact functor

$$\text{Mod}_G \to \text{Ab} : H^0(G, A) = A^G = \text{Hom}_{\mathbb{Z}[G]}(\mathbb{Z}, A),$$

so $H^n(G, A) = \text{Ext}^n_{\mathbb{Z}[G]}(\mathbb{Z}, A)$.

The group homology $H_n(G, A)$ is the left derived functor of the right exact functor

$$\text{Mod}_G \to \text{Ab} : H_0(G, A) = A^\mathbb{G} = \mathbb{Z} \otimes_{\mathbb{Z}[G]} A,$$

so $H_n(G, A) = \text{Tor}^n_{\mathbb{Z}[G]}(\mathbb{Z}, A)$.

Prop. (10.1.1.2). For a normal subgroup $H$ of $G$, $A \mapsto A^H$ is left exact from $G$-mod to $G/H$-mod and preserves injectives because it is right adjoint to the exact inclusion functor as $\text{Hom}_G(B, A) = \text{Hom}_{G/H}(B, A^H)$. Dually for $A_H$.

Prop. (10.1.1.3). For $G = \mathbb{Z}$, we have a free resolution $0 \to \mathbb{Z}[t, t^{-1}] \xrightarrow{1+t} \mathbb{Z}[t, t^{-1}] \to \mathbb{Z} \to 0$. In particular, thus $H_n(\mathbb{Z}, \mathbb{Z}) = \mathbb{Z}$ iff $n = 0, 1$ and vanish otherwise.

Prop. (10.1.1.4) [Tate Cohomology]. There is a standard resolution of the $\mathbb{Z}[G]$-module $\mathbb{Z}$:

$$\cdots \leftarrow X_{-2} \leftarrow X_{-1} \xleftarrow{\mu_G} X_0 \leftarrow X_1 \leftarrow \cdots$$

that $X_q = X_{-q-1}$ are $\mathbb{Z}[G]$-module generated by $q$-cells $(\sigma_1, \ldots, \sigma_q)$, $X_0 = X_{-1} = \mathbb{Z}[G]$.

It then can be verified that for $G \in \text{Ab}^{\text{fin}}$, $\text{Hom}$ from this resolution gives out the Tate cohomology

$$H^n_T(G, A) = \begin{cases} H^n(G, A) & n \geq 1 \\
A^G/\text{tr}_G A & n = 0 \\
\text{tr}_GA/\text{tr}_G A & n = -1 \\
H_{-1-n}(G, A) & n \leq -2 \end{cases}$$
and \( H^n_F \) is a long exact sequence.

In particular, the Hom complex looks like:

\[
\cdots \to A_{-2} \xrightarrow{\varphi_{-1}} A_{-1} \xrightarrow{\varphi_0} A_0 \xrightarrow{\varphi_1} A_1 \xrightarrow{\varphi_2} A_2 \to \cdots
\]

where \( A_{-1} = A_0 = A \) and \( \varphi_0 x = tr_G x \), \( (\varphi_1 x)(\sigma) = \sigma x - x \), \( \varphi_2(x)(\sigma_1, \sigma_2) = \sigma_1 x(\sigma_2) - x(\sigma_1 \sigma_2) + x(\sigma_1) \).

**Proof:** Cf.[Neukirch CFT P13]?

**Remark (10.1.1.5).** From now on, consider only Tate cohomology.

**Prop. (10.1.1.6).**

\[
H^{-2}(G, \mathbb{Z}) = G^{ab}, \quad H^{-1}(G, \mathbb{Z}) = 0, \quad H^0(G, \mathbb{Z}) = 0, \quad H^1(G, \mathbb{Z}) = 0, \quad H^2(G, \mathbb{Z}) = \chi(G).
\]

**Proof:** \( H^0 \) is trivial and \( H^1(G, \mathbb{Z}) = H^0(G, \mathbb{Q}/\mathbb{Z}) = 0, \quad H^2(G, \mathbb{Z}) = H^1(G, \mathbb{Q}/\mathbb{Z}) = \text{Hom}(G, \mathbb{Q}/\mathbb{Z}) \).

For \( H^{-2}(G, \mathbb{Z}) \), use the dimension shifting \( 0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0 = H^{-1}(G, I_G) = I_G/I_G^2 \).

And \( G^{ab} \cong I_G/I_G^2 \) by \( \sigma \mapsto \sigma - 1 \).

**Prop. (10.1.1.7) [Group Cohomologies are Torsion].** For \( G \in \text{Ab}^{\text{fin}} \), \( \#G \cdot H^n(G, A) = 0 \) for any \( A \in \text{Mod}_G \). (True for \( H^0 \) and use dimension shifting). In particular, a divisible \( G \)-module \( A \) has trivial cohomology.

**Operations**

**Prop. (10.1.1.8) [Dimension Shifting].** There are fundamental split exact sequence \( 0 \to I_G \to \mathbb{Z}[G] \to \mathbb{Z} \to 0 \) and \( 0 \to \mathbb{Z} \to \mathbb{Z}[G] \to J_G \to 0 \), thus \( A_G = A/I_G A \). This can be used to tensor with \( A \) and define natural dimension shifting of cohomology \( \delta \).

**Lemma (10.1.1.9).** If \( H \) is a subgroup of \( G \), then by Grothendieck spectral sequence applied to \( \text{Mod}_G \xrightarrow{\text{res}} \text{Mod}_H \xrightarrow{(\cdot)_H} \text{Ab} \) shows that for \( A \in \text{Mod}_G \), \( H^*(H, A) \) is the same as the right derived functor of the functor \((\cdot)^H\) on \( \text{Mod}_G \).

**Def. (10.1.1.10) [Restrictions, Corestrictions and Inflations].** Let \( H \) be a subgroup of \( G \),

- The **inflation** is the \( \delta \)-morphism \( H^*(G/H, A) \to H^*(G, A) \) on \( \text{Mod}_{G/H} \) induced by the natural transformation? How to define it?

- The **restriction** are the \( \delta \)-morphisms \( H^*(G, A) \to H^*(H, A) \) on \( \text{Mod}_G \) induced by the natural transformation \( A^G \to A^H \).

- The **corestriction** are the \( \delta \)-morphisms \( H^*(H, A) \to H^*(G, A) \) on \( \text{Mod}_G \) induced by the natural transformation \( A^H \to A^G : a \mapsto N_{G/H} a \).

**Proof:** These exist by(3.4.4.5) and(10.1.1.9).

**Cor. (10.1.1.11).** Let \( H \) be a subgroup of \( G \), then \( \text{cor} \circ \text{res} = [G:H] \text{id} \).

**Prop. (10.1.1.12) [Kernel of Restriction].** If \( G \) is a finite group and \( H_1, H_2 \) are conjugate subgroups of \( G \) and \( M \in \text{Mod}_G \), then the kernel of the restriction maps \( H^1(G, M) \to H^1(H_1, M) \) are identical.
10.1. PROFINITE COHOMOLOGY

Proof: If a 1-cycle $\sigma \mapsto f(\sigma)$ is a cocycle, then it is a boundary when restricted to $H_1$ iff $f(\sigma) = \sigma(a) - a$ for some $a \in M$ for any $\sigma \in H_1$. Thus

$$f(x^{-1}\sigma x) = f(x^{-1}) + x^{-1} f(\sigma x) = -x^{-1} f(x) + x^{-1} f(\sigma) + x^{-1} \sigma f(x) = x^{-1}(\sigma(f(x) + a) - (f(x) + a))$$

is also boundary when restricted to $x^{-1}H_1x$. \square

Prop. (10.1.1.13) [Serre-Hochschild Spectral Sequence]. If $H$ is a normal subgroup of a finite group $G$, by Grothendieck spectral sequence, the relation $A^G = (A^H)^{G/H}$ gives us a spectral sequence $E$

$$E_{2}^{p,q} = H^{p}(G/H, H^{q}(H, A)) \implies E^{n} = H^{n}(G, A).$$

The edge morphisms are:

- inflation maps $H^{k}(G/H, A^{H}) \xrightarrow{\inf} H^{k}(G, A)$.
- restriction maps $H^{k}(G, A) \xrightarrow{\res} H^{k}(H, A)^{G/H}$.

And the lower parts give us:

$$0 \to H^{1}(G/H, A^{H}) \xrightarrow{\inf} H^{1}(G, A) \xrightarrow{\res} H^{1}(H, A)^{G/H} \xrightarrow{\text{transgression}} H^{2}(G/H, A^{H}) \xrightarrow{\inf} H^{2}(G, A).$$

dually for homology group.

Moreover if $H^{k}(H, A) = 0$ for $k = 1, \ldots, n - 1$, then the rows are blank, thus the above lower part can change to dimension $n$.

Proof: Prove the compatibility of inflation, restriction with the definition given in (10.1.1.10). \square

Cor. (10.1.1.14) [Hopf]. If $G = F/R$, $F$ is free, then use the homology spectral sequence, $H_2(G, \mathbb{Z}) \cong \frac{R\cap [F,F]}{[F,R]}$. Cf.[Weibel P198].

Prop. (10.1.1.15). For an isomorphism $(\sigma^*, \sigma)$ of a group and its cochain map in the sense that $\sigma^*(g)(\sigma(a)) = g(a)$, we have an isomorphism of Conjugation acts trivially on the group cohomology, because it does on $H^0$ because $H^0 = A^G$ fixed by $G$, and it commutes with dimension shifting. (Warning, if you count directly $a(\sigma \tau \sigma^{-1}) - \sigma a(\tau)$, you won’t get 0, but a 1-coboundary).

Prop. (10.1.1.16) [Cup Products]. The cup product is defined by $C^p(X, A) \times C^q(X, B) \to C^{p+q}(X, A \otimes B)$:

$$(a \smile b)(\sigma_1, \ldots, \sigma_{p+q}) = a(\sigma_1, \ldots, \sigma_p) \otimes \sigma_1 \ldots \sigma_p b(\sigma_{p+1}, \ldots, \sigma_{p+q}).$$

It satisfies $\partial(a \smile b) = \partial(a) \smile b + (-1)^p a \smile \partial(b)$, thus defines $a:

$$\smile : H^p(G, A) \times H^q(G, B) \to H^{p+q}(G, A \otimes B)$$

for $p, q \geq 0$. And in negative dimension this is also definable but not computable, Cf.[Neukirch Cohomology of Number Fields P42] or [Neukirch Class Field Theory 2015 P45].

- $a \smile b = a \otimes b$ for $a \in H^p(G, A), b \in H^q(G, B)$.
- $\delta(a \smile b) = \delta a \smile b, \delta(a \smile b) = (-1)^p(a \smile \delta b)$ for $a \in H^p(G, A)$.
- $\smile$ is associative and skew-symmetric (follows from dimension shifting and the last one.)
Proof:

Prop. (10.1.1.17) [Duality and Cup Product]. Let \( 0 \to A' \xrightarrow{i} A \xrightarrow{j} A'' \to 0 \) and \( 0 \to B' \xrightarrow{u} B \xrightarrow{v} B'' \to 0 \) be exact and there is a pairing \( \varphi : A \times B \to C \) that \( \varphi(A' \times A') = 0 \) hence induce a compatible pairing on \( A' \times B'' \) and \( A'' \times B' \), then we have

\[
\delta(\alpha) \sim \beta + (-1)^p \alpha \sim \delta(\beta) = 0
\]

for \( \alpha \in H^p(G, A'') \) and \( \beta \in H^q(G, B'') \).

Proof: Use the definition of \( \delta \), let \( a, b \) be the preimage of \( \alpha, \beta \) in \( A \) and \( B \), then \( \delta(\alpha) \sim \beta + (-1)^p \alpha \sim \delta(\beta) = a' \sim vb + (-1)^p ja \sim b' = \partial a \sim b + (-1)^p a \sim \partial b = \partial(a \sim b) \) is a boundary.

Prop. (10.1.1.18) [Naturality of Cup Products].

\[
\text{res}(a \sim b) = \text{res}(a) \sim \text{res}(b), \quad \text{inf}(a \cup b) = \text{inf}(a) \cup \text{inf}(b), \quad \text{cor}(\text{res} a \sim b) = a \sim \text{cor} b.
\]

Proof: Cf.[Neukirch CFT P48] or [Central Simple Algebras]P100.

Prop. (10.1.1.19). Let \( \sigma \in G^\text{ab} = H^{-2}(G, \mathbb{Z}) \) and \( a_1 \in H^1(G, A), a_2 \in H^2(G, A) \), then

\[
a_1 \sim \sigma = a_1(\sigma), \quad a_2(\sigma) = \sum_{\tau} a_2(\tau, \sigma).
\]

Cf.[Neukirch CFT P50,P51].

Prop. (10.1.1.20) [Cyclic Group Cohomologies]. For cyclic group, the Tate cohomology is 2-cyclic.

In particular, if \( \sigma \) be a generator for \( \mathbb{Z}/(n) \), then \( H^p(\mathbb{Z}/(n), A) = A^G/\text{tr}(A) \) for \( p \) even and \( H^p(\mathbb{Z}/(n), A) = \nu A/\langle \sigma - 1 \rangle A \) for \( p \) odd.

Proof: There is an exact sequence \( 0 \to \mathbb{Z} \to \mathbb{Z}[G] \xrightarrow{\sigma - 1} \mathbb{Z}[G] \to \mathbb{Z} \to 0 \), and this defines an isomorphism \( \delta^2 : H^0(G, \mathbb{Z}) \cong H^2(G, \mathbb{Z}) \). And this is also true for any \( A \) when tensored with it. The isomorphism is \( a \mapsto \delta^2 a = \delta^2(1) \sim a \).

Prop. (10.1.1.21) [Duality]. The cup product induces an isomorphism \( H^i(G, A^\vee) \cong (H^{-i-1}(G, A))^\vee \), i.e, \( H^n(G, A^\vee) \) and \( H_a(G, A) \) are dual to each other when \( n > 0 \), where \( A^\vee = \text{Hom}(A, \mathbb{Q}/\mathbb{Z}) \).

Proof: We only need to verify \( A^* G/N_G A^* \cong (N_G A/I_G A)^* \) and use dimension shifting. Should use the injectivity of \( \mathbb{Q}/\mathbb{Z} \) and the compatibility of cup product with dual.

Cor. (10.1.1.22). When \( A \) is \( \mathbb{Z} \)-free, the cup product also induce an isomorphism \( H^i(G, \text{Hom}(A, \mathbb{Z})) \cong H^{-i}(G, A)^\vee \).

Prop. (10.1.1.23) [Theorem of Cohomological Triviality]. For a \( G \)-module \( A \), if there is a \( q \) s.t. \( H^q(g, A) = H^{q+1}(g, A) = 0 \) for all subgroups of \( G \), then \( H^p(g, A) = 0 \) for any \( p \) and subgroup \( g \).

Cf.[Neukirch CFT P57].

Prop. (10.1.1.24) [Tate’s Theorem]. Assume \( A \) is a \( G \)-module that \( H^1(G, A) = 0 \) and \( H^2(g, A) \) is cyclic of order \( |g| \) for any subgroup \( g \) of \( G \), then for a generator \( a \) of \( H^2(G, A) \), there is an isomorphism

\[
a \sim : H^q(G, \mathbb{Z}) \cong H^{q+2}(G, A).
\]

Cf.[Neukirch CFT P79].
Cor. (10.1.1.25). In particular, by dimension shifting, if \( A \) is a \( G \)-module that \( H^1(G, A) = 0 \) and \( H^2(g, A) \) is cyclic of order \( |g| \) for any subgroup \( g \) of \( G \) this gives an isomorphism:

\[
a ↣ H^q(G, \mathbb{Z}) \cong H^{q+2}(G, A).
\]

for a generator \( a \) of \( H^2(G, A) \), because cup product commutes with dimension shifting.

**Miscellaneous**

Prop. (10.1.1.26) \([H^2 and Extensions, Schreier]\). For a \( G \)-module \( A \), there is a correspondence of equivalence classes of extension of \( G \) over \( A \) that are compatible with the \( G \) action and \( H^2(G, A) \).

**Proof:** Cf. [Weibel P183]. In fact there are also interpretations of \( H^3(G, A) \) as \( 0 → A → N → E → G \) under some equivalences. \( □ \)

Prop. (10.1.1.27) \([Herbrand Quotients for Cyclic Groups]\). When \( G \) is a cyclic group and \( A \) is a \( G \)-module, let \( f = σ − 1, \ g = 1 + σ + \ldots + σ^{n−1} \), then we can form a cyclic complex of order 2 and compute the Herbrand quotient (3.3.4.7). In this case, \( g_f, g \) is just \( |H_0(G, A)| \leftarrow |H_{−1}(G, A)| \). And by (3.3.4.9), if a \( G \)-morphism \( A → B \) has finite kernel and cokernel, then they have the same Herbrand quotient.

2 Cohomology of Profinite Groups

Prop. (10.1.2.1) \([Abelian Sheaves on \( T_G \)]\). For \( G \in \text{Prof} \), the category of Abelian sheaves on the canonical topology (5.1.2.4) \( T_G \) of \( G \)-sets is equivalent to the the category \( \text{Mod}^{\text{alg}}_G \), by \( Z ↦ \text{Hom}(−, Z) \). The inverse map is given by \( F ↦ \lim ← F(G/H) \).

**Proof:** The task is to prove \( F \cong h_{\lim F(G/H)} \). Cf. [Tamme P29].

The inverse of the Yoneda functor is the functor \( F ↦ F(G) \) as a left \( G \)-set where \( g_σ = F(σ)g \). The task is to show that \( F \cong h_{F(G)} \). For this, for any \( U \) we consider the covering \( \{G \xrightarrow{φ_U} U \) where \( φ_U(g) = gu \). Sheaf condition says

\[
F(U) \rightarrow \prod_{u \in U} F(G) \Rightarrow F(G \times_U G)
\]

is exact, in other words, \( F(U) \cong \text{Hom}_G(U, F(G)) \). \( □ \)

Prop. (10.1.2.2) \([Profinite Cohomologies]\). The **profinite cohomology** is the derived functor of \( A → A^G \) on the Abelian category \( \text{Mod}^{\text{alg}}_G(10.1.2.1) \)(It has enough injectives by (15.1.1.14)). It satisfies

\[
H^r(G, A) \cong H^r(C^*(G, A)) \cong \lim ← H^r(G/U, A^U)
\]

where \( C^*(G, A) \) is the set of continuous cochain complex of morphisms from \( G \) to \( A \) and the colimit is taken over the transition maps defined by inflations. Moreover, for the same reason, when \( G = \lim ← G_i \), and \( A = \lim ← A_i \), then

\[
H^r(G, A) \cong \lim ← H^r(G_i, A_i).
\]
Proof: The second is an isomorphism because \( C^n(G, A) = \lim_{\rightarrow} C^n(G/U, A^U) \) and direct limit is exact.

For the first, the \( H^0 \) obviously coincide, so it suffice to prove \( H^*(C(G, A)) \) form a universal \( \delta \)-functor. It is effaceable because \((-)^U\) preserves injective modules.(10.1.1.2).

For the last one, we need to check \( C^n(G, A) = \lim_{\rightarrow} C^n(G_i, A_i) \). Notice \( G \) has the profinite topology, thus must factor through some \( G_i \), and the right through some \( A_i \) because the image of a morphism from \( G^n \) to \( A \) has finite image. Thus the result follows. \( \square \)

Prop. (10.1.2.3) [Cohomology Groups are Torsion]. For \( G \in \text{Prof}, M \in \text{Mod}^\text{alg}_G, i \in \mathbb{N}, H^i(G, M) \) are torsion Abelian groups. And if \( G \) is a pro-\( p \)-group, then \( H^i(G, M) \) are \( p \)-primary torsion subgroups.

Proof: Notice if \( M \in \text{Mod}^\text{alg}_G \), this follows from (10.1.2.2) and (10.1.1.7). The last assertion is similar. \( \square \)

Def. (10.1.2.4) [Restrictions, Corestrictions and Inflations]. Let \( G \in \text{Prof} \) and \( H < G \) be a closed subgroup, for any \( A \in \text{Mod}^\text{alg}_G \), taking colimits over all open subgroup \( U \alpha \) of \( G \) of the restriction maps

\[
\text{res} : H^i(G/U_\alpha, A^{U_\alpha}) \rightarrow H^i(H/(H \cap U_\alpha), A^{U_\alpha}) \rightarrow H^i(H/H \cap U_\alpha, A^{H\cap U_\alpha}),
\]

by (2.1.14.6), we get a restriction map

\[
\text{res} : H^i(G, A) \rightarrow H^i(H, A).
\]

Similarly, if \( H \) is open in \( G \), we can define a corestriction map

\[
H^i(H, A) \rightarrow H^i(G, A).
\]

And if \( H \) is closed and normal in \( G \), we can define an inflation map

\[
H^i(G/H, A^H) \rightarrow H^i(G, A),
\]

as the colimit of the inflation maps

\[
H^i(G/HU_\alpha, A^{HU_\alpha}) \rightarrow H^i(G/H, A^{U_\alpha}).
\]

Prop. (10.1.2.5). \( \text{cor} \circ \text{res} = [G : H] \) for a subgroup \( H \) is also true for profinite cohomology (10.1.1.11), if \( H \) is an open subgroup of \( G \). This is because of (10.1.2.2).

Prop. (10.1.2.6). If \( H \) is a closed subgroup of a profinite group \( G \), \( p \in \mathfrak{P} \) s.t. \( p \nmid [G : H] \), then for any \( A \in \text{Mod}^\text{alg}_G, i \in \mathbb{N}, \text{res} : H^i(G, A) \rightarrow H^i(H, A) \) is injective on the \( p \)-primary part of \( H^i(G, A) \).

Proof: This follows from (10.1.2.5) and (10.1.2.4) by taking filtered colimits. \( \square \)

Lemma (10.1.2.7) [Shapiro].

\[
H_*(G, \text{Ind}^G_H(A)) \cong H_*(H, A), \quad H^*(G, \text{Ind}^G_H(A)) \cong H^*(H, A)
\]

because (co)induction is adjoint to exact functors, so it preserves injectives(projectives) and it is exact because \( \mathbb{Z}[G] \) is free \( \mathbb{Z}[H] \)-module.

And in the finite case, this is also true for Tate cohomology using dimension shifting.
Prop. (10.1.2.8) [Serre-Hochschild Spectral sequence]. The same spectral sequence as in the finite case (10.1.1.13) also applies to profinite cohomology with \( H \) closed normal in \( G \).

Def. (10.1.2.9) [Cup Products]. For any \( U \subset G \) open and \( A, B \in \text{Mod}_G^{\text{alg}} \), there are natural cup product maps
\[
H^*(G/U, A^U) \times H^*(G/U, B^U) \to H^*(G/U, A^U \otimes B^U) \to H^*(G/U, (A \otimes B)^U).
\]
Then by the naturality of inflation and the fact inflation commutes with cup product (10.1.1.18), we get a natural cup product map
\[
H^*(G, A) \times H^*(G, B) \to H^*(G, A \otimes B).
\]

Prop. (10.1.2.10). The cup products for profinite groups (10.1.2.9) is associative, graded-commutative, and commutes with inflations, restrictions and corestrictions as in (10.1.1.18).

Proof: \( \square \)

Cohomological Dimensions

Def. (10.1.2.11). The \( p \)-cohomological dimension \( cd_p(G) \) of a profinite group \( G \) is defined as the smallest integer \( n \) that the \( p \)-primary part of \( H^i(G, A) \) vanish for any torsion \( G \)-module \( A \). The strict \( p \)-cohomological dimension \( scd_p(G) \) of a profinite group \( G \) is defined as the smallest integer \( n \) that the \( p \)-primary part of \( H^i(G, A) \) vanish for any \( G \)-module \( A \).

The cohomological dimension \( cd(G) \) is defined to be \( \text{sup}_p(cd_p(G)) \). The strict cohomological dimension \( scd(G) \) is defined to be \( \text{sup}_p(scd_p(G)) \).

Prop. (10.1.2.12). For a profinite group \( G \), the following are equivalent:

- \( cd_p(G) \leq n \).
- \( H^i(G, A) = 0 \) for any \( i > n \) and any \( p \)-torsion \( G \)-module \( A \).
- \( H^{i+1}(G, A) \) for any simple \( p \)-torsion \( G \)-module \( A \).

And if \( G \) is pro-\( p \), then it suffice to check \( H^{n+1}(G, \mathbb{Z}/p\mathbb{Z}) = 0 \)

Proof: For any torsion \( G \)-module \( A, A = \oplus pA(p) \), so \( H^i(G, A(p)) \) is the \( p \)-primary part of \( H^i(G, A) \), so \( 1 \iff 2 \). For \( 3 \to 1 \): use the fact cohomology commutes with colimits (10.1.2.2), reduce to the case of \( A \) finite, and then use use the quotient tower.

The last assertion is by (2.1.14.15). \( \square \)

Prop. (10.1.2.13). \( cd_p(G) \leq scd_p(G) \leq cd_p(G) + 1 \).

Proof: Let \( A_p = \ker(p : A \to A) \). There are exact sequences \( 0 \to A_p \to A \xrightarrow{p} pA \to 0 \) and \( 0 \to pA \to A \to A/pA \to 0 \). \( A_p \) and \( A/pA \) are \( p \)-torsion \( G \)-modules, so if \( i > cd_p(G) + 1 \), then \( H^i(G, A_p) \) and \( H^{i-1}(G, A/pA) \) vanish. so \( H^i(G, A) \xrightarrow{p} H^i(G < pA) \) and \( H^i(G, pA) \to H^i(G, A) \) are injections, so their composition \( H^i(G, A) \xrightarrow{p} H^i(G, A) \) is injective, showing \( (H^i(G, A))_p = 0 \), so \( scd_p(G) \leq cd_p(G) + 1 \). \( \square \)

Prop. (10.1.2.14). For a closed subgroup \( H \) of a profinite group \( G \), \( cd_p(H) \leq cd_p(G) \) and \( scd_p(H) \leq scd_p(G) \), and if \( [G : H] \) is relatively prime to \( p \), then equality holds.

Proof: The first is because of Shapiro’s lemma (10.1.2.7). For the equality, use (10.1.2.6). \( \square \)
Cor. (10.1.2.15). \(cd_p(G) = cd_p(G_p) = cd(G_p), \quad scd_p(G) = scd_p(G_p) = scd(G_p)\).

Prop. (10.1.2.16). If \(H\) is a closed normal subgroup of \(G\), then \(cd_p(G) \leq cd_p(H) + cd_p(G/H)\), by Hochschild-Serre spectral sequence.

Prop. (10.1.2.17). If \(K\) is a field of char \(p\), then \(cd_p(G(K_s/K)) = 0\).

If \(H^2(G(K_s/L), K^*_s) = 0\) for all \(L/K\) separable, then \(cd(G(K_s/K)) \leq 1\). In particular \(H^1(G(K_s/K), K^*_s) = 0\) for \(i \geq 1\).

Proof: Let \(G_p\) be the Sylow \(p\)-subgroup of \(G(K_s/K)\) and \(M = K_s^{G_p}\). There is an exact sequence

\[0 \to \mu_p \to K_s \xrightarrow{x^p-x} K_s \to 0\]

and combined with the fact that \(H^i(G_p, K_s) = H^i(G(K_s/M), K_s) = 0\) for \(i \geq 1\) (10.1.3.1), so \(H^i(G_p, Z/pZ) = 0\) for \(i \geq 2\). Thus by (10.1.2.12) and (10.1.2.15), \(cd_p(G(K_s/K)) \leq 1\).

For the second assertion, similarly, for \(l \neq p\), consider the kernel of \(x^l\), \(\mu_l\) of \(l\)-th roots of unity in \(K_s\), and \(H^2(G_l, \mu_l(K_s)) = \varprojlim L\to H^2(G(K_s/L), \mu_l(K_s)) = 0\), so \(cd_l(G(K_s/K)) \leq 1\). Then \(cd(G(K_s/K)) \leq 1\), and \(scd(G(K_s/K)) \leq 2\), so \(H^1(G(K_s/K), K^*_s) = 0\) for \(i \geq 1\).

Proof. (10.1.2.18). For \(L/K\) field extension, \(cd_p(G(L_s/L)) \leq cd_p(G(K_s/K)) + \text{tr.deg}(L/K)\).

Proof: Cf. [Etale Cohomology Fulei P169].

Cor. (10.1.2.19). If \(k\) is separably closed and \(K\) be a function field over \(k\), then \(cd(G(K_s/K)) \leq 1\).

And if \(K\) is of char \(p > 0\), \(H^2(G(K_s/K), K^*_s)\) is a \(p\)-torsion group.

Proof: The first one is clear, for the second, for any \(l \neq p\), use the exact sequence \(\mu_l(K_s) \to K^*_s \xrightarrow{x^l} K^*_s \to 0\), then \(H^2(G(K_s/K), \mu_l(K_s)) = 0\), and \(H^2(G(K_s/K), K^*_s) \xrightarrow{l} H^2(G(K_s/K), K^*_s)\) is injective. \(l\) is arbitrary, so \(H^2(G(K_s/K), K^*_s)\) must be a \(p\)-torsion group.

3 Galois Cohomology

References are [Neukirch, Cohomology of Number Fields] Chap6. Should include [Galois Cohomology Serre].

Prop. (10.1.3.1) [Hilbert’s Additive Satz 90]. For \(K \in \text{Field}\), if \(L/K\) is a Galois extension, then \(H^n(G(L/K), L) = 0\) for \(n > 0\), where \(L\) is equipped with the discrete topology.

Proof: Form the normal basis theorem??, for finite Galois extension \(L/K\), \(L\) is an induced module over \(K\), thus \(H^*(G, L) = H_s(G, L) = 0\) for \(* \neq 0\) and \(H^*_p(G, L) = 0\) by (10.1.2.7).

Hence the same is true, for arbitrary Galois extension, when \(L\) is equipped with the discrete topology, the same as in the proof of (10.1.3.16).

Prop. (10.1.3.2) [Hilbert’s Multiplicative Satz 90]. \(H^1(\text{Gal}(L/K), L^*) = 0\) for any Galois extension \(L/K\), where \(L\) is equipped with the discrete topology.

Proof: This follows from (10.1.3.16).

Prop. (10.1.3.3) [Generalized Hilbert’s Additive Satz 90]. For \(L/K\) a Galois extension and \(k \in Z_+\), \(H^1(\text{Gal}(L/K), W^+_{p,k}(L)) = 0\).
10.1. PROFINITE COHOMOLOGY

Proof: By linear independence of characters, if $L/K$ is finite, then there is some $x_0 \in L$ s.t. $\text{tr}_{L/K}(x_0) \neq 0$. Then by (4.5.3.17), $x = (x_0, 0, \ldots, 0)$ is a unit in $W_{p,k}^+(L)$. Given any cocycle $\mu : \sigma \mapsto \mu_\sigma$, let

$$\theta = \text{tr}_{L/K}(x)^{-1} \sum_{\sigma \in \text{Gal}(L/K)} \mu_\sigma \sigma(x),$$

then for $\tau \in \text{Gal}(L/K)$,

$$\theta - \tau(\theta) = \text{tr}_{L/K}(x)^{-1} \sum_{\sigma \in \text{Gal}(L/K)} [\mu_{\tau \sigma}(\tau \sigma(x)) - \tau(\mu_\sigma)(\tau \sigma(x))] = \text{tr}_{L/K}(x)^{-1} \sum_{\sigma \in \text{Gal}(L/K)} (\tau \sigma)(x) = \mu_\tau.$$

Thus $\mu$ is a coboundary.

Hence the same is true, for arbitrary Galois extension, when $L$ is equipped with the discrete topology, the same as in the proof of (10.1.3.16).

□

Def. (10.1.3.4) [Galois Cohomologies]. For $k \in \text{Field}$, for any $M \in \text{Mod}^{\text{alg}}(\text{Gal}_k)$, denote $H^i(k, M) = H^i(\text{Gal}_k, M)$.

Prop. (10.1.3.5). $\text{Br}(R) = \mathbb{Z}/(2)$.

Proof: By (10.1.1.20) and (10.1.1.4), $H^2(\text{Gal}(C/R), C^\times) \cong \{u \in C^\times | u = u/|u|^2, u \in C^\times\} \cong \mathbb{Z}/(2)$.

□

Prop. (10.1.3.6) [Kummer Cohomology]. For $L/K$ a Galois extension and $\text{char} k = p \in P, r \in \mathbb{Z}_+$, then there exists an isomorphism

$$k^\times/(k^\times)^m \xrightarrow{\partial \cong} H^1(k, \mu_m).$$

Proof: This follows from the Kummer exact sequence and Hilbert’s theorem (10.1.3.2).

□

Prop. (10.1.3.7) [Restrictions and Corestrictions on $H^0$]. Let $K/k$ be a separable field extension, then

$$\text{res}_K^k = i : k \to K, \quad \text{cor}_K^k = \text{Nm}_{K/k} : K \to k.$$

Proof: This follows from the definition (10.1.1.10).

□

Cor. (10.1.3.8) [Change of Fields and Kummer Cohomology]. Let $K/k$ be a separable field extension and $m \in \mathbb{Z} \cap k^\times$, then there are commutative diagrams

$$\begin{array}{ccc}
k^\times & \xrightarrow{\partial} & H^1(k, \mu_m) \\
\downarrow & & \downarrow \text{res} \\
k^\times & \xrightarrow{\partial} & H^1(K, \mu_m) \\
K^\times & \xrightarrow{\partial} & H^1(K, \mu_m) \\
\end{array} \quad \begin{array}{ccc}
K^\times & \xrightarrow{\partial} & H^1(k, \mu_m) \\
\downarrow \text{Nm}_{K/k} & & \downarrow \text{cor} \\
K^\times & \xrightarrow{\partial} & H^1(k, \mu_m)
\end{array}$$


□

Prop. (10.1.3.9) [Artin-Schreier Cohomology]. Let $k \in \text{Field}, m \in \mathbb{Z} \cap k^\times$, then there exists an isomorphism

$$W_{p,r}(k)^+/(\text{Frob} - \text{id})W_{p,r}(k)^+ \cong H^1(k, \mu_m).$$

Proof: This follows from the Artin-Schreier exact sequence (10.1.3.3) and Hilbert’s theorem (10.1.3.3).

□
Prop. (10.1.3.10) [Unramified Classes]. Let $F$ be a global field and $G = \text{Gal}_F$, then for a $\text{Gal}_F$-module $M$, is called a **unramified class** at a place $v \in \Sigma_F$ if it is trivial when restricted to $H^k(I_v, M)$, where $I_v$ is the inertia group at $v$, which is defined only up to conjugacy, but this notion is well-defined by (10.1.1.12).

Prop. (10.1.3.11) [Unramified Classes are Rare]. Let $C$ be a proper Dedekind domain or a complete non-singular curve over a field $k$ with fraction field $F$ and $G = \text{Gal}_F$, then for any finite $G$-module $M$, if $S$ is a finite set of places in $F$ and $H^1(\text{Gal}_F, M, S)$ the set of elements of $H^1(\text{Gal}_F, M, S)$ that is unramified outside $S$, then $\#H^1(G, M, S) < \infty$.

Proof: By the inflation restriction exact sequence (10.1.1.13), we can reduce $G$ to a subgroup of finite index. And because $M$ is a finite $G$-module, there is a finite index subgroup of $G$ that acts trivially on $M$. Thus we can assume $M$ is $G$-trivial. But then if $m > 0$ s.t. $mM = 0$, then the assertion follows from the fact the maximal Abelian extension of exponent $m$ unramified outside $S$ is finite over $K(12.4.5.4)$. \qed

**Non-Abelian Cohomology**

Def. (10.1.3.12) [Non-Abelian Cohomology]. Let $G, M$ be topological groups, with a continuous action of $G$ on $M$, then we define $H^0(G, M) = M^G$.

We define $Z^1(G, M) = \text{continuous maps } x : G \rightarrow M$ such that

$$\sigma_1(x(\sigma_2))x(\sigma_1 \sigma_2)^{-1}x(\sigma_1) = 1, \quad \text{i.e.} \quad x(gh) = x(g)x(h)$$

If $x \in Z^1(G, M)$, then $x_m : \sigma \rightarrow m^{-1}x(\sigma)m \in Z^1(G, M)$ too. This defines an equivalence relation on $Z^1(G, M)$, the equivalence classes are called $H^1(G, M)$. This is compatible with the commutative case.

Prop. (10.1.3.13). Restriction map and inflation map is definable for $H^0$ and $H^1$, and $H^1(H, M)$ is a $G/H$-set where $G$ acts on $H^1(H, M)$ by $g(c)(h) = g(c(g^{-1}h))$.

Prop. (10.1.3.14). There is an exact sequence of pointed sets:

$$0 \rightarrow H^1(G/H, M^H) \xrightarrow{\text{inf}} H^1(G, M) \xrightarrow{\text{res}} H^1(H, M)^{G/H}.$$  

Proof: First $\text{res}(H^1(G, M)) \subset H^1(H, M)^{G/H}$ because $g(c)(h) = c(g)^{-1}c(h)h(c(g))$ is checked so $g(c)$ is cohomological to $c$.

$\text{res} \circ \text{inf} = 0$ is easy, if $\text{res}(c) = 0$, then $c$ is trivial on $H$, hence $c(gh) = c(g)$ and $h(c(g)) = c(hg) = c(g \cdot g^{-1}hg) = c(g)$, so $c$ is inflated from $H^1(G/H, M^H)$.

For the injectivity of $\text{inf}$, if $c(\overline{g}) = g^{-1}g(a)$, then $a \in M^H$, so it is a coboundary in $H^1(G/H, M^H)$. \qed

Prop. (10.1.3.15). Let $1 \rightarrow A \rightarrow B \rightarrow C \rightarrow 1$ be an exact sequence of $G$-groups, then there is a long exact sequence of pointed sets

$$1 \rightarrow A^G \rightarrow B^G \rightarrow C^G \xrightarrow{\delta} H^1(G, A) \rightarrow H^1(G, B) \rightarrow H^1(G, C) \xrightarrow{\Delta} H^2(G, A)$$

the last term is defined only when $A$ is in the center of $B$.

Where $\delta$ is defined as follows: for $c \in C^G$, let $b$ be an inverse image of $c$ in $B$, then $a_\sigma = b^{-1}\sigma(b) \in A$, and it defines a cocycle in $H^1(G, A)$, different choice differ by a coboundary, so it is well-defined.

$\Delta$ is defined as: for $c_\sigma$ a cocycle in $H^1(G, C)$, choose $b_s$ inverse images of $c_s$, then $a_{\sigma, r} = b_\sigma \sigma(b_r)b_\sigma^{-1}$ is a cocycle in $H^2(G, A)$. 

Proof: This is a special case of (5.3.2.19).

Prop. (10.1.3.16) [Hilbert’s Theorem 90]. For $L/K$ a Galois extension, $H^1(\text{Gal}(L/K), \text{GL}_n(L)) = 1$, where $L$ is equipped with the discrete topology.

Proof: We prove any cocycle is a coboundary, for this, notice any cocycle factor through a finite quotient, and the images of it is contained in a finite extension of $K$, hence it reduce to the case of $L/K$ finite.

By definition, this is equivalent to any $B$-semi-linear representation of $G$ free of finite rank is trivial, which is by (14.2.4.4).

\[ \text{Cor. (10.1.3.17) [semi-linear representations]. The proposition implies that any semi-linear } \]
$L$-representation of $G_{L/K}$ is trivial.

\[ \text{Cor. (10.1.3.18). } H^1(G(L/K), \text{SL}_n(L)) = 1. \] This is seen from the exact sequence $1 \to \text{SL}(n, L) \to \text{GL}(n, L) \to L^\times \to 1.$

\textbf{Continuous Cochain Complex}

In this subsubsection cohomology of $G$-modules with topology is studied. References are [Cohomology of Number Fields, Neukirch Chap 2.7].

\[ \text{Prop. (10.1.3.19). } H^i_{cts}(G, -) \text{ forms a long exact sequence for any } 0 \to A \to B \to C \to 0 \text{ of continuous } G\text{-modules.} \]

\[ \text{Proof:} \]

\[ \text{Prop. (10.1.3.20). If } A \text{ is a compact } G\text{-module which is an inverse limit of finite discrete } G\text{-modules } A_n, \text{ then if } H^i(G, A_n) \text{ is finite for all } n, \text{ then} \]
\[ H^{i+1}_{cts}(G, A) = \varprojlim_n H^{i+1}(G, A_n). \]

\[ \text{Proof: Cf. [Cohomology of Number Fields Neukirch P142].} \]

\[ \text{Lemma (10.1.3.21). Let } \pi \text{ be a topologically nilpotent element of } A \text{ which is complete in the } \pi\text{-adic } \]
\[ \text{topology and } \pi \text{ is not a zero-divisor, let } R = A/\pi A \text{ equipped with discrete topology. Let } G \text{ be a } \]
\[ \text{group which acts continuously on } A \text{ and fix } \pi, \text{ then if } H^1(G, R) \text{ is trivial, then } H^1(G, A) \text{ is trivial, and if moreover } H^1(G, GL_n(R)) \text{ is trivial, then } H^1(G, GL_n(A)) \text{ is trivial.} \]

\[ \text{Proof: Cf. [Galois Representations Berger P15].} \]

\[ \text{Prop. (10.1.3.22) [Cyclic Case]. if } G \text{ is a topological cyclic group } \langle g \rangle, \text{ then the map } H^1(G, M) \to \]
\[ M/(1 - g) \text{ is well-defined and injective. And when } M \text{ is profinite, } p\text{-adically complete, then the map is also surjective.} \]

\[ \text{Proof: The surjection: there is only one choice: } c(g^j) = (1 + g + \ldots + g^{j-1})(m). \text{ And we need to verify that it is continuous. The case of } p\text{-adic can be deduced from profinite case, because } c(\gamma) \in p^{-k}M \text{ for some } k, \text{ and } p^{-k}M \text{ is then profinite. For any finite quotient } N \text{ of } M, \text{ there is a } k \text{ that } kM = 0, \text{ and a } n \text{ that } g^n = id \text{ on } N, \text{ so } c(g^{kn}) = 0 \text{ on } N, \text{ which shows } c \text{ is continuous.} \]
Interpretation of $H^1$ and Torsors

**Def. (10.1.3.23) [A-Torsors].** A $G$-set $X$ is a discrete set with a continuous $G$-action on $X$. Let $A$ be a $G$-group, an $A$-torsor is a $G$-set with a right $A$-action that is simply transitive and semi-linear in $G$.

**Prop. (10.1.3.24) [$H^1$ and Torsors].** We have a canonical bijection of pointed sets: $H^1(G, A) \cong TORS(A)$.

*Proof:* Let $X$ be an $A$-torsor, choose $x \in X$, then $\sigma(x) = xa_\sigma$ for $a_\sigma \in A$. Now that $\sigma \mapsto a(\sigma)$ is checked to be a cocycle, and change of $x$ changes to $\sigma \mapsto b^{-1}a_\sigma(b)$. Conversely, for an $a \in H^1(G, A)$, we let $X = A$ be a right $A$-module, and let $\sigma'(x) = a_\sigma(x)$, i.e. regarding coming from $x = 1$, then this is a inverse map. \[\Box\]

**Prop. (10.1.3.25) [Extension of Rings].**

**Prop. (10.1.3.26).** There is an isomorphism of pointed sets $H^1(G, O(\varphi_L)) \cong E_\varphi(L/K)$.

*Proof:* Cf. [Neukirch Cohomology of Number Fields P346]. \[\Box\]
10.2 Condensed Mathematics(Scholze)

Main references are [Condensed Mathematics, Scholze]. [Lectures on Condensed Mathematics, Clausen-Scholze], [Lectures on Analytic Geometry, Clausen-Scholze].

Notations(10.2.0.1).
• Use notations defined in Profinite Cohomology.

1 Introduction

Remark(10.2.1.1). Delete this subsection.

Condensed mathematics is invented to overcome the subtleties when dealing with algebra together with topology. For example, the category of topological Abelian groups doesn’t form an Abelian category.

2 Condensed Objects

Def.(10.2.2.1)[κ-Condensed Objects]. The pro-étale site $^*_{pro\text{-}et}$ of a point is isomorphic to $\mathcal{P}rof$ in the standard topology. For any uncountable strong limit cardinal $\kappa$, the site $\mathcal{P}rof_{\kappa}$ is the category of $\kappa$-small profinite sets $S$ in the standard topology.

Then for any $C \in \text{Cat}$, we can define the category $\text{Cond}_{\kappa}(C)$ of $\kappa$-condensed objects in $C$ to be the category $\text{Func}(\mathcal{P}rof_{\kappa}, C)$.

Prop.(10.2.2.2)[Adjointness]. Given an uncountable strong limit cardinal $\kappa$, the functors

$$X \mapsto X : \text{Top} / \mathcal{G}rp / \mathcal{C}Alg \to \text{Cond}(\text{Set}) / \text{Cond}(\mathcal{G}rp) / \text{Cond}(\mathcal{C}Alg)$$

are faithful, and fully faithful when restricted to the category of $\kappa$-small objects.

And there is an adjunction

$$X \mapsto X : \text{Top} \rightleftarrows \text{Cond}(\text{Set}) : T \mapsto T(*)_{\text{top}} = \lim_{S \in \mathcal{P}rof_{\kappa}/T} S.$$ 

In particular, $X(*)_{\text{top}} \cong X_{\text{K-CG}}$.

Proof: Firstly, $X$ is truly a condensed set: for the sheaf condition, let $S' \to S$ be surjective morphism of profinite spaces, then the sheaf condition is true set-theoretically, and for any map $S \to T$, if $S' \to S \to T$ is continuous, then $S \to T$ is continuous, because $S' \to S$ is a closed map.

It suffices to check the set case, and the faithfulness and fully faithfulness follows from the adjointness

$$\text{Hom}_{\kappa-\text{Cond}(\text{Set})}(T, X) = \text{Hom}(T(*)_{\text{top}}, X).$$

Notice that any $s \in T(S)$ induces a map of sets $\pi : S \to T(*) : x \mapsto T(* \xrightarrow{x} S)(s)$, inducing the topology of $T(*)$. And by definition, a morphism $T \to X$ is just a morphism $T(*) \to X$ that for any $S \to T$, the composition $S \to T(*) \to X$ is continuous. And by definition, this is just a morphism from $T(*)_{\text{top}} \to X$.

The last assertion follows from the fact any compact Hausdorff space $S$ is a quotient space of its Stone-Čech compactification. $\square$
Prop. (10.2.2.3) [Free Condensed Abelian Groups]. By the adjoint functor theorem (3.1.1.35), the forgetful functor from Cond(\text{Ab}) to Cond(\text{Set}) has a left adjoint \( T \mapsto \mathbb{Z}[T] \). Concretely, \( \mathbb{Z}[T] \) is the sheafification of the functor that sends a compact Hausdorff space \( S \) to the free Abelian group \( \mathbb{Z}[T(S)] \). In particular, by Yoneda lemma, for any compact Hausdorff space \( S \), there is a condensed Abelian group \( \mathbb{Z}[S] \) that for any condensed Abelian group \( M \), \( \text{Hom}(\mathbb{Z}[S], M) = M(S) \).

Lemma (10.2.2.4). Consider the site of all \( \kappa \)-small compact Hausdorff topological spaces, then the category of sheaves on this site is equivalent to that of \( \text{Prof}_\kappa \) (via restriction).

Proof: Use (5.1.2.24), because any \( \kappa \)-small compact Hausdorff space is a quotient space of a \( \kappa \)-small profinite space \( \beta S_0(3.6.2.15) \), noticing that \( |\beta S| \leq 2^{2|\mathbb{S}|} < \kappa \).

Lemma (10.2.2.5). Consider the site of all \( \kappa \)-small extremally disconnected spaces, then the category of sheaves on this site is equivalent to that of \( \kappa \)-small condensed sets, via restriction.

Proof: Because any \( \kappa \)-small compactly generated space is a quotient space of a \( \kappa \)-small extremally disconnected space \( \beta \mathbb{S}(3.6.2.17) \), noticing that \( |\beta S| \leq 2^{2|\mathbb{S}|} < \kappa \).

Cor. (10.2.2.6) [Cond(\text{Ab}) and Extremally Disconnected Spaces]. The category of \( \kappa \)-condensed Abelian groups is equivalent to the category of presheaves \( \mathcal{F} \) on the category of \( \kappa \)-extremally disconnected spaces that \( \mathcal{F}(\emptyset) = 0 \) and \( \mathcal{F}(S_1 \coprod S_2) = \mathcal{F}(S_1) \times \mathcal{F}(S_2) \).

Proof: It suffices to show that the second sheaf condition is automatic: For a surjective map of extremally disconnected spaces \( f : \tilde{S} \to S \), there is an isomorphism
\[
\mathcal{F}(S) \xrightarrow{\mathcal{F}(f)} \{ g \in \mathcal{F}(\tilde{S}) | \mathcal{F}(p_1)(g) = \mathcal{F}(p_2)(g) \}.
\]
By (3.6.1.30), there is a section \( \sigma : S \to \tilde{S} \) that \( f \circ \sigma = \text{id}_S \), thus \( \mathcal{F}(\sigma) \circ \mathcal{F}(f) = \text{id} \), thus \( \mathcal{F}(f) \) is injective. For the surjectivity, suppose \( \mathcal{F}(p_1)(g) = \mathcal{F}(p_2)(g) \), then
\[
\mathcal{F}(p_2)(\mathcal{F}(f)\mathcal{F}(\sigma)(g)) = \mathcal{F}((\sigma \circ f) \times_S \text{id}_{\tilde{S}})\mathcal{F}(p_1)(g) = \mathcal{F}((\sigma \circ f) \times_S \text{id}_{\tilde{S}})\mathcal{F}(p_2)(g) = \mathcal{F}(p_2)(g)
\]
And similarly \( \mathcal{F}(p_2) \) is injective, thus \( g = \mathcal{F}(f)\mathcal{F}(\sigma)(g) \) is in the image.

Prop. (10.2.2.7) [Category of Condensed Abelian Groups]. The category of \( \kappa \)-condensed Abelian groups satisfies Grothendieck’s Axiom \( \text{AB} 3, \text{AB} 4, \text{AB} 5, \text{AB} 6, \text{AB} 3^*, \text{AB} 4^* \). And also it is generated by compact projective objects.

Proof: We use (10.2.2.6). Because all limits and colimits of Abelian groups commutes with finite products, the limits and colimits in the category of condensed Abelian groups are just the pointwise limits and colimits, thus the axioms follow form that of the category \( \text{Ab} \).

By (10.2.2.3), the condensed Abelian group \( \mathbb{Z}[S] \) for \( S \) \( \kappa \)-extremally disconnected satisfies \( \text{Hom}(\mathbb{Z}[S], M) = M(S) \), and by arguments above, \( M \to M(S) \) commutes with all limits and colimits, thus \( \mathbb{Z}[S] \) is compact and projective. And we show every \( M \) admits a surjection from some direct sum of \( \mathbb{Z}[S] \): use Zorn’s lemma, choose the maximal object \( M' \) that admits a surjection, if \( M/M' \neq 0 \), then find a nonzero map \( \mathbb{Z}[S] \to M/M' \) (because \( M(S) = 0 \) for any \( S \) implies \( M = 0 \)), then it lifts to a nonzero map \( \mathbb{Z}[S] \to M \) by projectivity, contradiction.

Cor. (10.2.2.8).
- We can define the tensor of two condensed Abelian groups \( M, N \) as the sheafification of the presheaf \( S \mapsto M(S) \otimes N(S) \).
We can define an internal Hom, which is right adjoint to tensor operator. In particular, for any compact Hausdorff space \( S \), \( \operatorname{Hom}(M, N)(S) = \operatorname{Hom}(\mathbb{Z}[S] \otimes M, N) \).

The derived category \( D(\operatorname{Cond}(\mathbb{A}b)) \) is also compactly generated, and we can define \( \mathbb{R}\operatorname{tensor} \) and \( \mathbb{R}\operatorname{Hom} \) as in \( \text{in}^2 \).

**Proof:** Cf.[Condensed Mathematics, P13].

**Prop. (10.2.2.9).** Let \( \kappa' > \kappa \) be uncountable strongly limit cardinals, then there is a natural functor from the set of \( \kappa \)-condensed sets to the category of \( \kappa' \)-condensed sets by pulling back along the morphism of sites \( \text{Prof}_{\kappa'} \rightarrow \text{Prof}_\kappa \). Then this functor is fully faithful and commutes with all colimits and \( \lambda \)-small limits, where \( \lambda \) is the cofinality of \( \kappa \).

**Proof:** This should have something to do with \( (5.1.2.24) \), thus it is left adjoint to the restriction functor and \( i^*i_* \cong \text{id} \), thus it is fully faithful and commutes with all colimits. For the limits, cf.[Condensed Mathematics, P14].

**Def. (10.2.2.10)[Condensed Objects].** For any \( C \in \mathbb{C} \), define the category \( \operatorname{Cond}(C) \) of condensed objects in \( C \) is defined to be the filtered colimits of the category of \( \kappa \)-condensed sets along the filtered poset of all uncountable limit cardinals \( \kappa \).

**Prop. (10.2.2.11).** If \( X \) is a T1 topological space, then \( X \) is a condensed set that all maps from points are quasicompact. Conversely, if \( T \) is a condensed set that all maps from points are quasicompact, then \( T(*)_{\text{top}} \) is a compactly generated T1 space.

**Proof:** Cf.[Condensed Mathematics, P16].

**Prop. (10.2.2.12)[\text{Top and } \operatorname{Cond}(\mathbb{S}et)].**

- The functor \( X \mapsto X \) induces an equivalence between compact Hausdorff space and qcqs condensed sets.

- A compactly generated space \( X \) is weak Hausdorff iff \( X \) is quasi-separated. For any quasi-separated condensed set \( T \), the space \( T(*)_{\text{top}} \) is compactly generated weak Hausdorff.

**Proof:** Cf.[Condensed Mathematics, P16].

**Prop. (10.2.2.13).** The example \( (\mathbb{R}, \text{disc}) \rightarrow (\mathbb{R}, \text{Nat}) \).

In particular, enlarging topological abelian groups into an abelian category precisely forces us to include non-quasi-separated objects.

# Cohomologies

**Prop. (10.2.3.1).** For any set \( I \), there is an isomorphism

\[
\check{H}^i(\prod_I S^1, \mathbb{Z}) \cong \bigwedge^i(\oplus_I \mathbb{Z}).
\]

preserving the natural cup product.

**Proof:** If \( I \) is finite, this follows from the classical calculation of the cohomology of the tori. If \( I \) is infinite, then we should use lemma\( (10.2.3.2) \) below.
Lemma (10.2.3.2). If $S_j, j \in J$ is a filtered system of compact Hausdorff spaces and $S = \varprojlim_{j \in J} S_j$, then there are natural maps
\[
\varprojlim_j \hat{H}^i(S_j, \mathbb{Z}) \to \hat{H}^i(S, \mathbb{Z})
\]
are isomorphisms.

Proof:

Prop. (10.2.3.3) [Z-Cohomology]. Let $S$ be a compact Hausdorff space, then there are natural functorial isomorphisms
\[
\hat{H}^i(S, \mathbb{Z}) \cong H^i_{\text{Cond}}(S, \mathbb{Z}).
\]

Proof: Because the Čech and sheaf cohomology of $S$ are equal by (5.3.5.18), it suffices to calculate for Čech cohomology.

Firstly, if $S$ is a profinite set, let $S = \varprojlim_j S_j$ where $S_j$ are finite, then

Prop. (10.2.3.4) [R-Cohomologies Vanish]. For any compact Hausdorff space $S$,
\[
H^i_{\text{Cond}}(S, \mathbb{R}) = 0
\]
for $i > 0$, and $H^0(S, \mathbb{R}) = C(S, \mathbb{R})$.

Proof: Cf. [Condensed Mathematics, P21].

4 LCAs
5 Solid Abelian Groups

Def. (10.2.5.1) [Solid Abelian Group]. For a profinite set $S = \varprojlim_i S_i$, define the condensed Abelian group
\[
\mathbb{Z}[S] = \varprojlim_i \mathbb{Z}[S_i].
\]
There is a natural map $S \to \mathbb{Z}[S]$, inducing a map $\mathbb{Z}[S] \to \mathbb{Z}[S]$.

Then a solid Abelian group is a condensed Abelian group $A$ that for any profinite set $S$ and a morphism of Abelian groups $\mathbb{Z}[S] \to A$ extends to a morphism $\mathbb{Z}[S] \to A$.

A complex $C \subset D(\text{Cond}(A\text{-}Ab))$ is called a solid complex if for all profinite set $S$, the natural map
\[
R\text{Hom}(\mathbb{Z}[S], C) \to R\text{Hom}(\mathbb{Z}[S], C)
\]
is an isomorphism.

Prop. (10.2.5.2) [Free Solid Abelian Group]. For a profinite set $S$,

- Consider \[ Z[S] = \varprojlim_i \mathbb{Z}[S_i] = \varprojlim_i \text{Hom}(C(S_i, \mathbb{Z}), \mathbb{Z}) = \text{Hom}(C(S, \mathbb{Z}), \mathbb{Z}). \]

This means that the underlying Abelian group of $Z[S]$ is the $\mathbb{Z}$-valued measures on $S$.

- There is some set $|I| \leq 2^{|S|}$, that there is an isomorphism $Z[S] \cong \prod_I \mathbb{Z}$.

- $Z[S]$ is solid both as a module and a complex.
Proof: 2: Take an isomorphism $C(S, \mathbb{Z}) \cong \bigoplus I \mathbb{Z}$, then

$$Z[S]^\bullet = \text{Hom}(C(S, \mathbb{Z}), \mathbb{Z}) \cong \text{Hom}( \bigoplus I \mathbb{Z}, \mathbb{Z}) \cong \prod I \mathbb{Z}.$$ 

3: We need to show the extension property, but by 2, it suffices to show for $Z[S]^\bullet = \mathbb{Z}$.

Prop. (10.2.5.3) [Category of Solid Abelian Groups]. The category Solid $\subseteq \text{Cond}(\text{Ab})$ is an Abelian subcategory that is stable under all limits, colimits and extensions. The objects $\prod I \mathbb{Z}$, where $I$ is any set, form a family of compact projective generators. The inclusion Solid $\subseteq \text{Cond}(\text{Ab})$ admits a left adjoint $M \mapsto M^\bullet$ which is the unique colimit-preserving extension of $Z[S] \mapsto Z[S]^\bullet$.

The functor $D(\text{Solid}) \to D(\text{Cond}(\text{Ab}))$ is fully faithful and its essential image is precisely the solid Abelian groups, and the inclusion admits a left adjoint $C \mapsto C'^\bullet$ which is left derived functor of $M \to M^\bullet$.

6 Analytic Geometry
7 Complex Geometry
10.3 Topological Commutative Algebra

Main references are [Hub93], [Bos15], [B-S19], [Mor19] and [Sch12].

1 Topological Abelian Groups and Rings

Def. (10.3.1.1) [Topological Rings]. A topological Abelian group is an Abelian group with a topology structure that the addition and inversion are all continuous.

A topological ring is a ring endowed with a topology structure that the addition, multiplication and inversion are all continuous.

Similarly we can define a topological module over a topological ring.

Def. (10.3.1.2) [Topologically Nilpotent Element]. Let $A$ be a topological ring, then $x \in A$ is called topologically nilpotent iff $x^n \to 0$ when $n \to \infty$.

Def. (10.3.1.3) [Bounded Sets]. A subset $S$ in a topological ring is called bounded iff for all open nbhd $U$ of 0, there exists an open nbhd $V$ of 0 that $VS \subset U$.

Def. (10.3.1.4) [Strict Morphism]. A strict morphism of topological rings is a continuous morphism that the quotient topology and the subspace topology coincides on the image.

Completion of Topological Abelian Groups

Prop. (10.3.1.5) [Completion]. There exists a completion functor left adjoint to the forgetful functor from the category of complete topological Abelian groups to the category of topological Abelian groups, given by Cauchy filters.

Proof: \[\square\]

Prop. (10.3.1.6) [Subgroups and Completion]. Let $A$ be a topological Abelian group, then the completion $\varphi : A \to \hat{A}$ induces a bijection between the set of open subgroups of $A$ and the open subgroups of $\hat{A}$, given by $G \mapsto \varphi(G) = \widehat{G}$.

Proof: Cf. [Mor19]P74. \[\square\]

Def. (10.3.1.7) [Restricted Power Series]. Let $R$ be a topological ring, then we can define the restricted power series over $R$ to be

$$R\langle X_1, \ldots, X_n \rangle = \{ \sum a_v X^v \in R[[X_1, \ldots, X_n]] | \lim_{v \to \infty} a_v \to 0 \}$$

Adic Rings

Def. (10.3.1.8) [Adic Rings]. An adic ring $R$ is a topological ring that the topology coincides with the $a$-adic topology for some ideal $a$ of $R$, and any such $a$ is called a ideal of definition.

Prop. (10.3.1.9) [Topologically Nilpotent Elements]. Let $A$ be an adic ring and $x \in A$, then the following are equivalent:

- $x$ is topologically nilpotent.
- There exists an ideal of definition $I$ that the image of $x$ in $A/I$ is nilpotent.
- There exists an ideal of definition $I$ that $x \in I$. 

In particular, the set $A^{00}$ of nilpotent elements is an open radical ideal of $A$, and it is the union of all ideals of definitions in $A$.

**Proof:** $3 \rightarrow 1 \rightarrow 2$ is trivial. $2 \rightarrow 3$: if $x$ is nilpotent in $A/I$, let $J = I + xA$, then $J$ is an open ideal, and $J^n \subseteq I$, so $I$-adic and $J$-adic topologies on $A$ coincide, so $J$ is an ideal of definition.

The rest is easy. \qed

**Prop. (10.3.1.10)** [Adic Localization]. If $R$ is an adic ring with an ideal of definition $a$, the restricted power series $R(\xi)$ is complete w.r.t. the $(a)$-adic topology, and in fact

$$R(\xi) \cong \lim_{n} R/a^n[\xi].$$

For $f \in R$, we can define the **adic completion** of $R$ at $f$ to be the

$$R\langle f^{-1} \rangle = \lim_{n} (R/a^n[\frac{1}{f}]).$$

The natural map $R(\xi) \to R\langle f^{-1} \rangle$ induces an isomorphism

$$R(\xi)/(1 - f\xi) \cong R\langle f^{-1} \rangle.$$

**Proof:** There is an isomorphism $R[\langle f^{-1} \rangle]/(a^n) \cong (R/a^n)[f^{-1}]$ because localization is flat, so we are done. \qed

**Remark (10.3.1.11).** There is another canonical morphism $R[\langle f^{-1} \rangle] \to R\langle f^{-1} \rangle$ which exhibits $R\langle f^{-1} \rangle$ as the completion of $R[\langle f^{-1} \rangle]$ w.r.t. the ideal $aR[\langle f^{-1} \rangle]$.

Then $R\langle f^{-1} \rangle$ is endowed with an $a$-adic topology, and if $a$ is f.g., then $R\langle f^{-1} \rangle$ is complete w.r.t. to the $aR\langle f^{-1} \rangle$-adic topology. Also we see $R\langle f^{-1} \rangle$ doesn’t depend on the choice of ideal of definition of $a$.

**Proof:** Consider the projective system of exact sequences:

$$0 \to (1 - f\xi)R/a^n[\xi] \to R/a^n[\xi] \to R/a^n[f^{-1}] \to 0,$$

which is a surjective system so by Mittag-Leffler(3.1.1.45), $\lim_{n}$ is exact(4.6.3.2), and there is an exact sequence

$$0 \to \lim_{n}(1 - f\xi)R[\xi] \to \lim_{n} R[\xi] \to \lim_{n} R[\langle f^{-1} \rangle] \to 0.$$

Now $\lim_{n}(1 - f\xi)R[\xi] \cong (1 - f\xi) \cong (1 - f\xi)R(\xi)$, because $1 - f\xi$ is not a zero-divisor in $R/a^n$, and we get the desired isomorphism. \qed

**Def. (10.3.1.12)** [Completed Tensor Product]. Let $(A, a), (B, b)$ be two complete adic rings, then we can define a **complete tensor product** ring $A \hat{\otimes} B$ as

$$A \hat{\otimes} B = \lim_{n} (A/a^n \otimes B/b^n)$$

this is just the $(a \otimes B + A \otimes b)$-adic completion of the tensor product $A \otimes B$, because $(a \otimes B + A \otimes b)^n$ and $(a^n \otimes B + A \otimes b^n)$ are cofinal.
Properties of \( R \)-Algebras

Def. (10.3.1.13) [Topologically of Finite Presentation]. Let \( R \) be an adic ring with an ideal of definition \( I \), then an \( R \)-algebra \( A \) is called

- of **topologically finite type** if it is isomorphic to an \( R \)-algebra \( R\langle \zeta_1, \ldots, \zeta_n \rangle / \frak{a} \) that is endowed with the \( I \)-adic topology and \( \frak{a} \) is an ideal of \( R\langle \zeta_1, \ldots, \zeta_n \rangle \).

- of **topologically finite presentation** if moreover the ideal \( \frak{a} \) is f.g.

- **admissible** if it is of topologically finite presentation and has no \( I \)-torsion.

Prop. (10.3.1.14) [Raynaud–Gruson]. Let \( A \) be an \( R \)-algebra of topologically finite type and \( M \) a finite \( A \)-module that is flat over \( R \). Then \( M \) is an \( A \)-module of finite presentation.

Proof: Cf.[Bos15]P165.

Cor. (10.3.1.15). Let \( A \) be an \( R \)-algebra of topologically finite type, then if \( A \) has no \( I \)-torsion, then \( A \) is of topologically finite presentation, in particular admissible(10.3.1.13).

Proof: Cf.[Bos15]P166.

Prop. (10.3.1.16) [Topologically of Finite Presentation is Local]. Let \( A \) be an \( R \)-algebra that is \( I \)-adically complete and separated, \( f_1, \ldots, f_r \) be a set of elements generating the unit ideal, then \( A \) is of topologically finite type/topologically finite presentation/admissible iff each \( A(f_i^{-1}) \) does.


2 Valuation Rings

Def. (10.3.2.1) [Valuation Ring]. A **valuation ring** is the maximum elements in the dominating ordering of local rings in a field \( K \), where \( B \) dominates \( A \) iff \( A \subset B \) and \( \frak{m}_B \cap A = \frak{m}_A \).

A valuation ring in \( K \) is called **absolutely algebraically closed** if \( K \) is alg. closed.

Prop. (10.3.2.2) [Valuation is Maximal]. Any local ring \( A \) in a field \( K \) is dominated by a valuation ring with fractional field \( K \).

Proof: Note that the dominating relation satisfies the condition of the Zorn’s lemma, so it suffices to prove that \( A \) is not maximal if its fractional field is not \( K \). Let \( t \notin K_0 = \text{frac} A \). If \( t \) is transcendental over \( K_0 \), then \( A[t] \) with the maximal ideal \( (\frak{m}, t) \) dominate \( A \). If \( t \) is algebraic over \( K_0 \), then there is a \( a \) that \( at \) is integral over \( A \), hence by (4.2.1.5) there is a maximal ideal of \( A[at] \) above \( A \), which proves the lemma.

Prop. (10.3.2.3) [Valuation Ring Criterion]. \( A \) is a valuation ring with field of fraction \( K \) iff for any \( x \in K, x \) or \( x^{-1} \) is in \( A \).

Proof: If \( A \) is a valuation ring, then for \( x \notin A \), we know that \( A[x] \) is a local ring, hence there is no prime over \( \frak{m} \) otherwise \( A[x] \) is a bigger local ring, so we see \( \frak{m} A[x] = A[x] \), i.e. \( 1 = \sum t_i x^i \), so \( x^{-1} \) is integral over \( A \). Now \( A[x^{-1}] \) has a \( \frak{m}' \) over \( \frak{m} \), so \( A = A[x^{-1}]_{\frak{m}'} \), which shows \( x^{-1} \in A \).

Conversely, if for any \( x \in K, x \) or \( x^{-1} \) is in \( A \), we assume \( A \) is not \( K \), so \( A \) is not field by the condition. Then it has a non-zero maximal ideal, but only one, otherwise we can choose \( x, y \) that \( x/y, y/x \notin A \). And \( A \) is maximal because if there is a \( A \subset A' \), and a \( x \in A' \), then if \( x \notin A \), then \( x^{-1} \in A \), hence also in \( \frak{m}_A \), so it is in \( \frak{m}_{A'} \), but now \( x^{-1} \) cannot be in \( A' \), contradiction.
Cor. (10.3.2.4). For $K \subset L$ subfield, if $A$ is a valuation ring of $L$, then $A \cap K$ is a valuation ring of $K$. And if $L/K$ is algebraic and $A$ is not a field, then $A \cap K$ is not a field. (This is because the primes of $A$ are all over 0 so cannot contain each other (4.2.1.5) so $A$ is a field).

Cor. (10.3.2.5). The quotient $A/p$ at a prime is a valuation ring, and any localization of valuation ring is a valuation ring, by this criterion.

Prop. (10.3.2.6) [Valuation Ring is Normal]. Valuation ring is normal, because for $x$ algebraic over $A$, either $x \in A$, or $x$ is a combination of $x^{-1}$ thus in $A$, by (10.3.2.3).

Cor. (10.3.2.7) [Integral Closure and Valuation Ring]. The integral closure of a subring in a field $K$ is the intersection of valuation rings containing $A$.

Proof: Valuation ring is integrally closed, so it suffices to prove if $x$ is not algebraic over $A$, then there is a valuation ring of $A$ not containing $x$. This is because $x \notin B = A[x^{-1}]$ otherwise $x$ is integral over $A$. Now $x^{-1}$ is not a unit in $B$, hence $x \in p \in B$, hence $B_p$ is dominated by some valuation ring $V$, and $x \notin V$ because $x^{-1} \notin m_V$.

Prop. (10.3.2.8) [Bezout Domain and Valuation Ring]. A valuation ring is equivalent to a Bezout local domain.

Proof: One way is because the element of minimum valuation generate the ideal. Conversely, for $f, g \in A$, $(f, g) = (h)$, so $f = ah, g = bh$, and $h = cf + dg$, then $ab + cd = 1$, hence $a$ or $b$ is a unit, so $f/g \in A$ or $g/f \in A$. By (10.3.2.3), $A$ is a valuation ring.

Prop. (10.3.2.9). A valuation ring is Noetherian iff it is discrete valuation iff it is PID.

Proof: Only need to prove Noetherian then $\Gamma = \mathbb{Z}$. we know ideals of $\Gamma$ of the form $\{x | x \geq \gamma\}$, where $\gamma > 0$ has a maximal element, so there is a minimal element bigger than 0, so $\Gamma \cong \mathbb{Z}$.

Prop. (10.3.2.10). In a fixed field, any inclusion relation of two valuation ring is given by localization.

Proof: Just localize at the image of the maximal ideal $m_B \cap A$, then they are valuation rings (10.3.2.5) that dominate each other, thus they are the same by definition (10.3.2.1).

Def. (10.3.2.11) [Extension of Valuation Rings]. An injective local homomorphism of valuation rings is called an extension of valuation rings. By (4.4.1.29), it is equivalent to a f.f. morphism of valuation rings.

3 Valuations

Def. (10.3.3.1) [Valuations]. A valuation on a field $K$ is surjective map $v : K \to \Gamma$ where $\Gamma$ is an ordered Abelian group (2.2.8.1), called the value group of $K$.

The rank of a valuation is defined as the height of its value group (2.2.8.4).

Prop. (10.3.3.2) [Valuation Ring and Valuation]. Valuation rings (10.3.2.1) $A$ of a field $K$ is equivalent to valuations on $K$ (10.3.3.1).

The equivalence is given by $K = Q(A), \Gamma = K^*/A^*$ and that $A = v^{-1}(\{x \geq 0\})$.

Proof: These are definitely valuation rings, and if $A$ is a valuation ring by (10.3.2.3), then we set $\Gamma = K^*/A^*$, where $A^*$ is the invertible elements of $A$ and $x \leq y$ iff $y/x \in (A - \{0\})/A^*$. This is totally ordered by (10.3.2.3).
Cor. (10.3.3.3) [Rank and Dimension]. A valuation ring of rank \( n \) has Krull dimension \( n \), because clearly the convex subgroups of \( \Gamma \) is in bijection with ideals of \( A \).

Prop. (10.3.3.4) [DVRs]. For a Noetherian local domain \( A \) of dimension 1 with maximal ideal \( \mathfrak{m} \) and residue field \( k \) that is not a field, the following are equivalent:

1. \( A \) is a valuation ring corresponding to a discrete valuation in (10.3.3.2).
2. \( A \) is normal.
3. \( \mathfrak{m} \) is a principal ideal.
4. \( A \) is regular.
5. Every nonzero ideal is a power of \( \mathfrak{m} \).
6. There exists a \( x \in A \) that every nonzero ideal is of the form \((x^k)\).

Such a ring is called a **discrete valuation ring** or a DVR.

**Proof:**

1 \( \rightarrow \) 2: Valuation ring is integrally closed, by (10.3.2.6).

2 \( \rightarrow \) 3: As the radical of any non-trivial ideal \((a)\) is \( \mathfrak{m} \), and \( A \) is Noetherian, so there is an \( n \) that \( \mathfrak{m}^n \subseteq a \) and \( \mathfrak{m}^{n-1} \nsubseteq a \). Then choose \( b \in a - \mathfrak{m}^{n-1} \), \( x = a/b \in K \), then \( x^{-1} \notin A \), then it is not integral over \( A \). So \( x^{-1} \mathfrak{m} \nsubseteq \mathfrak{m} \), but \( x^{-1} \mathfrak{m} \subseteq A \), so it equals \( A \), which means \( \mathfrak{m} = (x) \).

3 \( \rightarrow \) 4: Clear.

4 \( \rightarrow \) 5: For any ideal \( a \), its radical is \( \mathfrak{m} \) and \( A \) is Noetherian, so \( \mathfrak{m}^n \subseteq a \). Now \( A/\mathfrak{m}^n \) is Artinian by (4.1.3.4), so by (4.1.3.6) \( a \) is a power of \( \mathfrak{m} \).

5 \( \rightarrow \) 6: And \( x \in \mathfrak{m} - \mathfrak{m}^2 \) will do.

6 \( \rightarrow \) 1: Define \( v(a) = k \) if \( (a) = (x^k) \).

\( \square \)

Cor. (10.3.3.5) [Noetherian Valuation Rings are DVRs]. A Noetherian valuation rings are automatically DVRs.

**Proof:** This is implicit in the proof above.

\( \square \)

Prop. (10.3.3.6). Let \( R \) be a Noetherian local domain with fraction field \( K \) and \( R \neq K \), then there exists a Noetherian local ring \( R' \) of dimension 1 that dominates \( R \) s.t. \( R \rightarrow R' \) is essentially of f.t..

**Proof:** Cf. [Sta]00PS.

\( \square \)

Cor. (10.3.3.7) [Dominance by DVRs]. Let \( R \) be a Noetherian local domain with fraction field \( K \) and \( R \neq K \), \( L/K \) a f.g. filed extension, then there exists a a DVR \( A \) with fraction field \( L \) which dominates \( R \).

**Proof:** First we can reduce to the case \( L/K \) is finite: If it is not finite, choose a transcendence basis \( x_1, \ldots, x_r \), and replace \( R \) by \( R[x_1, \ldots, x_r]/\mathfrak{m}_R, x_1, \ldots, x_r \).

In the finite case, first we can reduce to the case \( \dim R = 1 \) by (10.3.3.6), and let \( A \) be the integral closure of \( R \) in \( L \), then by (4.1.1.50), \( A \) is Noetherian, and \( R \rightarrow A \) is integral so there exists a maximal prime \( \mathfrak{n} \subseteq A \) that \( \mathfrak{n} \cap R = \mathfrak{m}_R \). Thus \( A_\mathfrak{n} \) is a DVR by (10.3.3.5).

\( \square \)

Valuations of Rank 1

In this subsubsection, all valuations are of rank 1.

Remark (10.3.3.8) [Real Valuations]. As an ordered Abelian group of height 1 can be embedded into \( \mathbb{R}(2.2.8.5) \), a valuation \( v \) on a field of rank 1 is equivalent to a real-valued valuation.
Def. (10.3.3.9) [Multiplicative Valuation]. For a real continuous valuation $v$, we can define a multiplicative valuation $| \cdot |$ where $|a| = \exp(-v(a))$. Then it is multiplicative.

Def. (10.3.3.10) [non-Archimedean Valuations]. A valuation is called non-Archimedean if $|x + y| \leq \max\{|x|, |y|\}$. It is called Archimedean if it is not non-Archimedean.

Def. (10.3.3.11) [Non-Archimedean field]. A non-Archimedean field is a topological field that the valuation is given by a rank1-valuation.

Prop. (10.3.3.12). A valuation is non-Archimedean iff $\{n|n \in \mathbb{N}\}$ is bounded.

**Proof:** If it is non-archimedean, then clearly by induction and $n = 1 + (n - 1)|n| \leq 1$. Conversely, if $|n| \leq M$, then consider $|x + y|^n = |(x + y)^n| \leq \sum |C_n^k| x^k y^n - k| \leq M \max\{|x|, |y|\}$, so letting $n$ be large, clearly $|x + y| \leq \max\{|x|, |y|\}$.

Cor. (10.3.3.13). Any valuation on a field of char $\neq 0$ is non-Archimedean.

Prop. (10.3.3.14) [Equivalent Valuations]. Two valuation on a field is equivalent iff $|x|_1 < 1 \Rightarrow |x|_2 < 1$ and is equivalent to $|x|_1 = |x|_2^s$ for some $s > 0$.

**Proof:** if two valuation are equivalent, then $x^n \rightarrow 0$ in $\tau_1$ iff $x^n \rightarrow 0$ in $\tau_2$, so $|x|_1 < 1 \Rightarrow |x|_2 < 1$.

If $|x|_1 < 1 \Rightarrow |x|_2 < 1$, then let $y$ be an element that $|y|_1 > 1$, then any element $|x| = |y|^\alpha$ for some $\alpha \in \mathbb{R}$. Let $\frac{\partial x}{\partial m}$ converges to $\alpha$ from above, then $|\frac{x^n}{y^m}|_1 < 1$, so $|\frac{x^n}{y^m}|_2 < 1$, so $|x|_2 \leq |y|_2^s$.

Similarly, $|x|_2 \geq |y|_2^s$, so $|x|_2 = |y|_2^s$. So $|x|_1 = |x|_2^s$ for some $s > 0$.

If $|x|_1 = |x|_2^s$ for some $s > 0$, then these two valuations are clearly equivalent.

Cor. (10.3.3.15) [Weak Approximation]. If $|\cdot|_1, \ldots, |\cdot|_n$ be pairwise inequivalent valuations on $K$, then for any $a_1, \ldots, a_n \in K$ and $\varepsilon > 0$, there is an $x \in K$ that $|x - a_i| < \varepsilon$.

**Proof:** As $|\cdot|_1, \ldots, |\cdot|_n$ are inequivalent, there are $\alpha, \beta$ that $|\alpha|_1 < 1, |\alpha|_n \geq 1, |\beta|_n < 1, |\beta|_1 \geq 1$ by (10.3.3.14), so let $y = \beta/\alpha$, then $|y|_1 > 1, |y|_n < 1$.

Now we prove by induction that there is an $\alpha$ that $|\alpha|_1 > 1, |\alpha|_i < 1$ for $i = 2, \ldots, n$. the case $n = 2$ is done, for general $n$, if the $z$ for $n - 1$ satisfies $|z|_n \leq 1$, then $z^m y$ will do, for $m$ large. if $|z| > 1$, then the sequence $|t_m|_i = |\frac{z^m}{1 + z^m}|_i$ converges to $1$ for $i = 1, n$ and converges to $0$ for $i = 2, \ldots, n - 1$, so $t^m y$ will do, for $m$ large.

Prop. (10.3.3.16) [Gelfand]. Any field $K$ with an Archimedean valuation is a subfield of $\mathbb{C}$.

**Proof:** We consider its completion. when it contains $\mathbb{C}$, this is a corollary of??, otherwise, we consider $K \otimes \mathbb{C}$, then it is a finite dimensional module over $K$ thus also complete.

Remark (10.3.3.17). Because of this, we usually don’t consider only non-Archimedean valuations, and refer to all valuations as places, cf.(12.2.4.5).

Prop. (10.3.3.18) [Ostrowski].

1. $\Sigma_0 = \mathbb{P} \cup \{\infty\}$. Thus any complete Archimedean field is isomorphic to $\mathbb{R}$ or $\mathbb{C}$ by (10.3.3.16).

2. Any non-trivial valuation on $\mathbb{F}_q(t)$ is of the form $\cdot |_p$ or $\cdot |_{\infty}$, where $p$ is an irreducible polynomial in $\mathbb{F}_q[t]$. 
Proof: 1: if it is non-Archimedean, then $|n| \leq 1$, and it is not trivial, so there is a minimal $p$ that $|p| < 1$. Then $p$ is easily seen to be a prime. Then for any $(a, p) = 1$, $a = dp + r$, so $|r| = 1$, so $|a| = 1$.

And if it is Archimedean, then we prove that in $\mathbb{N}, |m| = m^\lambda$ for some $\lambda$: Let $F(n) = |n|$ and $f = \log_2 F$, then $f(m + n) \leq \max\{f(m), f(n)\} + 1$, and if $m = \sum_{i=1}^r d_i n^i$, then $f(m) \leq r(1 + f(n)) + a_n$, where $a_n = \sup\{f(k)|k < n\}$. And $r \leq \log m / \log n$, so

$$\frac{f(m)}{\log m} \leq \frac{a + f(n)}{\log n} + \frac{b}{\log n}$$

then letting $m \to m^k, k \to \infty$, and then let $n \to n^k, k \to \infty$, we get $\frac{f(m)}{\log m} \leq \frac{f(n)}{\log n}$, for any $m, n$.

2: Any valuation on $\mathbb{F}_q(t)$ is non-Archimedean(10.3.3.13), and $|n| = 1$ if $(n, p) = 1$, because $n^{p-1} = 1$. Similarly, if there is a minimal hence irreducible $P$ that $|P| < 1$, then use induction and $Q = sP + r$ for some $s, r$ of degree $< \deg Q$, so $|Q| = 1$ for all $(Q, P) = 1$. Otherwise, $|P| \leq 1$ for all $P$, then $|t| > 1$, otherwise $|\cdot|$ is trivial, so it is easy by induction that $|F(t)| = |t|^\deg F$.  

Lemma(10.3.3.19) [Continuity of Roots]. For a separable polynomial $f$ over a valued alg.closed field $\overline{K}$, there is a $\varepsilon$ that every polynomial $g$ that are closed enough to $f$, the roots of $g$ is closed to roots of $f$ respectively.

Proof: This is easy to see by decomposition as each root of $f$ is close to a root of $g$. $f, g$ have the same degree so the roots correspond to each other. 

Prop. (10.3.3.20) [Fundamental Inequality], if $(K, v)$ is a valued field and $L/K$ be a field extension of degree $n$, if $w_i$ are the valuations of $L$ above $v$, then

$$\sum_{w_i|v} e(w_i/v)f(w_i/v) \leq [L : K].$$

The equality holds when $v$ is discrete and $L/K$ is separable.

Proof: Cf.[Clark note Theorem4].? 

Def. (10.3.3.21) [Spherically Complete Valued Field]. A valued field $K$ is called spherically complete iff each descending chain of metric balls has a nonempty intersection.

Microbial Valuations

Prop. (10.3.3.22) [Microbial Valuation]. For a valuation ring $R \subset K$, a $f \neq 0 \in R$ is called topologically nilpotent iff $f^n \to 0$ in the valuation topology of $A$. The following are equivalent:

- The topology on $\overline{K}$ coincides with a rank 1 topology.
- There exists a nonzero topologically nilpotent element in $K$.
- $R$ has a prime ideal of height 1.

If this is the case, then the valuation defined by $A$ is called microbial.

And in this case, for any topological nilpotent element $\varpi$, $K = R[\varpi^{-1}]$, and $\varpi^r \in R$ for some $r$, and the topology on $R$ is $\varpi^r$-adic. And if $p$ is a prime ideal of rank 1, then the valuation ring $R_p$ is of rank 1, and defines the same topology on $R$. 
**Proof:** $1 \to 2$: if there is a rank 1 valuation $|\cdot|$ that defines the same topology as $R$, then any $|x| < 1$ will be a topological nilpotent element by (10.3.3.23).

$2 \to 3$: if $\varpi$ is a topological nilpotent element, then $p = \sqrt{\langle \varpi \rangle}$ is a prime ideal, and it is minimal, because if there is another $q \subseteq p$, then $\varpi \notin q$, but $p \subset (\varpi^n)$ by induction: because $(\varpi) \not\subseteq q$, $q \subset (\varpi)$, and if $x \in q$, then $x = \varpi^ny$, and $\varpi \notin q$, so $y \in q \subset (\varpi^n)$, so $x \in (\varpi^{n+1})$. Now $q = 0$ because $\varpi$ is topological nilpotent.

$3 \to 1$: It suffices to prove that the valuation defined by $R_p$ is the same as the topology of $R$. But this is true in general, just notice that the valuation topology of a nontrivial valuation is also defined by $B(a, \gamma)$.

The final remark is clear as $x\varpi^n \in R \iff |\varpi^n| \leq |x^{-1}|$.

**Lemma (10.3.3.23).** Let $R$ be a valuation ring, if $x \in R^*$ is topologically nilpotent, then $|x| < 1$, and the converse is also true if $R$ has rank 1.

**Proof:** if $|x| \geq 1$, then $x^n \not\in B(0,1)$, so it is not topologically nilpotent. And if $R$ has rank 1, $|x| < 1$, then for any $\delta \neq 0$, there is some $n$ that $|\delta^{-1}| < |x^{-n}|(2.2.8.5)$, so $|x^m| < |\delta|$ for $m$ large, thus $x$ is topologically nilpotent.

**Prop. (10.3.3.24) [Constructing Microbial Valuations].** If $A$ is a valuation ring and $f \notin A$ is a non-zero non-unit, then the $f$-adic Hausdorffization $\overline{A} = A/\cap_n f^nA$ and the completion $\overline{A}$ are all microbial.

**Proof:** Easy, Cf.[Bhatt Perfectoid Spaces, P63].

## 4 Affinoid Algebras

### Tate Algebras

**Def. (10.3.4.1) [Tate Algebra].** For a complete non-Archimedean field $K$ with residue field $k$, we define the **Tate algebra** $T_n = K(x_1, \ldots, x_n)$ to be the restricted power series (10.3.1.7) consists of elements $\sum a_vx_v^n$ that $\lim_{|v| \to \infty} |a_v| = 0$. It is endowed with the norm $|f| = \max |a_v|$.

The norm satisfies $|fg| = |f||g|$ and $|f + g| \leq |f| + |g|$.

There is a **reduction map** from $T_n$ to $k[x_1, \ldots, x_n]$, it is surjective.

**Proof:** $T_n$ is an algebra because the values of coefficients of $f$ is bounded. $|fg| \leq |f||g|$ is easy, to show $|fg| \geq |f||g|$, we assume $|f| = |g| = 1$, then their reduction in $K[x_1, \ldots, x_n]$ is non-zero, thus $\overline{fg}$ is non-zero, which shows $|fg| \geq 1$.

**Prop. (10.3.4.2) [Maximum Principle].** A formal power series $f$ converges in $B^n(\overline{K})$ iff it is in $T_n$.

And when it is in $T_n$, $|f(x)|$ attains a maximum $|f|$ in $B^n(\overline{K})$.

**Proof:** If it converges at $(1, \ldots, 1)$, then $\lim_{|v| \to \infty} |a_v| = 0$ by (12.1.1.20). Conversely, for any point in $B^n(\overline{K})$, it can be considered in a finite extension field of $K$, thus complete, hence we can apply (12.1.1.20) again.

For the second assertion, we assume $|f| = 1$, then consider its reduction to $k[x_1, \ldots, x_n]$, then there is a $\overline{x}$ in the alg.closure of $k$ that $\overline{f}(\overline{x}) \neq 0$. Now $\overline{k}$ can be seen as the residue field of $\overline{K}$. Then the lifting of $\overline{x}$ to a $x \in \overline{K}$ has valuation 1 and $|f(x)| = 1$.

**Prop. (10.3.4.3).** $T_n$ is a Banach algebra (Easy).
Cor. (10.3.4.4). An element \( f \) of norm 1 of \( T_n \) is invertible in \( T_n \) iff its reduction in \( k[x_1, \ldots, x_n] \) is a unit. Elements of other norms can be reduced to the case of norm 1.

Proof: One direction is trivial, the other is because \( |f - f(0)| < 1 \), hence \( f = f(0)(1 + g) \), this is invertible by power expansion as \( T_n \) is complete. \qed

Def. (10.3.4.5). A restricted power series \( g = \sum g_v X^n_{v} \in T_n \) with coefficients in \( T_{n-1} \) is called \( X_n \)-distinguished of order \( s \) iff \( g_s \) is a unit in \( T_{n-1} \), \( |g_s| = |g| \) and \( |g_v| > |g_v| \) for all \( v > s \).

Lemma (10.3.4.6). For any f.m. elements \( f_i \in T_n \), there is a continuous automorphism of \( T_n \) that maps \( T_n \to T_{n_i}, T_i \to T_i + T_{n_i}^a \) that maps \( f_i \) to \( X_n \)-distinguished elements.

Proof: Cf. [Rigid and Formal Geometry P16]. \qed

Prop. (10.3.4.7) [Weierstrass Division]. If \( g \in T_n \) is \( X_n \)-distinguished of order \( s \), for any \( f \in T_n \), there is a unique form \( f = qg + r \), where \( q \in T_n \) and \( r \in T_{n-1}[X_n] \) of degree \( r < s \). Moreover, \( |f| = \max\{|g||g|, |r|\} \).

Proof: Cf. [Rigid and Formal Geometry P17]. \qed

Cor. (10.3.4.8) [Weierstrass Preparation]. If \( g \in T_n \) is \( X_n \)-distinguished of order \( s \), then there exists uniquely a \( r \in T_{n-1}[X_n] \) of degree \( s \) and \( g = re \), where \( e \) is a unit in \( T_n \).

Proof: By (10.3.4.7) applied to \( X_n^s = qg + r \) with \( |r| \leq 1 \). Then \( \omega = X_n^s - r \) is \( X_n \) is the desired polynomial, it suffice to show \( q \) is a unit. Let \( g \) be normalized so \( |g| = 1 \), then \( |q| = 1 \), by reduction to polynomials, we see \( \tilde{\omega} = \tilde{qg} \), and \( \tilde{\omega}, \tilde{g} \) are both polynomials of degree \( s \), so \( \tilde{q} \in k^s \), so \( q \) is a unit by (10.3.4.4).

Uniqueness: if \( g = e\omega \), then \( X_n^s = e^{-1}g + (X_n^s - \omega) \), so uniqueness follows from that of Weierstrass division. \qed

Prop. (10.3.4.9) [Noether Normalization]. For any proper ideal \( \alpha \) of \( T_n \), there is a \( d \) and a finite injection \( T_d \to T_n/\alpha \).

Proof: We may assume \( \alpha \neq 0 \), thus choose a \( g \in \alpha \neq 0 \), then using (10.3.4.6), we may assume \( g \) is \( X_n \)-distinguished. Now the Weierstrass division theorem (10.3.4.7) says that \( T_{n-1} \to T_n/(g) \) is finite. Hense \( T_{n-1} \to T_n/(g) \to T_n/\alpha \) is finite. Now we can use induction to find a \( d \to T_{n-1}/T_{n-1} \cap \alpha \) finite, thus also \( T_d \to T_n/\alpha \) is finite. \qed

Cor. (10.3.4.10) [Residue Field of Tate Algebra]. The residue field of a maximal ideal of \( T_n \) is a finite extension field of \( K \), because \( T_n/\mathfrak{m} \) has dimension 0, thus \( K \to T_n/\mathfrak{m} \) finite injective.

Proof: Because finite injection \( T_d \to T_n/\mathfrak{m} \) shows \( T_n \) is a field (4.2.1.3), thus we must have \( d = 0 \). \qed

Cor. (10.3.4.11). The map from \( B^n(K) \) to the set of maximal ideals of \( T_n \) are surjective.

Proof: Evaluation map defines a map \( T_n \to K(x_1, \ldots, x_n) \) that is surjective, thus the kernel is a maximal ideal. Conversely, for any maximal ideal \( \mathfrak{m} \subset T_n \), \( K' = T_n/\mathfrak{m} \) is finite over \( K \), so we may assume \( K' \subset K \).

We show that this map \( \varphi : T_n \to K \) is contractive, otherwise there is a \( |\alpha| = 1, |\alpha = \varphi(\alpha)| > 1 \). Consider the minimal polynomial \( p \) of \( |\alpha| \), all the conjugates of \( \alpha \) has the same valuation as \( K \), as \( K \) is Henselian, thus \( p \) has ascending Newton polygon, thus by (10.3.4.4) it is invertible in \( T_n \). But \( \varphi(p(\alpha)) = 0 \), contradiction.

So \( |\varphi(x)| \leq |x| \), then it is continuous, and \( (\varphi(T_1), \ldots, \varphi(T_n)) \subset B^n(K^n) \), so we are done. \qed
**Cor. (10.3.4.12)** [Main Theorem]. $T_n$ is Noetherian, UFD, Jacobson of Krull dimension $n$.

**Proof:** Noetherian: Use induction, as in the proof of (10.3.4.9), $T_{n-1} \to T_n/(g)$ is finite for some $g \subseteq a$, then also $T_n/a$ is finite over $T_{n-1}$, thus Noetherian as a $T_{n-1}$ module, thus Noetherian as a ring.

UFD: Cf. [Rigid and Formal Geometry P20].

Jacobson: We need to show that any prime ideal $p$ is an intersection of maximal ideals. The case of $p$ is by (10.3.4.2). For $p \neq 0$, by Noetherian normalization (10.3.4.9), there is a $T_d \subset T_n/p$ finite. Then use induction and generalized Nullstellensatz (4.2.6.10), $T_n/p$ is Jacobson, thus $p = \text{rad}(T_n/p)$.

Dimension $n$: Cf. [Formal and Rigid Geometry P22].

**Prop. (10.3.4.13).** For an ideal $a \subseteq T_n$, there are $a_1, \ldots, a_r$ which generate $a$ that $|a_i| = 1$, and any elements in $f$ has a representation of the form $\sum f_i a_i$ with $|f_i| \leq |f|$.

The same assertion holds for submodules of $T_n^k$.

**Proof:** Cf. [Formal and Rigid Geometry P27,29].

**Cor. (10.3.4.14).** Each ideal of $T_n$ is closed hence complete in $T_n$. This follows immediately from (10.3.4.12) and (12.1.2.12).

**Cor. (10.3.4.15).** For any ideal $a$ of $T_n$, the distance from an element to $a$ attains minimum.

**Proof:** Cf. [Bos15] P28.

### Affinoid Algebras

**Def. (10.3.4.16)** [Affinoid Tate Algebra]. A normed algebras of the form $A = T_n/a$ are called **affinoid (Tate) algebras**, so it is Noetherian and Jacobson by (10.3.4.12). An affinoid algebra has a natural semi-norm by $|f|_\text{sup} = \sup |f|_m$ in $A/m$ for a maximal ideal $m$ of $A$ by (10.3.4.10).

**Proof:** We need to show the sup is finite, for this, notice $|f| = |g|$ for some $g$ in the residue norm (10.3.4.17), so for any maximal ideal $m$ of $A$, the inverse is a maximal ideal $n$ in $T_n$ by finiteness, thus $|f|_m = |g|_m \leq |g|_\text{sup} = |g| = |f|$, so $|f|_\text{sup} \leq |f|$.

For the second-last equality, notice on $T_n$, $|\cdot|_\text{sup}$ and $|\cdot|$ equal, by (10.3.4.2) and (10.3.4.11).

**Def. (10.3.4.17)** [Residue Norm]. For a Tate algebra $A = T_n/a$, there is a natural residue norm on it. This is a complete $K$-algebra norm on $A$, and $T_n \to A$ is continuous and open. For any $f \in A$, the residue norm is attained at an element of $T_n$.

Any residue norm is bigger than the sup-norm, by the proof of (10.3.4.16).

**Proof:** It is a $K$-algebra norm is easily verified, should notice $|f| = 0$ iff $f = 0$, because $a$ is closed (10.3.4.14). The last assertion follows from (10.3.4.15).

**Remark (10.3.4.18).** The sup norm may not even be a norm, if $a$ is not radical, but the fact that sup norm is smaller than any residue norm, together with (10.3.4.22), is enough for use.

**Prop. (10.3.4.19).** For $T_d \to A$ a finite injection, assume $A$ is a torsion-free $T_d$-module, then for any $f \in A$, there is a unique minimal monic polynomial $P$ of $f$ over $T_d$.

In this case, $|f|_\text{sup} = \sup |a_i|_\text{sup}$ where $a_i$ are coefficients of $P$. 
Proof: Because $A$ is torsion-free, we reduce to the quotient field of $T_n$, then $f$ has a minimal monic polynomial, and $T_n$ is UFD, hence Gauss lemma shows that this polynomial has coefficients in $T_d$. Hence $T_n[f] = T_n[X]/(p)$.

For the second, notice first for finite extension the Spec map is surjective, thus we may assume $A = T_n[f] = T_n[X]/(p)$, and for a maximal ideal $\mathfrak{m}$ of $T_n$, let $T_n/\mathfrak{m} = k$, then $A/(\mathfrak{m}) = k[X]/(\mathfrak{p})$, then maximal ideals of $A/(\mathfrak{m})$ corresponds to roots $\alpha_i$ of $\mathfrak{p}$ in $\overline{k}$, so

$$\sup_{\varphi^{-1}(\mathfrak{m})} |f|_{\mathfrak{m}} = \sup |\alpha_i| = \max |\alpha_i|_{\mathfrak{m}}^{1/i},$$

so the result follows. □

Cor. (10.3.4.20). $|f|_{\sup} \in \sqrt[n]{K}$ for some $N$ and all $f \in A$, because the minimal polynomial has coefficients in $T_n$, and sup norm and Gauss norm coincide on $T_n$ by the proof of (10.3.4.16).

Cor. (10.3.4.21) [Maximum Principle]. $|f|_{\sup} = |f|_{\mathfrak{m}}$ for some maximal ideal $\mathfrak{m}$.

Proof: Since $A$ is Noetherian (10.3.4.12), it has f.m. minimal primes, hence $|f|_{\sup} = |f|_{\sup}$ in $A/p_i$ for some minimal prime of $A$. Hence we reduce to the case of (10.3.4.19), hence the conclusion follows from (10.3.4.2) and the proof of (10.3.4.19). □

Prop. (10.3.4.22) [Residue Norms Equivalent]. Any morphism from a Noetherian $k$-algebra to an affinoid algebras $A$ is continuous w.r.t any residue norms. In particular, any $k$-Banach algebra topology on $A$ coincides with the $k$-affinoid topology on $A$, and all residue norms on an affinoid algebra are equivalent.

Moreover, for any morphism of $k$-affinoid algebras $B \rightarrow A$, the norm on $A$ can be replaced by an equivalent one that makes $A$ into a normed $B$-algebra.

Proof: Use (12.1.2.9), it suffices to show the condition holds, for $\mathcal{B} = \{\mathfrak{m}^n\}$ where $\mathfrak{m}$ are maximal ideals of $A$: The residue field is finite by (10.3.4.10), their intersections is (0) because if $f \in \cap_{\mathfrak{m}} \cap_{n} \mathfrak{m}^n$, Krull’s theorem (4.2.2.15) (use localization) says for each maximal ideal $\mathfrak{m}$ there is a $m \in \mathfrak{m}$ that $(1 - m)f = 0$, so $Ann(f) = (1)$, so $f = 0$.

For the second assertion, see [non-Archimedean Analysis P229]. □

Cor. (10.3.4.23). The notion of powerboundedness and topological nilpotence is independent of residue norm chosen.

Cor. (10.3.4.24) [Restricted Power Series]. For an affinoid algebra $A$, the restricted power series in $A$:

$$A\langle X_i \rangle = \{ \sum a_v X^v | \lim_{|v| \to \infty} a_v = 0 \}$$

is an affinoid algebra, this is independent of the residue norm chosen.

Def. (10.3.4.25) [Strongly Noetherian]. $A$ is called strongly Noetherian if $A(T_1, \ldots, T_n)$ are Noetherian for any $n \geq 0$.

Lemma (10.3.4.26). The image $A$ is dense in $A(X)/(X - f)$ (in the residue norm, and thus in all other norms, by (10.3.4.22)(10.3.4.17)), this is because a restricted power series can be truncated by a finite part and a part with small norm, and the finite part is in the image of $A.$
Def. (10.3.4.27) [Affinoid Generator]. For a morphism of affinoid algebras $A \to A'$, a set of elements $h_i$ in $A'$ is called a set of affinoid generator iff there is a surjection

$$A(X_1, \ldots, X_n) \to A', \quad X_i \mapsto h_i$$

Of course $h_i$ is power-bounded, by the residue norm given.

Lemma (10.3.4.28). If $\pi' : A(X_1, \ldots, X_n) \to A' : X_i \to h_i'$ is a surjective morphism of affinoid algebras that $A(X_1, \ldots, X_n)$ is endowed with the Gauss norm and $A'$ is endowed with the residue norm, then any set of elements $h = (h_1, \ldots, h_n)$ that $|h_i - h_i'| < 1$ is a set of affinoid generators.

Proof: By non-Archimedean property, $|h_i| \leq 1$ thus also $|h_i'| \leq 1$, and Let $\varepsilon = \max\{|h_i| - |h_i'| \} < 1$. The strategy is simple, if for each $g$ in $A'$, there is a $f$ that $|f| = |g|, |\pi(f) - g| \leq \varepsilon |g|$, then by iteration, there is a $f$ that $\pi(f) = g$. But by (10.3.4.17) and (10.3.4.15), if we choose a $f$ that $\pi'(f) = g$ and $|f| = |g|$, then

$$|\pi(f) - g| = |\sum a_v h^v - \sum a_v h'^v| = |\sum a_v (h^v - h'^v)| \leq \varepsilon |f| = \varepsilon |g|.$$

Def. (10.3.4.29) [Distinguished Element]. For an affinoid algebra $A$ and an element $x \in \text{Sp} A(14.5.1.1)$, a element $f \in A(X_1, \ldots, X_n)$ is called $X_n$-distinguished of order $s$ at $x$ iff it is distinguished in $A/\mathfrak{m}_x(X_1, \ldots, X_n)$ is distinguished of order $s$ in the sense of (10.3.4.5) (notice $A/\mathfrak{m}_x$ is a complete valued field by (10.3.4.10)).

Prop. (10.3.4.30) [Fibererd-Pushouts]. When $R, A_1, A_2$ are all affinoid algebras, the amalgamated sum is also an affinoid algebra. In other words, the category of affinoid algebras admits amalgamated sums (fibered pushouts by (12.1.1.15)).

Proof: Cf. [Formal and Rigid Geometry P245].

Prop. (10.3.4.31). $T_n \otimes T_m \cong T_{m+n}, \ K^n \otimes T_{n,K} = T_{n,K'}$.

Prop. (10.3.4.32). For affinoid algebras $R, A_1, A_2$ and ideals $a_1 \subset A_1, a_2 \subset A_2$, there is an isomorphism:

$$(A_1 \otimes_R A_2)/(a_1, a_2) \cong (A_1/a_1) \otimes_R (A_2/a_2)$$

Proof: Cf. [Rigid and Formal Geometry P248].

Prop. (10.3.4.33) [Finite Extension of Affinoid Algebras]. If $B$ is an affinoid $K$-algebra and $\varphi : B \to A$ is a finite ring map, then $A$ can be provided a topology to make it an affinoid $K$-algebra, and $\varphi$ is continuous.

Proof: We can associate to $A$ a Banach algebra topology induced from $B^n \to A \to 0$ that is continuous. Now it is an affinoid $K$-algebra: we may assume $A = T_n$, then $A = \sum T_n a_i$, and we may assume $|a_i| < 1$ then clearly there is a continuous extension $T_n(X_i) \to A$ extending this map, so $A$ is affinoid.

Construction of Affinoid Tate Algebras

Def. (10.3.4.34) [Affinoid Localizations]. Let $A$ be an affinoid Tate algebra, then for a finite set of elements $\{f_i, g_j\} \subset A$, we can define the localization

$$A(f_i, g_j^{-1}) = A(\zeta_1, \ldots, \zeta_i, \xi_i^{-1}, \ldots, \xi_j)/(\zeta_i - f_i, 1 - \xi_j g_j).$$
5 Huber Rings

Def.(10.3.5.1) [Huber Ring]. A topological ring is called Huber if there exists an open subring $A_0$ that the induced topology on $A_0$ is $I$-adic for some f.g. ideal $I$ of $A$. Such a $A_0$ is called a ring of definition, and $I$ is called the ideal of definition. Morphisms of Huber rings are just a continuous morphisms of topological rings.

Prop.(10.3.5.2) [Boundedness and Rings of Definition]. A subring $A_0 \subset A$ of a Huber ring is a ring of definition iff it is open and bounded.

Proof: Clearly a ring of definition is open and bounded, for the converse, let $(A'_0, I)$ be a couple of definition, and $A_0$ is an open and bounded subset of $A$, then $I^k \subset A_0$ for some $n$, and set $J = I^k A_0$. As $A_0$ is bounded, for any open nbhd $U$ of 0, there exists $m > 0$ that $I^{km} A_0 \subset U$, thus $J^m \subset U$. This shows $J$ is a fundamental system of nbhd of 0, thus $A_0$ is $J$-adic and is a ring of definition.

Cor.(10.3.5.3). Let $A$ be a Huber ring, then

- If $A_0, A_1$ are two rings of definition of $A$, then so does $A_0 \cap A_1$ and $A_0 A_1$.
- Every open subring $B$ of $A$ is a Huber ring.
- If $B \subset C$ are subrings of $A$ and $B$ is bounded, $C$ is open, then there is a ring of definition $A_0$ that $B \subset A_0 \subset C$.

Proof: 1: By(10.3.5.2).
2: Let $I^n \subset B$, then $(B \cap A_0, I^n)$ is a couple of definition of $B$.
3: By2, $C$ is Huber, take a ring of definition $A_0$ of $C$, then $A_0 B$ is open and bounded in $C$, thus a ring of definition.

Lemma(10.3.5.4). If $A$ is a Huber ring and $T \subset A$ is a subset that generates an open ideal of $A$, then for any open nbhd $U$ of $A$, the subgroup $T^n U$ is open.

Proof: Let $(A_0, I)$ be a couple of definition. By assumption the ideal $J$ generated by $T$ is open, thus $J^n$ is also open, and contains some $I^m$. Now we can change $I^m$ to $I$. Now $I$ is f.g., so there is a finite subset $M \subset A$ that $I \subset T^n M$. Notice $M$ is bounded because it is finite, so there is an integer $r$ that $r M \subset U$, thus $r^n U \subset T^n U$, and $T^n U$ is open.

Def.(10.3.5.5) [Tate Huber Ring]. A Tate Huber ring is a Huber ring s.t. there exists an open subring $A_0$ that the induced topology on $A_0$ is $t$-adic for some $t \in A_0$ which becomes a unit in $A$. Such a $t$ is called a pseudo uniformizer.

Prop.(10.3.5.6) [Examples of Tate Huber Rings].
- If $K$ is a complete non-Archimedean field and $R$ is a $K$-Banach algebra, then $R$ is Tate with a ring of definition by $(R_{< 1}, t)$, where $t$ is a pseudo-uniformizer of $K$.
- If $A_0$ is any ring and $g \in A_0$ is a non-zero-divisor, and let $A = A_0[g^{-1}]$ equipped with the $g$-adic topology, then it is an Tate Huber ring.

Prop.(10.3.5.7) [Properties of Tate Huber Rings]. If a Huber ring $A$ is Tate with a topological nilpotent unit $g$ and $A_0 \subset A$ is any ring of definition, then there exists $n$ large that $g^n \subset A_0$. And in this case, $A_0$ is $g^n$-adic and $A = A_0[(g^n)^{-1}]$.

In this case, a subset $S \subset A$ is bounded iff $S \subset g^{-n} A_0$ for some $n$. 
Prop. (10.3.5.8) [Power-Bounded Elements and Topologically Nilpotent Elements]. The subset \( A^0 \) of power-bounded elements in \( A \) is a subring, and it is the filtered colimit of all the ring of definition in \( A \), thus open. It is also integrally closed in \( A \).

The subset \( A^{00} \) fo topologically nilpotent elements of \( A \) is a radical ideal of \( A^0 \). But it is in general not an ideal of \( A \).

Recall \( A \) is called uniform if \( A^0 \) is bounded (12.1.1.6), or equivalently \( A^0 \) is a ring of definition, by (10.3.5.2).

Proof: By (10.3.5.3), every power-bounded element is contained in a ring of definition, and any ring of definition is bounded, so \( A^0 \) is the union of all rings of definitions of \( A \), and this is filtered by (10.3.5.3).

To show \( A^0 \) is integrally closed, notice by what we already proved, if \( a \) is integral over \( A^0 \), then it is integral over a ring of definition \( A_0 \), but then \( \{a^n\} \subset A_0[a] \) is bounded, so \( a \in A^0 \).

Showing \( A^{00} \) is a radical ideal of \( A^0 \) is easy and omitted.

\[ \square \]

Cor. (10.3.5.9). If a Huber ring \( A \) is separated, Tate and uniform, then \( A \) is reduced.

Proof: Assume that \( A_0 \) the set of power-bounded elements is a ring of ideal and \( g \in A_0 \) is a pseudo-uniformizer. If \( x \) is nilpotent, then \( g^n x \) is nilpotent for any \( x \), so power-bounded and \( g^{-n} x \in A_0 \), which means \( x \in g^n A_0 \) for any \( n \). But \( A_0 \) is separated, so \( x = 0 \).

\[ \square \]

Cor. (10.3.5.10). Let \( A \) be a Huber ring, then an ideal \( J \) is open iff \( A^{00} \in \sqrt{J} \).

Proof: If \( J \) is open, then clearly \( A^{00} \subset \sqrt{J} \). Conversely, if \( A^{00} \subset \sqrt{J} \) and \( (A_0, I) \) is a couple of definition, then \( I \subset A^{00} \) by (10.3.1.9), so \( I \subset \sqrt{J} \). And \( I \) is f.g., so \( I^n \subset J \) for some \( J \), thus \( J \) is open.

\[ \square \]

Prop. (10.3.5.11). If \( K \) is a complete non-Archimedean field, then any Banach \( K \)-algebra \( R \) is a complete Tate ring, and if \( K, R \) are perfectoids, then \( R^{00} = K^{00} R^0 \).

Proof: In the perfectoid case, first \( K^{00} R^0 \subset R^{00} \), and for any topological nilpotent \( \alpha, \alpha^n \subset t R^{00} \) for a pseudo-uniformizer \( t \). Thus \( R^{00} \) and \( K^{00} R^0 \) has the same radical, it suffices to show \( K^{00} R^0 \) is radical, but the quotient \( R^0/K^{00} R^{00} \) is a perfect \( K^0/K^{00} \)-algebra by perfectoidness, thus it must be radical.

\[ \square \]

Prop. (10.3.5.12) [Complete Perfect Tate ring is Uniform, André]. If \( A \) is a complete Tate ring of charp that is perfect, then \( A \) is uniform.

Proof: Let \( (A_0, t) \) be a ring of definition, let \( A_n = A_0^{1/t^n} \), then \( A_\infty = \text{colim} A_n = (A_0)_{\text{perf}} \). We check \( t^{1/t^n} A_0 \subset A_\infty \subset t^{-1} A_0 \), which shows \( A^0 \) is bounded.

If \( f \in A^0 \), then \( t^a f^N \subset A \subset A_\infty \), and \( A_\infty \) is perfect, so \( t^{1/t^n} f \in A_\infty \) for all \( n \). Notice the Frobenius is a continuous bijection of Banach spaces, so it is open by Banach theorem (10.6.2.4), so \( A^0 \supset t^{mp} A_0 \), thus \( t^m A_1 \subset A_0 \), and then \( t^{1/t^n} A_{n+1} \subset A_n \). So \( t^{1/t^n} A_{\infty} \subset A_1 \). So \( t^c A_\infty \subset A_0 \), for \( c \) large.

\[ \square \]
Huber Pairs

Def. (10.3.5.13) [Huber Pairs]. For a Tate ring $A$, a ring of integral elements is an open and integrally closed subring of $A$ contained in $A^0$ (10.3.5.8) (for example $A^0$ itself). A Huber pair is a pair $(A, A^+)$ that $A$ is a Huber ring and $A^+$ is a ring of integral elements. A morphism of Huber pairs should preserve the ring of integers.

A Huber ring is called an Affinoid Tate ring if $A$ is Tate.

Prop. (10.3.5.14). $A^00 \subset A^+$ as an ideal for any ring of integral elements $A^+$. In particular, $A^+$ contains any pseudo-uniformizer, and the set of rings of integral elements is in bijection with integrally closed subrings of $A/A^00$.

Also, $A^+$ is a filtered colimits of rings of definitions.

Proof: $t \in A^00$ is topologically nilpotent hence $t^n \subset A^+$ for some $n$ as it is open, and then $t \in A^+$ as it is integrally closed. It is an ideal because it is an ideal of $A_0$ (10.3.5.8).

For the last assertion, notice that $A^0$ is the filtered colimits of rings of definitions (10.3.5.8), and the intersection of a ring of definition with $A^+$ is also a ring of definition, because it is open and bounded (10.3.5.2), the result follows.

Def. (10.3.5.15) [Zariski, Henselian, Complete Huber Pairs]. A Huber ring $(A, A^+)$ is called
- complete iff $A$ is complete.
- Henselian iff $(A^+, A^00)$ is a Henselian pair.
- Zariski iff $(A^+, A^00)$ is a Zariski pair.

Prop. (10.3.5.16). An affinoid Tate ring $(A, A^+)$ with a ring of definition $(A_0, I)$ that $A_0 \subset A^+$ is
- Zariski iff $I$ is in the Jacobson radical of $A_0$.
- Henselian iff the pair $(A_0, I)$ is Henselian.
- Complete then it is Henselian.
- Henselian then it is Zariski.

Proof: 1: We prove that if $t \in \text{rad}(A_0)$, the for any other $B_0 \supset A_0$, $t \in \text{rad}(B_0)$. If this is true, then as $A^+$ is a filtered colimits of rings of definitions (because $A^0$ does), it is clear that $t$ lies in the maximal ideal (check $1 + at$ is unit). For this, if $m \subset B_0$ is maximal and $t \notin m$, choose $n$ that $t^n B_0 \subset A_0$, and an element $b \in B_0$ that maps to $t^{-n-1}$ modulo $m$, then $a = t^n b \in A_0$ is mapped to $t^{-1}$. Thus the composition $A_0 \to B_0 \to B_0/m$ is surjective: $\overline{b}$ is the image of $a^n(t^n b) \in A$. So $t$ is not in a maximal ideal of $A_0$, contradiction.

Conversely, Cf.[Bhatt Perfectoid Space P57].

2: Cf.[Bhatt Perfectoid Spaces P57].

3: $A$ is complete then $A_0$ is complete, hence $(A_0, I)$ is Henselian by (4.3.10.6), so it is Henselian by item2. 4: Trivial.

Adic Morphisms

Def. (10.3.5.17) [Adic Morphisms]. A morphism of Huber rings $f : A \to B$ is called an adic morphism if we can choose rings of definitions $A_0, B_0$ and an ideal of definition $I$ of $A$ that $f(A_0) \subset B_0$, and $f(I)B_0$ is an ideal of definition of $B_0$.

A morphism $(A, A^+) \to (B, B^+)$ of Huber pairs is called adic if $A \to B$ is.
Prop. (10.3.5.18). Let $f : A \rightarrow B$ be an adic morphism between Huber rings, then:

1. $f$ is continuous and open.

2. If $A_0, B_0$ are rings of definition s.t. $f(A_0) \subset B_0$, then for any ideal of definition $I \subset A_0$, $f(I)B_0$ is an ideal of definition in $B_0$.

3. $f$ maps bounded sets to bounded sets.

Proof: Let $f(A_0) \subset B_0$ and $J = f(I)B_0$. Then $I^n \subset f^{-1}(J^n)$, so $f$ is continuous.

If $E$ is bounded in $A$, for any $n$, let $m$ be that $I^mE \subset I^n$, then $f(E)f(I)^m = f(EI^m) \subset f(I^n) \subset J^n$, thus $f(E)J^m \subset J^n$, so $f(E)$ is bounded.

Construction of Huber Rings

Main references are [Mor19].

Prop. (10.3.5.19) [Quotient]. Let $(A, A^+)$ be a Huber ring and $a$ be an ideal of $A$, then the quotient pair $(A/a, (A/a)^+)$ where $A/a$ is the integral closure of $A^+/a$ in $A/a$.

Prop. (10.3.5.20) [Completion of Huber Rings]. Let $A$ be a Huber ring and $(A_0, I)$ be a couple of definition. Set $\hat{A} = \lim_{\leftarrow n} A/I^n$ (as an Abelian group), then:

1. The canonical map $\hat{A}_0 \rightarrow \hat{A}$ is injective and $\hat{A}_0 \cap A = A_0$.

2. If we put the unique topology on $\hat{A}$ that $\hat{A}_0$ is an open subgroup, then $\hat{A}$ is complete.

3. There is a unique topological ring structure on $\hat{A}$ that $A \rightarrow \hat{A}$ is continuous.

4. $\hat{A}$ is Huber with a couple of definition $(\hat{A}_0, I\hat{A}_0)$, and the canonical map $A \rightarrow \hat{A}$ is adic.

5. $\hat{A}_0 \otimes A_0 A \rightarrow \hat{A}$ is an isomorphism.

Proof: Cf. [Mor19] P72.

Prop. (10.3.5.21). Let $A$ be a Huber ring and $i : A \rightarrow \hat{A}$ be the completion, then under the bijection of (10.3.1.6),

- $\hat{A}^0 = \hat{A}_0, \hat{A}^{00} = \hat{A}_{00}$.
- $G \subset A$ is a ring of definition iff $\hat{G} \subset \hat{A}$ is a ring of definition.
- The map $\text{Cont}(\hat{A}) \rightarrow \text{Cont}(A)$ is a bijection.

Proof: Cf [Mor19] P75.

Prop. (10.3.5.22). Let $A$ be a Huber ring, then under the bijection of (10.3.1.6), an open ring $A_0$ is a ring of integral elements of $A$ iff $A_0^\wedge$ is a ring of integral elements of $A^\wedge$.

Proof: It is easy to show $A_0^\wedge$ is a ring iff $A_0^\wedge$ is a ring, and by (10.3.5.21), $A_0 \subset A^0$ iff $A_0^\wedge \subset (A^\wedge)^0$.

It suffices to prove that if $A_0$ is open and integrally closed, then $A_0^\wedge$ is integrally closed in $A^\wedge$.

Let $x \in A^\wedge$ satisfy $x^d + a_{d-1}x^{d-1} + \ldots + a_0 = 0$, where $a_i \in A_0^\wedge$, because $A_0^\wedge$ is open, we can find $x' \in A$ and $a'_i \in A_0$ that $(x')^d + a'_{d-1}(x')^{d-1} + \ldots + a'_0 \in A'_0$, but then $x' \in A_0$ because $A_0$ is integrally closed, and thus $x = (x' - x') + x' \in A_0^\wedge$.

Cor. (10.3.5.23) [Completion of Huber Pairs]. The forgetful functor from the category of complete Huber pairs to the category of Huber pairs has a left adjoint called completion, where $(A, A^+)^\wedge = (A^\wedge, (A^\wedge)^+)$, where $(A^\wedge)^+$ is the closure of the image of $A^\wedge$ in $A^\wedge$. 
Prop. (10.3.5.24) [Completion, Henselization, Zariski Localization]. There are left adjoint to the forgetful functors from the category of complete/Henselian/Zariski pairs to the category of pairs, called the completion/Henselization/Zariski localization of pairs. And there are natural maps

\[(A, A^+) \to (A, A^+)_{\text{Zar}} \to (A, A^+)_{\text{Hens}} \to (\hat{A}, \hat{A}^+)\]

Proof: □

Prop. (10.3.5.25) [Tensor Products of Adic Maps of Huber Rings].

- If \((A, A^+) \to (B, B^+)\) is adic, then pullback along the associated map of topological spaces \(\text{Spa}(B, B^+) \to \text{Spa}(A, A^+)\) preserves rational subsets.

- Let \((B, B^+) \leftarrow (A, A^+) \to (C, C^+)\) be a diagram of Huber pairs where both morphisms are adic. Let \(A_0, B_0, C_0\) be rings of definition compatible with the morphisms, and \(I \subset A_0\) be an ideal of definition. Let \(D = B \otimes_A C\) and let \(D_0\) be the image of \(B_0 \times_{A_0} C_0\) in \(D\). Make \(D\) into a Huber ring by declaring \(D_0\) to be a ring of definition with \(ID_0\) as its ideal of definition and \(D^+\) be the integral closure of the image of \(B^+ \otimes_A C^+\) in \(D\). Then \((D, D^+)\) is a Huber pair, and it is the pushout of the diagram in the category of Huber pairs.

Proof: For 1, it suffices to show that if \(T\) is a finite set of \(A\) that \(TA\) is open, then \(TB\) is open in \(B\): \(I \subset TA\) for some ideal of definition \(I \subset A_0\), in which case \(IB_0 \subset B_0\) is also an ideal of definition by (10.3.5.18), thus open, and so \(TB\) is also open as \(IB \subset TB\).

2 just follows from the definition. □

Remark (10.3.5.26) [Non-Adic Morphisms]. Pushouts may not exists for non-adic morphisms of Huber rings. For example, \(\mathbb{Z}_p \to \mathbb{Z}_p[[T]]\) is not adic (10.3.5.18), and the diagram

\[\{(\mathbb{Z}_p[[T]], \mathbb{Z}_p[[T]]) \leftarrow (\mathbb{Z}_p, \mathbb{Z}_p) \to (\mathbb{Q}_p, \mathbb{Z}_p)\}\]

has no pushout in the category of Huber pairs: If there is a pushout \((D, D^+)\), then we will have a morphism

\[(D, D^+) \to (\mathbb{Q}_p\langle T, T^n/p \rangle, \mathbb{Z}_p\langle T, T^n/p \rangle)\]

for each \(n \geq 1\). But notice that \(T\) is nilpotent in \(D\), and \(1/p \in D < T^n/p \to 0 \in D\) as \(n \to \infty\). So \(T^n/p \in D^+\) for some \(n\), but then \(T^n/p \in \mathbb{Z}_p\langle T, T^{n+1}/p \rangle\), which is impossible.

Def. (10.3.5.27) [Topological Polynomial Functions]. Let \(A\) be a non-Archimedean topological ring, and \(\{X_i\}_{i \in I}\) be a family of indeterminates, \(\{T_i\}_{i \in I}\) be a family of subsets of \(A\) that satisfies \(T_i^n U\) is open for any \(n > 0, i\) and open nbhd \(U\) of \(A\).

Let \(N(I)\) be the set of functions \(I \to \mathbb{N}\) with finite support, then for any \(\nu \in N(I)\), let \(T^\nu = \prod T_i^\nu(i)\). For any nbhd \(U\) of \(A\), we set

\[U|_{[X,T]} = \{ \sum_{\nu \in N(I)} a_\nu X^\nu | a_\nu \in T^\nu U \},\]

Then there exists a unique topological structure on \(A[X]\) that \(U|_{[X,T]}\) form a fundamental system of nbhds of 0, and denote it by \(A[X]_T\). It satisfies:

- the canonical inclusion \(\iota : A \to A[X]_T\) is continuous and the set \(\{T_i X_i\}_{i \in I}\) is power-bounded.
• \( \iota \) satisfies the universal property that any continuous map \( f : A \to B \) to another non-Archimedean topological ring \( B \) that \( \{ f(T_i)X_i \}_{i \in I} \) is power-bounded factors through \( A[X]_T \).

**Proof:** Just notice that \( (U \cap V)[X,T] \subset U[X,T] \cap V[X,T] \) and \( U[X,T] \cdot V[X,T] = (UV)[X,T] \), so they form a topological basis because \( A \) is topological.

The first properties are easily verified. For the second, the extension \( f' : A[X] \to B \) exists abstractly, and it suffices to show it is continuous. If we let \( E \subset B \) be the subring generated by \( \{ f(T_i)X_i \}_{i \in I} \), then \( E \) is bounded, so for any open subgroup \( H \subset B \), there is some open subgroup \( G \subset B \) that \( EG \subset H \), and thus \( f^{-1}(G) \) is open and contains some nbhd \( U \), then \( U[X,T] \subset (f')^{-1}(G) \), so \( f' \) is continuous.

**Def. (10.3.5.28) [Topological Power Series].** Let \( A, X, T \) as in (10.3.5.27), then the set

\[
A(X)_T = \left\{ \sum_{\nu \in \mathbb{N}(I)} a_{\nu} X^\nu \in A[[X]] | a_{\nu} \in T^\nu U \ a.e. \right\},
\]

is a subring of \( A[[X]] \), and there is a unique topological structure on \( A[[X]] \) that

\[
U_{(X,T)} = \left\{ \sum_{\nu \in \mathbb{N}(I)} a_{\nu} X^\nu \in A(X)_T | a_{\nu} \in T^\nu U \right\},
\]

form a fundamental system of nbhds of \( A(X)_T \).

**Proof:** The proof is not hard and similar to that of (10.3.5.27) so omitted.

**Prop. (10.3.5.29).** Let \( A, X, T \) as in (10.3.5.27), then

- \( A[X]_T \) is dense in \( A(X)_T \) and the topology coincide.
- If \( A \) is Hausdorff and \( T_i \) is bounded for any \( i \in I \), then \( A[X]_T \) and \( A(X)_T \) are all Hausdorff.
- If \( A \) is complete and \( T_i \) is bounded for any \( i \in I \), then \( A(X)_T \) is complete, so it is the completion of \( A[X]_T \).

**Proof:** Only the completeness needs proof, Cf.[?]:P80.

**Prop. (10.3.5.30) [Power Series is Huber].** Let \( A \) be a Huber ring with a couple of definition \( (A_0, I) \), and \( X = \{ X_\lambda \} \) be a finite set of indeterminates, \( T_\lambda \) is a family of subsets of \( A \) that \( T_\lambda A \) is open in \( A \), then

- \( A[X]_T \) is a Huber ring with a couple of definition \( ((A_0)[X,T], I[X,T]) \), and there is a canonical map \( A \to A[X]_T \) which is adic.
- \( A(X)_T \) is Huber with a couple of definition \( ((A_0)_T(X), I(X,T)) \), and there is a canonical map \( A \to A(X)_T \) which is adic.

**Proof:** It suffices to prove for any ideal of definition \( J \), \( J_{[X,T]} = J \cdot (A_0)[X,T] \) and \( J_{(X,T)} = J \cdot (A_0)_T(X) \). The first is clear. For the second, use the fact \( J \) is f.g. and \( \{ J^n \} \) is a fundamental basis of nbhds of 0.

**Prop. (10.3.5.31) [Example].** Let \( A = \mathbb{Z}_p \) and \( T = p \), then there is a Huber ring

\[
\mathbb{Z}_p(X)_T = \{ \sum_{n \geq 0} a_n X^n \in \mathbb{Z}_p[[X]] | l^{-n} a_n \to 0 \}
\]
with a ring of definition

\[(Z_p)_{(X,T)} = \{ \sum_{n \geq 0} a_n X^n \in Z_p(X)_T | a_n \in p^nZ_p \}.\]

Notice that \(Z_p(X)_T\) is not adic although \(Z_p\) is (because \(p\) is nilpotent but \(pX\) is not).

**Def. (10.3.5.32) [Localizations].** Let \(A\) be a non-Archimedean topological ring and \(\{T_i\}\) is a family of subsets of \(A\) satisfying \(T_i^n U\) is open for any \(n > 0, i\) and open nbhd \(U\) of \(A\), and \(\{s_i\}\) is a family of elements of \(A\), which generates a multiplicative subset \(R \subset A\).

Then there is a unique non-Archimedean ring structure on \(R^{-1}A\), denoted by \(A(T_S)\), that the canonical map \(\varphi: A \rightarrow A(T_S)\) is continuous and the set \(\{ \varphi(t) \varphi(s_i) \}\) is power-bounded, and it is the initial map for all maps \(A \rightarrow B\) satisfying this property.

**Proof:** Cf. [Mor19]P83. \(\square\)

**Cor. (10.3.5.33).** Let \(J\) be the ideal of \(A[\frac{T}{S}]\) generated by \(\{1 - s_iX_i\}\), then \(A[\frac{T}{S}]\) with the quotient topology satisfies the same universal property as \(A(T_S)\), so there is a canonical isomorphism

\[A[\frac{T}{S}] \cong A(T_S).\]

In particular, \(A(T_S)\) is a Huber ring, and the canonical map \(A \rightarrow A(T_S)\) is adic. Explicitly, \(B_0\) is the \((A_0)_{(X,T)}\)-subalgebra of \(B\) generated by the elements \(\frac{T_i}{s_i}\).

**Def. (10.3.5.34).** If \(A\) is Huber ring, then we denote the completion of \(A(T_S)\) by \(A(T_S)\), which is also a Huber ring, and the canonical map \(A \rightarrow A(T_S)\) is adic, by (10.3.5.30) and (10.3.5.33). It satisfies the natural universal property.

**Cor. (10.3.5.35).** If \(A\) is complete, then we can also regard \(A(T_S)\) as the quotient of \(A(X)_T\) by the closure of the ideal generated by \(\{1 - s_iX_i\}\).

**Prop. (10.3.5.36) [Example].** Let \(A = Z_p[[T]]\) with the \((p, T)\)-adic topology, then

\[A(\frac{p, T}{T}) = Z_p[[T]][T^{-1}]\]

with a ring of definition \(A[p, T]\), and

\[A(\frac{p, T}{p}) = Z_p[[T]][p^{-1}]\]

with a ring of definition \(A[p, T]\).

In \(A(\frac{p, T}{T})\), a ring of definition is \(A(X)_T/(1 - pX)\), which is isomorphic to

\[A(\frac{T}{p}) = \{ \sum_{n \geq 0} a_n \frac{T}{p}^n | a_n \in A, a_n \rightarrow 0 \}\]

by (10.3.5.33).
6 Analytic Points and Analytic Huber Pairs

Def. (10.3.6.1) [Analytic Huber Rings]. A Huber ring is called analytic if the ideal generated by the topologically nilpotent elements is the unit ideal. Any Tate ring is analytic.

Prop. (10.3.6.2) [Equivalent Definitions of Analytic Rings]. For a Huber ring $A$, the following are equivalent:
1. $A$ is analytic.
2. Any ideal of definition in any ring of definition of $A$ generates the unit ideal of $A$.
3. Any open ideal of $A$ is trivial.
4. For any non-trivial ideal $I$ of $A$, the quotient topology on $A/I$ is not discrete.
5. The only discrete $A$-module is the $0$-module.
6. The set $\text{Spa}(A, A^+)$ contains no point with induced topology on the residue field trivial.

Proof: Cf. [?] P4.

Prop. (10.3.6.3) [Analytic Open Mapping Theorem]. If $A$ is an analytic Huber ring, and $M, N$ are complete Banach $A$-modules, then any continuous surjective map $M \to N$ is open.

Proof: Hub94, L2.4(i).

Analytic Points

Def. (10.3.6.4) [Analytic Points]. Let $A$ be a Huber ring, then a point $x \in \text{Cont}(A)$ is called an analytic point if $p_x$ is not open in $A$. The set of analytic points of $\text{Cont}(A)$ is denoted by $\text{Cont}(A)_{an}$.

If $A$ is Tate, then $\text{Cont}(A)_{an} = \text{Cont}(A)$, because the only open ideal of $A$ is $A$ itself.

Prop. (10.3.6.5) [Characterizations of Analytic Points]. Let $A$ be a Huber ring, then for a point $x \in \text{Cont}(A)$, the following is equivalent:
1. $x$ is analytic.
2. $|A^0|_x \neq 0$.
3. For any ring of definition and ideal of definition $(A_0, I)$ of $A$, $|I|_x \neq 0$.

Proof: 1 $\to$ 2: $p_x$ is non-open, so it cannot contain the open subset $A^0$ of $A$. 2 $\to$ 3: trivial because any ring of definition contains $A^0$ of $A$.

Cor. (10.3.6.6). Let $A$ be a Huber ring and $I$ an ideal of definition with a set of generators $(f_1, \ldots, f_n)$, then

$$\text{Cont}(A)_{an} = \bigcup_{i=1}^n U\left(\frac{f_1, \ldots, f_n}{f_i}\right).$$

Prop. (10.3.6.7) [Analytic Valuation Microbial]. Let $A$ be a Huber ring and $x \in \text{Cont}(A)_{an}$, then $x$ has rank $\geq 1$, and the valuation $|\cdot|_x$ on $k(x)$ is microbial (10.3.3.22).

Proof: If $x$ has rank 1, then $\Gamma_x = 1$, and $p_x = \{a \in A | a|_x < 1\}$ is open.

If $x$ is analytic, then there are some $a \in A^0$ that $|a|_x \neq 0$ of (10.3.3.22), thus the image of $a$ in $k(x)$ is non-zero and topologically nilpotent, thus $k(x)$ is microbial by (10.3.3.22).
Prop. (10.3.6.8) [Adic Morphism and Analytic Points]. Let $\varphi : (A, A^+) \to (B, B^+)$ be a morphism of Huber pairs, then:

- If $x \in \text{Spa}(B, B^+)$ is not analytic, then $\text{Spa}(\varphi)(x)$ is not analytic.
- If $\varphi$ is is adic, then $\text{Spa}(\varphi) : \text{Spa}(B, B^+) \to \text{Spa}(A, A^+)$ carries analytic points to analytic points.
- If $B$ is complete and $\text{Spa}(\varphi) : \text{Spa}(B, B^+) \to \text{Spa}(A, A^+)$ carries analytic points to analytic points, then $\varphi$ is adic.
- If $\varphi$ is adic, then the $\text{Spa}(\varphi)$ maps rational subsets to rational subsets. In particular, $\text{Spa}(\varphi)$ is spectral.

Proof: 1: Trivial.
2: If $f(x)$ is not analytic, then $I \subset \varphi^{-1}(p_x)$, so $f(I) \subset p_x$, which means $p_x$ is not analytic because $f(I)A_0$ is open.
3: Cf. Morel P96.
4: Only notice that $(f(T))$ is open if $(T)$ is open. □

Cor. (10.3.6.9). If $A$ is an analytic Huber ring, then any continuous morphism $f : A \to B$ is adic, by (14.8.4.24).

7 Huber and Banach Rings

Cf. [Ked19] 1.5.

Prop. (10.3.7.1). Let $A$ be a uniform Huber ring, then for $x = \sum_{n=0}^{\infty} x_n T^n \in A(T)$ such that the coefficients $x_n$ generate the unit ideal of $A$, then multiplication by $x$ defines a strict inclusion $A(T) \to A(T)$, i.e. $|xg| \geq |g|$.


8 Perfectoid Fields

Def. (10.3.8.1). The basis setting is a non-Archimedean complete valued field $K$, and denote $K^0 = \{x \in K | |x| \leq 1\}$, and $K^{00} = \{x \in K | |x| < 1\}$, which are rings because $K$ is non-Archimedean. $K = K^0 / K^{00}$ is the residue field of $K$. A non-zero element of $K^{00}$ is called a pseudo-uniformizer. $K^{00}$ is just the set of topological nilpotent elements of $K$.

Prop. (10.3.8.2). The valuation can in fact be constructed from $K^0$ as $|x| = \sup \left\{ \frac{n}{k} | x^k \in t^n K^0 \right\}$ by (2.2.8.5), as it is a rank 1 valuation.

Def. (10.3.8.3) [Perfectoid Field]. A perfectoid field is a non-Archimedean complete field with residue field of charp s.t.:
- The value group $|K^*| < \mathbb{R}^*$ is not discrete.
- $\mathcal{O}_K/p$ is semi-perfect.

Prop. (10.3.8.4) [Examples of Perfectoid Fields].
- $K = \mathbb{Q}_p(\mu_\infty)^\wedge$. Its valuation ring $K^0$ is $\mathbb{Z}_p(\mu_\infty)^\wedge$, and $K^0 / p \cong \mathbb{F}_p(\mu_\infty^\wedge)/(t)$, which is clearly semi-perfect. And its value group is $\mathbb{Z}[p^{-1}]$. 


• \( K = \mathbb{C}_p = \widehat{\mathbb{Q}_p} \), its value group is \( \mathbb{Q} \), and \( K \) is alg.closed, so \( K^0 \) is clearly perfect.

• if \( K \) is a non-Archimedean field of charp, then \( K \) is a perfectoid field iff \( K \) is perfect: if \( K \) is perfect, then it is clearly perfectoid, and the semi-perfectness of \( K^0 \) implies its perfectness, so also \( K \) is perfect (multiply by a \( p \)-power of an element in \( K^{00} \)).

• If \( K \) is a perfectoid field and \(|p| \leq |\pi| < 1 \) is a pseudo-uniformizer, then \( K/\pi \) is perfect hence perfectoid.

**Prop.(10.3.8.5)**[Perfectoid Field and Integral Perfectoid Rings]. The ring of integers \( \mathcal{O}_K \) for a perfectoid field \( K \) is an integral perfectoid ring(6.7.3.1).

**Proof:** We assume that \( K \) is of char0, then we check conditions in(6.7.3.6). It is clear that \( \mathcal{O}_K \) is \( p \)-adically complete, \( p \)-normal. To find \( \varpi^p = pu_1 \), as \( |K^*| \) is not discrete, we find \( x \) that \( x^p \) divides \( p \), and then there exists some \( y \) that \( y^p \equiv x^p/p \mod p \), thus \( (xy)^p \equiv 1 \mod p \), thus \( \varpi = xy \) satisfies the condition. \( \square \)

**Prop.(10.3.8.6).** If \( K \) is a perfectoid field, then

- \(|K^*| \) is \( p \)-divisible.
- \((K^{00})^2 = K^{00} \), and \( K^{00} \) is flat.
- \( K^0 \) is not Noetherian.

**Proof:** 1 : First if \(|p| < |x| \leq 1 \), we show \(|x| \) is \( p \)-divisible: there is a \( y, z \in K^0 \) that \( y^p = x + pz \), so \(|y|^p = |x| \). Now because \(|K^*| \) is not discrete, so there is a \(|x| \notin |p|^\mathbb{Z} \), by rescaling, we may assume \(|p| < |x| \leq 1 \), thus \( p = xy \) for some \( y \), and \(|p| < |y| \leq 1 \), too. So \(|p| \) is also divisible by \( p \), so it is clear now \(|K^*| \) is divisible by \( p \).

2 follows from(6.7.3.5)(10.3.8.5).

2 \to 3 by Nakayama’s lemma, because otherwise \( K^{00} = 0 \). \( \square \)

**Cor.(10.3.8.7).** The proof of 1 also shows that \(|K^*| \) is generated by \(|x| \) that \(|p| < |x| < 1 \).

**Lemma(10.3.8.8).** If \( C^0 \) is a perfectoid space of charp, then \( 1 + m_{C^0} \) is a \( \mathbb{Q}_p \)-algebra.

**Proof:** Both \( \varphi \) and exponentiation of \( \mathbb{Z}_p^\ast \) is definable, so \( p^n t \cdot (1 + x) = (\varphi^n(1 + x))^k \). \( \square \)

**Tilting**

**Prop.(10.3.8.9).** Fix a pseudo-uniformizer \(|p| \leq |\pi| < 1 \), consider the tilting(4.5.1.10) \( K\tilde{^b} \), then by(4.5.1.12), the group together with the topology doesn’t depends on \( p \) chosen.

\[
\lim_{x \to x^p} K^0 \xrightarrow{\approx} K^0.
\]

**Remark(10.3.8.10).** There are diagrams:

\[
K^{0b} = \lim_{\varphi} K^0/\pi \longrightarrow K^0/\pi
\]

**Prop.(10.3.8.11)**[Tilting of \( K^0 \)]. Let \( K^{0b} \) be given as in(10.3.8.9), then there is an element \( t \in K^{0b} \) that \(|t^p| = |\pi| \), and \( t \) maps into \((\pi)\) and gives an isomorphism \( K^{0b}/t \approx K^0/\pi \).

Moreover, the \( t \)-adic topology on \( K^{0b} \) is complete, and coincides with the topology of \( K^{0b} \) given as in(4.5.1.10).
Proof: There are canonical surjective map $K^0 \to K^0/p \to K^0/\pi$, and by $p$-divisibility of the value group (10.3.8.6), there is a $f \in K^0$ that $|f|^p = |\pi|$, so in particular $|f| > |\pi|$, thus $f \neq 0 \in K^0/\pi$. And choose a $g \in K^0$ lifting $f$ mod $\pi$, then $g^\sharp \equiv f$ mod $\pi$, see diagram (10.3.8.10). So $|g^\sharp| = |f|$, as $|f| > |\pi|$. Now let $t = g^p$, then $|t^\sharp| = |f|^p = |\pi|$. Now clearly $t$ maps into $(\pi)$, and if $g$ maps to 0 in $K^0/\pi$, then by the diagram again, $g^\sharp \in (\pi)$, and $(t^\sharp) = (\pi)$, so $g^\sharp = at^\sharp$ for some $a \in K^0$. So $t|g$ in $K^0$, as by (4.5.1.17), $K^0$ is a valuation ring in the valuation $|\cdot| \circ \sharp$.

For the last assertion, just use the commutative diagrams:

$$\begin{array}{ccc}
K^0/\langle t^p \rangle & \longrightarrow & K^0/\langle t^{p-1} \rangle \\
\downarrow & & \downarrow \\
K^0/(\pi) & \xrightarrow{\varphi} & K^0/(\pi)
\end{array}$$

the vertical are isomorphisms, and compute their inverse limits. □

Cor. (10.3.8.12)[Tilting of Perfectoid Field].

- $K^0$ is a valuation ring of rank 1, with the field of fraction $K^\flat = K^0[t^{-1}]$ which is a perfectoid.
- Its maximal ideal is $(t^{\frac{1}{mp}})$, and of Krull dimension 1.
- The value group and residue field of $K$ and $K^\flat$ is canonical isomorphic.

Proof: $K^0$ has rank no more than $K^0$ which is 1 (10.3.8.3), and it is non-trivial because $|t| = |\pi|$, so the rank is 1, and it is perfect by definition, so $K$ is perfectoid by (10.3.8.4).

For the maximal ideal, the maximal ideal of $K^0/t$ is its nilradical, as it is a valuation ring of rank 1 (2.2.8.5), which is clearly $(t^{\frac{1}{mp}})$. For the dimension, by (10.3.3.3), the Krull dimension equal the rank, which is 1.

For the residue field, use the isomorphism (10.3.8.11), $K^0/t = K^0/\pi$ and the second item just proved, and for the value group, the same lemma (10.3.8.11) gives any $|p| \leq |\pi| < 1$ are in the value group of $K^\flat$, and $|K^\flat|$ is generated by these values by (10.3.8.7). □

Prop. (10.3.8.13)[Tilting Continuous Valuations]. If $K$ is perfectoid, for any continuous valuation on $K$ of any rank, the function $|\cdot|^\flat = |\cdot| \circ \sharp$ is a continuous valuation on $K^0$, and all continuous valuation of $K^0$ comes from this way.

Proof: Clearly $|\cdot|^\flat$ is multiplicative and has trivial kernel, and it is non-Archimedean: for $f = (f_n), g = (g_n) \in K^\flat$, $f + g = (\lim_k (f_n+k+g_n+k)^{p^k})$ by (4.5.1.14). So

$$|f + g|^\flat = |(f + g)| = |\lim_k (f_k + g_k)^{p^k}| = \lim_k |f_k + g_k|^{p^k} \leq \lim_n \max(|f_n|, |g_n|)^{p^n} = \max(|f_0|, |g_0|).$$

so it is non-Archimedean. It is also continuous because $\sharp$ is continuous.

Conversely, we notice a continuous valuation on a rank 1 valuation field corresponds to valuation rings in the residue field $K^0/K^0$, so by (10.3.8.12), we get a bijection on the continuous valuations. □

Prop. (10.3.8.14)[Almost Purity in Dimension 0]. If $K$ is a perfectoid field, $L/K$ is a finite field ext, with the natural topology, then:

- $L$ is perfectoid.
- $[L^\flat : K^\flat] = [L : K]$.
- The map $L \to L^\flat$ defines an isomorphism $K_{\text{et}} \cong K_{\text{et}}^\flat$. 


10.3. TOPOLOGICAL COMMUTATIVE ALGEBRA

\[\text{Prop. (10.3.9.3)}\] Faithfully flatness of Perfectoids.

\[\text{Remark (10.3.9.2)}\]

\[\text{Def. (10.3.9.1)}\] Perfectoid Algebra.

\[\text{Remark (10.3.8.17)}\]

\[\text{Lemma (10.3.8.15)}\] [Kedlaya]. If \(K^\circ\) is alg.closed, then \(K\) is alg.closed.

**Proof:** This is a special case of almost purity theorem (10.3.10.1). \(\square\)

**Lemma (10.3.8.15)** [Kedlaya]. If \(K^\circ\) is alg.closed, then \(K\) is alg.closed.

**Proof:** Let \(P(X) = X^d + a_{d-1}X^{d-1} + \ldots + a_0 \in K^0[X]\) be an irreducible monic polynomial, then its Newton polygon is a line, and we may assume \(|a_0| = 1\), as \(K^0\) is alg.closed, so \(|K^0\| = |K^{0*}|(10.3.8.12)\) is a \(Q\)-vector space.

Next we choose a \(Q(X) \in K^0[X]\) that \(Q(X) \equiv P[X]\) mod \(t\), as \(K^0/t \cong K^0/\pi(10.3.8.11)\). Now consider \(P(x + y^\pi)\), then \(P(y^\pi)\) is divisible by \(\pi\), so its Newton polygon is now of positive slope, so \(c^{-d}P(cx + y^\pi) \in K^0[X]\) again, where \(c^d = |P(y^\pi)| \leq |\pi|\). Then notice by iteration this argument, we get a sequence of \(y^\pi_n\), and then \(y^\pi_1 + c_1 y^\pi_2 + c_1c_2 y^\pi_3 + \ldots + c_1 \ldots c_n y^\pi_{n+1}\) that converges to a root of \(P(X)\). \(\square\)

**Prop. (10.3.8.16)** [Examples of Tilting].

- If \(K = \mathbb{Q}_p(p^{\frac{1}{p^\infty}})^\wedge\), then \(K^0 = \mathbb{Z}_p[p^{\frac{1}{p^\infty}}]^\wedge\), thus \(K^\circ = \mathbb{F}_p((t))_{\text{perf}}(4.5.1.5)\). And if \(L = \mathbb{K}(\sqrt{p})\), then similarly \(L^0 = \mathbb{Z}_p[p^{\frac{1}{p^\infty}}],\) and \(L^\circ = K^\circ(\sqrt{L})\).

- If \(K = \mathbb{Q}_p(\mu_{p^\infty})^\wedge\), then \(K^0 = \mathbb{Z}_p[\mu_{p^\infty}]^\wedge\), notice there is a map \(\mathbb{Z}_p[p^{\frac{1}{p^\infty}}] \to \mathbb{Z}_p[\mu_{p^\infty}]\) with kernel \((1 + \varepsilon^p + \ldots + \varepsilon^{p^{-1}}),\) so

\[
K^0/p = \mathbb{F}_p[p^{\frac{1}{p^\infty}}]/(\varepsilon^p - 1)^n \cong \mathbb{F}_p[p^{\frac{1}{p^\infty}}]/(p^n - 1)
\]


with the substitution \(t = \varepsilon^p - 1\). Then by (10.3.8.4), \(K^{0b} = \mathbb{F}_p[t^\frac{1}{p^\infty}],\) and \(K^\circ = \mathbb{F}_p((t))_{\text{perf}}\).

**Remark (10.3.8.17).** Notice that \(K = \mathbb{Q}_p(\mu_{p^\infty})^\wedge\) and \(K = \mathbb{Q}_p(p^{\frac{1}{p^\infty}})^\wedge\) have the same tiltings, so the tilting functor is not faithful. This is due to the fact that \(\mathbb{Q}_p\) is not perfectoid. This will not happen over a perfectoid base field, see (10.3.9.13).

9 Perfectoid Algebras

**Def. (10.3.9.1)** [Perfectoid Algebra]. For \(K\) a perfectoid field with tilt \(K^\circ\), let \(t \in K^\circ\) be a pseudo-uniformizer with \(\pi = t^2\) satisfying \(|p| \leq |\pi| < 1\), so it has a compatible collection of \(p^n\)-th roots \((t^{p^n})^2\). Now:

- A **perfectoid algebra** over \(K\) is a uniform Banach \(K\)-algebra \(R\) that \(R^{0}/\pi\) is semi-perfect.

- A **perfectoid algebra** over \(K^{0a}\) is a \(K^{0a}\)-algebra \(A\) that is \(t\)-adically complete and flat over \(K^{0a}\) (or \(A\_\text{a} \) over \(K^0\), by (4.8.3.3)), and \(K^{0a}/\pi \to A/\pi\) is relative perfect, i.e. the Frobenius induces an isomorphism \(A/\pi^\frac{1}{n} \cong A/\pi\).

- A **perfectoid algebra** over \(K^{0a}/\pi\) is a \(K^{0a}/\pi\)-algebra \(A\) that is flat over \(K^{0a}/\pi\) (or \(A\_\text{a} \) over \(K^0/\pi\), by (4.8.3.3)), and the map \(K^{0a}/\pi \to A\) is relatively perfect, i.e. the Frobenius induces an isomorphism \(A/\pi^\frac{1}{n} \cong A\).

**Remark (10.3.9.2).** notice the definition regarding the relative perfectness doesn’t depend on \(\pi\) chosen, by the power lifting theorem (20.1.2.8).

**Prop. (10.3.9.3)** [Faithfully flatness of Perfectoids]. Nonzero flat \(K^{0a}/\pi\)-algebras are faithfully flat, so does \(t\)-adically complete flat \(K^{0a}\)-algebras. In particular, \(\text{Perf}_{K^{0a}/\pi}\) and \(\text{Perf}_{K^{0a}}\) are all faithfully flat modules.
Prop. (10.3.9.5) [Tilting Equivalence].

Prop. (10.3.9.4) [Examples of Perfectoid Algebras].

- If \( K \) has charp, then a \( K \)-Banach algebra is perfectoid iff it is uniform and perfect. Likewise, a \( \pi \)-adically complete and \( \pi \)-torsion free \( K^{0a} \)-algebra is perfectoid iff it is perfect.

- Let \( A = K^0 \left[ x_1^{\frac{1}{p}}, \ldots, x_n^{\frac{1}{p}} \right] \dagger \), then \( A^a \in \text{Perf}_{K^{0a}} \), and \( R = A[\pi^{-1}] \in \text{Perf}_K \) in the Banach metric as in (12.1.2.7).

Proof: 1: a perfectoid algebra of charp is perfect, because by semi-perfectness, \( x = x_1^p + \pi z_1 = x_1^p + \pi x_2^p + \pi^2 z_2 = \ldots \), so \( x = (x_1 + \pi^2 x_2 + \pi^3 x_3 + \ldots)^p \). In fact, uniformity is automatically implied by perfectness, by (10.3.5.12). The case of \( K^{0a} \)-algebra is similar.

2: \( A^a \) is \( K^{0a} \)-flat because \( A^s \) does, because it is a colimit of completions of polynomial algebras over \( I \) and \( I \) is flat over \( K^0(10.3.8.6). \) and \( R \) is perfectoid by (12.1.2.7) because \( A \) is totally integrally closed in \( R \), because \( K^0 \left[ x_1^{\frac{1}{p}}, \ldots, x_n^{\frac{1}{p}} \right] \) does (trivially), and use (4.8.2.10). \( \square \)

Tilting Equivalence

Prop. (10.3.9.5) [Tilting Equivalence]. There are canonical isomorphisms of categories:

\[ \text{Perf}_K \cong \text{Perf}_{K^{0a}} \cong \text{Perf}_K^{0a}/\pi, \]

where the first map is by \( R \mapsto R^{0a} \) and \( A \to A^s[\pi^{-1}] \) just as in (12.1.2.7). The second map is reduction by \( \pi \).

In particular, using tilting (10.3.8.11), there are canonical isomorphisms of categories:

\[ \text{Perf}_K \cong \text{Perf}_{K^{0a}} \cong \text{Perf}_K^{0a}/\pi = \text{Perf}_{K^{0a}/t} \cong \text{Perf}_{K^{0a}} \cong \text{Perf}_K. \]

Now if \( R \in \text{Perf}_K \) corresponds to \( S \in \text{Perf}_{K^\flat} \), then we call \( S = R^\flat \) the tilting of \( R \) and \( R = S^\dagger \) the untilting of \( S \).

Proof: \( [\text{Perf}_K \cong \text{Perf}_{K^{0a}}] \)

Firstly, if \( R \in \text{Perf}_K \), then \( A = R^{0a} \in \text{Perf}_{K^{0a}}: R^0/\pi^\frac{1}{p} \to R^0/\pi \) is surjective by definition, for injectivity, if \( x^p/\pi \in R^0 \), then \( x/\pi^{\frac{1}{p}} \) is also power bounded, thus in \( R^0 \). And by (12.1.2.7), \( A \) is \( \pi \)-adically complete and \( \pi \)-torsion-free, hence \( R \)-flat by (4.4.1.12).

Next we show if \( A \in \text{Perf}_{K^{0a}} \), then \( A^s \) is \( \pi \)-adically complete, \( t \)-torsion free and \( p \)-root closed in \( A[\pi^{-1}] \), hence is an left inverse to the mapping \( R \mapsto R^{0a} \), by (4.8.3.5). It is complete by (4.8.3.2.3).

For \( p \)-root closedness, by (4.8.3.3), \( A^s/\pi^{\frac{1}{p}} \subset (A/\pi^{\frac{1}{p}})^s \leftrightarrow (A/\pi)^s \) by Frobenius, and then so does \( A^s/\pi^{\frac{k}{p}} \to A^s/\pi \). Now if \( x \in A^s[\pi^{-1}] \) satisfies \( x^p \in A^s \), then \( y = \pi^{\frac{k}{p}} x \in A^s \) for some \( k \), and we want to lower \( k \) by \( 1 \) inductively, thus showing \( x \in A^s \): As \( y^p \in \pi A^s \), \( y \in \pi^{\frac{k}{p}} A^s \) by what we have proved, thus \( \pi^{\frac{k-1}{p}} x \subset A^s \).
For surjectivity of Frob: $A_*/\pi \rightarrow A_*/\pi$, notice first it is almost surjective, because $(A_*/A_*/\pi)^\alpha = A \rightarrow (A_*/A_*/\pi)^\alpha \subset (A/\pi)^\alpha = A/\pi$ is surjective by hypothesis, then by (4.8.2.3), it suffices to show that Frob is surjective on $\text{IA}/A$. For some $x \in A^*$, choose $0 < 1 < c$, almost surjectivity shows that $\pi^c x \equiv y^p \bmod \pi A_*$, so $(y/p^\hat{c})^p \in A_*$, thus $y \in p^\hat{c} A_*$, thus $x \equiv (y/p^\hat{c})^p \bmod \pi^{1-c} A_* \subset IA$, so we are done.

Finally, this is also a right inverse, because we know that $A_* \cong R^0$ by (4.8.3.5), thus $A \cong R^{00a}$ in $\text{Mod}_R^\alpha$.

Proof: $[\text{Perf}_{K^{00a}} \cong \text{Perf}_{K^{00a}/\pi}]$

Firstly the reduction is a perfectoid $K^{00a}/\pi$-algebra: it is flat because flatness is stable under base change, and the rest are trivial. To construct a converse is a problem of deformation theory, we need to lift from $K^{00a}/\pi$-algebra via $K^{00a}/\pi^n$-algebras to a $K^{00a}$-algebra, suppose each lifting is unique up to isomorphism and the lift $A_n$ is flat over $K^{00a}/\pi^n$, then we can form their inverse limit, which is flat, because it is $\pi$-torsion-free: if $\pi(x_n) = 0$, then by $0 \rightarrow \pi^n K^{00a}/\pi^{n+1} \rightarrow K^{00a}/\pi^{n+1} \pi^{n}, K^{00a}/\pi^n \rightarrow 0$ and the flatness of $A_{n+1}, x_{n+1} \in \pi^{n}A_{n+1},$ thus $x_n = 0$, and $x = 0$.

Now $0 \neq A \in \text{Perf}_{K^{00a}/\pi}$, then $A$ is faithfully flat by (10.3.9.3), then by (4.8.1.4), $A_!!$ is faithfully flat, and by (10.3.9.3) preserves all colimits and also Frobenius, so $A_!!$ is relatively perfect. Then we use the above argument, and (8.2.4.1) to show that there is a $A \in \mathcal{C}$ which is $\pi$-adically complete and $K^0$-flat, then $A = (A_!!)^a$ is also $p$-adically complete and $K^{00a}$-flat, by (4.8.3.3).

And we check $\tilde{A}/\pi = (A_!!/\pi)^a = (A_!!)^a = A$ as $(\tilde{A_!!})!!$ commutes with colimits, and conversely, if $A \in \text{Perf}_{K^{00a}}$, we need to show $A = \tilde{A}/\pi$, notice by hypothesis, $A_!!$ is faithfully flat $K^0$-algebra that is relatively flat over $K^0/\pi$, now it is also complete, because $A_!! \rightarrow A_*$ is an injection(because $(\tilde{A_!!})^a$ is exact) and almost isomorphism, so the cokernel is $\pi$-torsion, and $A_*$ is complete, so does $A_!!$, by (4.2.3.9). Now $A_!!/\pi = (A_!!/\pi)$ as $(\tilde{A_!!})!!$ commutes with colimits, so $A_!!$ is just the lift, and $(A_!!/\pi)^a = A_!!^a \cong A$.

Cor. (10.3.9.6) [Tilting via Fountain’s Functors]. The tilt $R^\circ$ is just the Fontain’s tilting, i.e. $R^\circ = R^{00}[t^{-1}]$, and $R^\circ = \lim_{x \rightarrow x^p} R$, $R^{00} = (R^0)^0$.

Proof: Consider the diagram

\[
\begin{array}{ccc}
K^{00}/t^p \cong K^0/\pi \\
\downarrow \gamma^n \\
K^{00}/t \cong K^0/\pi \\
\end{array}
\]

Then the upper row is just the unique flat and relative perfect lifting along $K^{00}/t^p \rightarrow K^{00}/t$. Taking inverse limit, we get the structure map $K^{00} \rightarrow R^{00}$, so after almostification, this is just the lifting we are looking for, because it is unique. So $(R^{00})^a = (R^{00})^a$, and $R^\circ = R^{00}[t^{-1}]$ unwinding the tilting equivalence.

For $R^\circ$, notice there is a map

\[
R^\circ \cong \left( \lim_{x \rightarrow x^p} R^0[\pi^{-1}] \right) \rightarrow \lim_{x \rightarrow x^p} (R^0[\pi^{-1}]) \cong \lim_{x \rightarrow x^p} R
\]

Now injectivity is clear as $t$ is non-zero-divisor, and if $(f_n) \in \lim_{x \rightarrow x^p} R$, then $\pi^cf_n \in R^0$ for some $c$, then $\pi^{\frac{n}{c}} f_n \in R^0$ because $R^0$ is $p$-root closed (4.8.3.5), so $t^c(f_n) \subset R^{00}$.
For the last assertion, it is true if $R^{\emptyset}$ is totally integrally closed in $R^\circ$, by (4.8.3.5). For this, if $t^\ast f^\emptyset \subset R^{\emptyset}$, then $\pi^\ast (f^2)^\emptyset \subset R^\circ$, thus $f^2 \in R^\circ$. And by $p$-root closedness, $p^n$-th roots of $f^2$ are all in $R^\circ$, so $f = (f_n) \in \lim_{\to +\infty} R$ is in $R^{\emptyset}$.

\textbf{Prop. (10.3.9.7) [Fountain's Functor $\theta$].} Given a perfectoid field $K$, the kernel of the Fontaine’s map $\theta : A_{inf}(K) \to K^0 (4.5.1.15)$ is generated by a non-zero-divisor, in fact, if $\text{char} K = 0$, the generator can be chosen to be any element that maps to a generator of $\ker \overline{\theta}$ and if $\text{char} K = p$ this diagram is trivial. In particular, the diagram is a pushout.

\textit{Proof:} See the proof of (6.7.3.6) in the $p$-torsionfree case.

\textbf{Prop. (10.3.9.8) [Untilting via $A_{inf}$].} For any perfect $K^{\emptyset}$-algebra $A$, by deformation theory (or in fact Witt theory) there is a unique lifting $W(A)$ lifting it to $A_{inf}(K^{\emptyset})$. And then pushout $W(A) \otimes_{A_{inf}(K^{\emptyset})} K^0$ is just the lifting of $A/\pi$, because the diagram above is pushout. This is in fact the method of [Kedlaya-Liu] used to prove the tilting-equivalence without the use of almost mathematics and deformation theory.

\textbf{Cor. (10.3.9.9) [Limits and Colimits].} Any of the categories in (10.3.9.5) has arbitrary limits and colimits.

\textit{Proof:} We construct for $\text{Perf}_{K^{\emptyset}}$: The limits is just the limits of topological rings, as the properties of $t$-adically complete, $t$-torsion free and perfect is preserved by limits (4.2.3.19). For the colimit, just use the $t$-adic completion of the left perfection of the colimits in the category of $K^{\emptyset}$-algebras, its $t$-torsion is almost zero because of perfectness, thus it is almost flat (4.8.3.3).

\textbf{Remark (10.3.9.10).} Note also for further reference that in the category $\text{Perf}_{K^{\emptyset}}$, a filtered colimits is just the $\pi$-adically completion of the filtered limits as rings, because perfectness and flatness is preserved (4.4.1.6).

\textbf{Prop. (10.3.9.11) [Un] Tilting Preserves Fields.} A perfectoid $K$-algebra $R$ is a perfectoid field iff its tilt $R^\circ$ is a perfectoid field.

\textit{Proof:} It is proven that if $R$ is a perfectoid field, then $R^{\emptyset}$ is a perfectoid field. Conversely, $R$ is a perfectoid field if the spectral norm given by $||x|| = \inf \{|t|^{-1}: t \in R^*, tx \in R^0\}$ is the Banach valuation of $R$ and $R$ is a field.

For the multiplicativity of $||-||_R$, notice that $R^\circ$ is a perfectoid field, so its non-Archimedean valuation coincides with the spectral norm of $||-||_{R^\circ}$, and this equals $||-||_R \circ \pi$, because $R^{\emptyset} = R^\circ$. Now the norm extends that of $K$ and commutes with scalar multiplication, so for any $f, g$, we may assume $f, g \in R^0 - \pi^k R^0$, now choose $a, b \in R^\circ$ that $a^2 - f, b^2 - g \in \pi R^0$, this can be done because $R^{\emptyset} = R^\circ \to R^0/\pi$ is surjective, then $a, b, ab \notin tR^0$ because $R^{\emptyset} = R^\circ$. Then clearly $||f||_R = ||a||_{R^\circ}, ||g|| = ||b||_{R^\circ}, ||fg||_R = ||ab||_{R^\circ}$, so it is multiplicative by the multiplicativity of $R^\circ$.

To show $R$ is a field, consider and $f \in R - \frac{1}{\pi} R$, choose $a \in R^\circ$ that $f = a^2 + \pi g$, then as $R^\circ$ is a field, there is a $b$ that $ab = 1$. Now $||\pi||_R < ||\pi^2||_R \subset ||f||_R = ||a||_{R^\circ} \leq 1$, so we get $||\pi b^\circ g|| < 1$, then

$$f^{-1} = \frac{1}{a^2 + \pi g} = \frac{b^\circ}{1 + \pi b^\circ g} = b^\circ (\sum (-\pi b^\circ g)^k)$$

can be constructed in $R$. 

\hfill $\Box$
Perfectoid Affinoid Algebra

**Def. (10.3.9.12)** [Perfectoid Affinoid \( K \)-algebras]. Fix a perfectoid field \( K \) and write \( \mathfrak{m} \subset K^0 \) and \( \mathfrak{m}^p \subset K^{0p} \) for the maximal ideals, and choose a pseudo-uniformizer \( t \) that \( |p| \leq |t|^{-1} < 1, \pi = t^2 \). Then an affinoid \( K \)-algebra \((R, R^+)\) is just an affinoid Tate ring over \((K, K^0)\). It is called a perfectoid affinoid \( K \)-algebra iff \( R \) is a perfectoid algebra.

**Prop. (10.3.9.13)** [Tilting Equivalence]. The categories of perfectoid affinoid algebras over \( K \) and \( K^p \) are equivalent, where \((R, R^+)\) is identified with \((R^p, R^{p0})\) iff \( R^p \) is the tilting of \( R \) and

\[
\begin{align*}
R^+ / \mathfrak{m} R^0 & \xrightarrow{\cong} R^{p+} / \mathfrak{m}^p R^{p0} \\
\downarrow & \downarrow \\
R^0 / \mathfrak{m} R^0 & \xrightarrow{\cong} R^{p0} / \mathfrak{m}^p R^{p0}
\end{align*}
\]

Moreover, in this case, \( R^+ / \pi \) is semi-perfect, and \( R^{+b} \cong R^{p0} \) as a subring of \( R^{0b} \cong R^{00} \).

**Proof:** The case \( R^+ = R^0 \) is already known by tilting equivalence (10.3.9.5) and (10.3.9.6).

By (10.3.5.11) and (10.3.5.14), \( \mathfrak{m} R^0 = R^{00} \subset R^+ \subset R^0 \), thus \( R^+ \to R^0 \) is an almost isomorphism and \( R^+ \) is determined by its image \( \overline{R^+} \subset R^0 / \mathfrak{m} R^0 \), which is integrally closed if \( R^+ \) does, so the identification is clear.

For the semi-perfectness: as \( R^+ / \mathfrak{m} R^0 \) is integrally closed, it is perfect. Now \( R^+ \to R^0 \) is an almost isomorphism, so Frob on \( R^+ / \pi \) is almost surjective because it does on \( R^0 / \pi \) by definition, and now we know Frob is surjective on \( R^+ / \pi \) by (4.8.2.3).

To show \( R^{+b} \cong R^{p0} \), we show there is a Cartesian diagram

\[
\begin{array}{c}
R^{+b} \xrightarrow{\cong} R^{p+} / \mathfrak{m}^p R^{p0} \\
\downarrow & \downarrow \\
R^0 & \xrightarrow{\cong} R^0 / \mathfrak{m}^p R^0
\end{array}
\]

is the Cartesian diagram

\[
\begin{array}{c}
R^+ / \pi \xrightarrow{} R^+ / \mathfrak{m} R^0 \cong R^{p+} / \mathfrak{m}^p R^{p0} \\
\downarrow & \downarrow \\
R^0 / \pi & \xrightarrow{} R^0 / \mathfrak{m}^p R^0
\end{array}
\]

applied the functor \((-)^{\text{perf}} \) which preserves limits (4.5.1.10). (Notice that \( R^+ / \mathfrak{m} R^0 \cong R^{p+} / \mathfrak{m}^p R^{p0} \) is already perfect).

**Cor. (10.3.9.14).** Notice that the proof also shows that \( R^+ \to R^0 \) is an almost isomorphism, thus if \( R \) is a perfectoid \( K \)-algebra, then \( R^+ \) is automatically a perfectoid \( K^{0\alpha} \)-algebra by (10.3.9.1).

**Cor. (10.3.9.15)** [Perfectoid Affinoid Field]. A perfectoid affinoid \( K \)-algebra \((R, R^+)\) is called a perfectoid affinoid field iff \( R \) is a perfectoid field and \( R^+ \) is an open valuation ring.

Notice this is equivalent to \( R^+ / \mathfrak{m} R^0 \) is a valuation ring in \( R^0 / \mathfrak{m} R^0 \). In particular, combining with (10.3.9.11), affinoid perfectoid fields are preserved under tilting and untilting.

**Cor. (10.3.9.16).** The tilting equivalence also shows that for any perfectoid affinoid \( K \)-algebra \((R, R^+)\), the tilting induces an equivalence of categories \( \text{Perf}_R \cong \text{Perf}_{K^0} \).

**Prop. (10.3.9.17)** [Filtered Colimits of Perfectoid Affinoid \( K \)-Algebras]. The category of perfectoid affinoid \( K \)-algebras has filtered colimits, and it is just the colimits in the category of complete uniform affinoid Tate rings (14.8.2.27). In particular, the filtered colimits of \((A_i, A^+_i)\) is \((\text{colim}_i A_i, \text{colim}_i A^+_i)\).

**Proof:** The colimit is perfectoid because the filtered colimits is exact.
10 Almost Purity Theorem

Prop. (10.3.10.1) [Almost Purity Theorem]. For a perfectoid $K$-algebra $R$ and its tilt $S$,

- Almost purity in characteristic $p$: (take $(-)_p$, and) Inverting $t$ gives an equivalence $S_{\text{f\acute{e}t}}^0 \cong S_{\text{f\acute{e}t}}$.
- Almost purity in characteristic 0: Inverting $\pi$ gives an equivalence $R^0_{\text{f\acute{e}t}} \cong R_{\text{f\acute{e}t}}$.
- Tilting and untilting functors induce equivalences $R^{0\ast}_{\text{f\acute{e}t}} \cong S^{0\ast}_{\text{f\acute{e}t}}$.

In particular, there are equivalences

$$S_{\text{f\acute{e}t}} \xleftarrow{a} S^{0\ast}_{\text{f\acute{e}t}} \rightarrow (S^{0\ast}/t)_{\text{f\acute{e}t}} \cong (R^{0\ast}/\pi)_{\text{f\acute{e}t}} \xleftarrow{c} R^{0\ast}_{\text{f\acute{e}t}} \rightarrow R_{\text{f\acute{e}t}}$$

Proof: The map $a$ is already given in (4.8.2.14) by passing the power bounded-elements (equivalently, $F_s$) and inverting $t$. And it is an isomorphism.

The equivalence of $b$ and $c$ follows from [Almost Ring theory, Thm5.3.27].

The functor $d$ is given by $A \rightarrow A_s[t^{-1}]$. Firstly, $A$ is a perfectoid $K^{0\ast}$-algebra. This is because it is almost finite projective thus almost flat, and $R^{0\ast}/\pi \rightarrow A/\pi$ is weakly relative perfect by (4.8.2.15), so does $K^{0\ast}/\pi \rightarrow A/\pi$ because relative perfect is stable under composition. And it is finite projective thus almost direct summand of a finite free module.

So now the tilting equivalence (10.3.9.5) shows that $A_s[t^{-1}] \in R_{\text{f\acute{e}t}}$ : it is finite etale because the $A_s$ is finite projective by the right adjointness of $(-)_s$, and unramified is defined in terms of $A_s$. The converse of $d$ is supposed to be the functor that extract from $A_s$ from $A_s[t^{-1}]$ the total integral closure $A_{\text{tic}}$ of $R^0$, which is functorial. We already know that $A_s$ is totally integrally closed in $A_s[t^{-1}]$ by (10.3.9.5), so $A_{\text{tic}} \subset A_s$. Conversely, as $A$ is almost totally generated over $R^0$, for $f \in A_s$, $\pi f^R$ lies in a f.g. $R^0$-submodule of $A_s$, so $f^R$ is totally integral over $R^0$, so $A_s = A_{\text{tic}}$.

It's left to show that $d$ is essentially surjective, but this uses perfectoid spaces. For now, we only check that this is true for $R$ being a perfectoid field (of char 0). For this, we show directly that the untangling functor $\sharp : K^{0\ast}_{\text{f\acute{e}t}} \rightarrow K_{\text{f\acute{e}t}}$ is essentially surjective. Now $\sharp$ is an equivalence of categories $\text{Perf}_{K^{0\ast}} \rightarrow \text{Perf}_K$, and it preserves degree, at least for field extensions, so it preserves Galois extensions. Now that finite étale algebra over fields are just disjoint of finite separable extensions (4.4.7.19), so it suffices to show that any finite extension of $K$ is contained in some $L^\sharp$.

Consider $M = \widehat{K^0}$, it is alg.closed of charp so clearly a perfectoid field, and by (10.3.8.15) $M^\sharp$ is alg.closed. $M^\sharp$ is just the colimit in the category of uniform Banach $K$-algebras, so its valuation ring is just the completion of the valuation ring of $L^\sharp$ for $L/K^\sharp$ finite Galois. Then if $N = \cup L^\sharp$, then $N$ is dense in $M^\sharp$, and $N/K$ is clearly algebraic and in particular Hensel. So $N \subset \overline{N} \subset M^\sharp$ is dense, so by Krasner’s lemma (12.1.1.35), $N = \overline{N}$. Now $N = \cup L^\sharp$ is an alg.closure of $K$, so every finite extension of $K$ is contained in some $L^\sharp$.

The proof of the general case of the essentially surjectivity of $d$ is continued at (14.8.7.10).
10.4 Real Analysis

Basic references are [Fol99], [周 08], [H-J99] and [谭-伍 06].

Notations (10.4.0.1).
- Use notations defined in Topology I.
- Use notations defined in Formal Power Series.

1 Measures

Def. (10.4.1.1) [σ-Algebra]. Let $A \in \text{Set}$, then an algebra of subsets of $A$ is a subset of $\mathcal{P}(A)$ that is closed under finite intersections and finite unions. A σ-algebra on $A$ is an algebra of subsets of $A$ that is closed under countable unions.

Def. (10.4.1.2) [Measurable Space]. A measurable space is a tuple $(X, \mathcal{M})$ where $X$ is a set and $\mathcal{M}$ is a σ-algebra on $X$.

Def. (10.4.1.3) [Measure]. A measure on a measurable space $(X, \mathcal{M})$ is a function $\mathcal{M} \to [0, \infty]$ that
- $\mu(\emptyset) = 0$.
- If $E_i$ is a countable family of disjoint sets in $\mathcal{M}$, then $\mu(\bigcup_{i=1}^{\infty} E_i) = \sum_{i=1}^{\infty} \mu(E_i)$.
A measure space is a measurable space together with a measure $\mu$. A probabilistic measure is a measure $\mu$ on $(X, \mathcal{M})$ that $\mu(X) = 1$.

Def. (10.4.1.4) [Complex Measure]. A complex measure on a measurable space $(X, \mathcal{M})$ is a function $\nu : \mathcal{M} \to \mathbb{C}$ that
- $\nu(\emptyset) = 0$.
- If $E_i$ is a countable family of disjoint sets in $\mathcal{M}$, then $\mu(\bigcup_{i=1}^{\infty} E_i) = \sum_{i=1}^{\infty} \mu(E_i)$, where the series converges absolutely.

Def. (10.4.1.5) [Measurable Map]. A measurable map $f : (X, \mathcal{M}) \to (Y, \mathcal{N})$ is a map $f : X \to Y$ that $f^{-1}(E) \in \mathcal{M}$ for any $E \in \mathcal{N}$.

Def. (10.4.1.6) [Non-Singular Maps]. A non-singular measurable map is a measurable map of measure spaces that the preimage of every set of measure 0 has measure 0.

Def. (10.4.1.7) [Lebesgue Space]. A one-point subset with positive measure is called an atom. A Lebesgue space is a finite measure space that is isomorphic to a finite union of intervals and countably many atoms.

Thm. (10.4.1.8) [Radon-Nikodym]. If two σ-finite measures $v, \mu$ on a measurable space satisfies $v$ is absolutely continuous w.r.t $\mu$, then there is a $\mu$-integrable function $f$ such that
\[ dv = fd\mu. \]

Proof: This is a special case of the Freudenthal spectral theorem (10.8.4.18).
Borel Sets

Def. (10.4.1.9) [Radon Measure]. Let \( X \in \text{Top} \), a Borel measure on \( X \) is a measure defined on the \( \sigma \)-algebra generated by open sets.

A Borel measure \( \mu \) is called \textit{inner regular} on a Borel set \( E \) iff \( \mu(E) = \inf \{ \mu(K) | K \subset E \text{ compact} \} \) for every Borel set \( E \). It is called \textit{outer regular} iff \( \mu(E) = \sup \{ \mu(U) | E \subset U \text{ open} \} \).

A Radon measure is a Borel measure that is finite on compact set, outer regular on Borel sets, inner regular on open sets.

Prop. (10.4.1.10). Every Radon measure is inner regular on all of its \( \sigma \)-finite sets.

\textit{Proof:} Cf. [Folland, Real Analysis, P216]. \( \square \)

Cor. (10.4.1.11). Every \( \sigma \)-finite Radon measure is regular. In particular, if \( X \) is \( \sigma \)-compact, then every Radon measure is regular.

Measurable Functions

Prop. (10.4.1.12) [convergences]. There are three different kinds of convergences:

- \textit{almost everywhere convergence} iff \( f_n(x) \to f(x) \) a.e.
- \textit{almost uniform convergence} iff for any \( \delta > 0 \), there is a measurable subset \( E_\delta \) that \( f_n \) convergent to \( f \) uniformly on \( E - E_\delta \).
- \textit{convergence in measure} iff \( \lim_{k \to \infty} m(\{x \in E | |f_n(x) - f(x)| > \varepsilon \}) = 0 \).

Prop. (10.4.1.13) [Relations between Convergences].

- (Egoroff) If \( m(E) < \infty \) and \( f_k \) converges to \( f \) a.e. then \( f_k \) converges to \( f \) almost uniformly.
- If \( f_k \) converges to \( f \) almost uniformly, then \( f_k \) converges to \( f \) in measure.
- (Riesz) If \( f_k \) converges to \( f \) in measure, then there is a subsequence \( f_{nk} \) that converges to \( f \) a.e.

\textit{Proof:} 1: Cf. [实变函数周明强 P113].
2: Trivial.
3: Cf. [实变函数周明强 P118]. \( \square \)

2 Integrations

Def. (10.4.2.1) [Simple Functions].

Def. (10.4.2.2). A measurable function \( f : \mathbb{R}^n \to \mathbb{C} \) is called \textit{locally integrable} if \( \int_K |f(x)|dx < \infty \) for every bounded measurable set \( K \) of \( \mathbb{R} \). The set of locally integrable function is denoted by \( L^1_{\text{loc}}(\mathbb{R}^n) \).

Prop. (10.4.2.3). A function \( f \) is real analytic on an open set of \( \mathbb{R} \) iff there is a extension to a complex analytic function to an open set of \( \mathbb{C} \). And this is equivalent to: For every compact subset, there is a constant \( C \) that for every positive integer \( k \), \( |\frac{d^k f}{dx^k}(x)| \leq C^{k+1}k! \).

\textit{Proof:} Use Lagrange residue (中值定理) to show that it will converge to \( f \). \( \square \)

Prop. (10.4.2.4) [Monotone-convergence-theorem].
Prop. (10.4.2.5) [Dominant Convergence Theorem].

Prop. (10.4.2.6). The set $E$ of nowhere differentiable functions are of second category in $C[0,1]$, and its complement set is of first category.

Proof: let $A_n$ be the sets of functions $f$ that there exists a $s$ that for any $|h| \leq 1/n$, $|\frac{f(s+h)-f(s)}{h}| \leq n$. It is easy to see that $C[0,1] - E \subset \cup_n A_n$, so it suffices to show each $A_n$ is of first category.

Firstly $A_n$ is closed, because if $s \notin A_n$, then for any $s$, there is a $|h_s| \leq 1/n$ that $|f(s+h_s) - f(s)| > n|h_s|$. So by continuity, there is a $\varepsilon > 0$ and some nbhd $J_s$ of $s$ that $|f(\sigma - h_s) - f(\sigma)| > n|h_s| + 2\varepsilon$ for all $\sigma \in J_s$. Then there are f.m. $J_s$, that covers $[0,1]$, so let $\varepsilon = \min\{\varepsilon_i\}$, then if $\|g - f\| < \varepsilon$, then $g \notin A_n$.

And $A_n$ has no interior point, because for any $f \in A_n$, $f$ can be approximated by a polynomial $g$, by Stone-Weierstrass theorem (10.4.6.1), and by Mean-value theorem, there is a $M$ that $|g(s + h) - g(s)| \leq M|h|$ for all $s$ and $|h| < 1/n$. So if $p$ is a pairwise-linear function that $\|p\|$ is small and the slopes of $p$ are bigger than $M + n$, then $g + p$ is near $f$ but $g + p \notin A_n$.

Finally, $E$ is of second category by Baire theorem (3.6.9.2). □

Prop. (10.4.2.7) [Fubini-Tonelli]. For two $\sigma$-finite measure spaces $X, Y$,

- If $f \in L^+(X \times Y)$, then $f_x \in L^+(Y)$ and $f^y \in L^+(X)$, and

$$\int_{X \times Y} f dx dy = \int_Y \int_X f dx dy = \int_X \int_Y f dy dx.$$

- If $f \in L^1(X \times Y)$, then $f_x \in L^1(Y)$ and $f^y \in L^1(X)$, a.e. and the product formula is definable and holds.

Proof: Cf. [Folland P67]. □

3 Differentiations

Lemma (10.4.3.1) [Vitali Covering Theorem]. Let $C$ be a collection of balls in $\mathbb{R}^n$, and let $U = \cup_{B \in C} B$. Then if $c > m(U)$, then there exists disjoint $B_1, \ldots, B_k \in C$ that $\sum_{i=1}^k m(B_k) > 3^{-n}c$.

Proof: □

Lemma (10.4.3.2). If $f \in L^1_{\text{loc}}$ and $A_r f(x) = \frac{1}{\text{vol}(B(r,x))} \int_{B(r,x)} f(y) dy$, then $A_r f$ is continuous in both $r$ and $x$.

Proof: Cf. [Folland P96]. □

Prop. (10.4.3.3). If $f \in L^1_{\text{loc}}$, then $\lim_{r \to 0} A_r f(x) = f(x)$ for a.e. $x \in \mathbb{R}^n$.

Proof: Cf. [Folland P97]. □

Differentiation on Euclidean Spaces

Prop. (10.4.3.4) [Fermat]. Let $x_0 \in \mathbb{R}, \delta \in \mathbb{R}_+$, $f$ is a function on $U(x_0, \delta)$. If $x_0$ is an extreme point of $f$, and $f'(x_0)$ exists, then $f'(x_0) = 0$.

Proof: By changing $f$ to $-f$ if necessary, we can assume $x_0$ is a supremum point. Then for $0 < h < \delta$, $\frac{f(x_0+h) - f(x_0)}{h} \leq 0$, and for $-\delta < h < 0$, $\frac{f(x_0+h) - f(x_0)}{h} \geq 0$, so $f'(x) = 0$. □
**Lemma (10.4.3.5) [Rollé’s Mean Value Theorem].** If \( a < b \in \mathbb{R} \), \( f \in C([a, b]) \) is differentiable on \([a, b]\), and \( f(a) = f(b) \), then there exists some \( \xi \in (a, b) \) s.t. \( f'(\xi) = 0 \).

**Proof:** As \( f \) is continuous on \([a, b]\), which is compact, \( f \) has minimum \( m \) and maximum \( M \) on \([a, b]\). If \( m = M \), then \( f \) is constant, and any \( \xi \in (a, b) \) will do. If \( M > m \), then \( M \neq f(a) \) or \( m \neq f(a) \). Suppose WLOG the first case happens, then if \( f(\xi) = M, \xi \in (a, b) \), then \( f'(\xi) = 0 \) by Fermat’s theorem (10.4.3.4). \( \square \)

**Thm. (10.4.3.6) [Lagrange’s Mean Value Theorem].** If \( a < b \in \mathbb{R} \), \( f \in C([a, b]) \) is differentiable on \([a, b]\), then there exists some \( \xi \in (a, b) \) s.t. \( f'(\xi) = \frac{f(b) - f(a)}{b - a} \).

**Proof:** This follows from Rolle’s mean value theorem by considering the function
\[
F(x) = f(x) - [f(a) + \frac{f(b) - f(a)}{b - a}(x - a)].
\]
\( \square \)

**Cor. (10.4.3.7) [Cauchy’s Mean Value Theorem].** If \( a < b \in \mathbb{R} \), \( f, g \in C([a, b]) \) is differentiable on \([a, b]\), and \( g' \neq 0 \). then there exists some \( \xi \in (a, b) \) s.t. \( \frac{f(b) - f(a)}{g(b) - g(a)} = \frac{f(\xi)}{g'(\xi)} \).

**Proof:** This follows from Rolle’s mean value theorem by considering the function
\[
G(x) = f(x) - [f(a) + \frac{f(b) - f(a)}{g(b) - g(a)}(g(x) - g(a))].
\]
\( \square \)

**Prop. (10.4.3.8) [Commutativity of Integration].** Let \( n \in \mathbb{Z}_+, n \geq 2, \Omega \subset \mathbb{R}^n \) be open and \( f \in C(\Omega) \). If \( 1 \leq j < k \leq n \) and \( \frac{\partial}{\partial x_j} \frac{\partial}{\partial x_k} f, \frac{\partial}{\partial x_k} \frac{\partial}{\partial x_j} f \) exist and continuous on \( \Omega \), then
\[
\frac{\partial}{\partial x_j} \frac{\partial}{\partial x_k} f = \frac{\partial}{\partial x_k} \frac{\partial}{\partial x_j} f.
\]
In particular, this holds for \( f \in C^2(\Omega) \).

**Proof:** For simplicity we prove for \( n = 2, i = 1, j = 2 \), and the general case is verbatim. For \( \mathbf{x} = (x, y) \in \Omega \), if \( \Delta x, \Delta y \) is sufficiently small, define
\[
I(\Delta x, \Delta y) = \frac{f(x_0 + \Delta x, y_0 + \Delta y) - f(x_0 + \Delta x, y_0)}{\Delta x \Delta y} - \frac{f(x_0, y_0 + \Delta y) - f(x_0, y_0)}{\Delta x \Delta y}
\]
and
\[
g(x) = f(x, y_0 + \Delta y) - f(x, y_0), \quad h(y) = f(x_0 + \Delta x, y) - f(x_0, y).
\]
Then by mean value theorem (10.4.3.6),
\[
I(\Delta x, \Delta y) = \frac{g(x_0 + \Delta x) - g(x_0)}{\Delta x \Delta y} = \frac{g'(x_0 + \theta_1 \Delta x)}{\Delta y}
\]
\[
\frac{\partial}{\partial x} f(x_0 + \theta_1 \Delta x, y_0 + \Delta y) - \frac{\partial}{\partial x} f(x_0 + \theta_1 \Delta x, y_0) \\
= \frac{\partial}{\partial y} \frac{\partial}{\partial x} f(x_0 + \theta_1 \Delta x, y_0 + \theta_2 \Delta y)
\]

where \(\theta_1, \theta_2 \in [0, 1]\), and

\[
I(\Delta x, \Delta y) = \frac{h(y_0 + \Delta y) - h(y_0)}{\Delta x \Delta y}
\]

\[
= \frac{h'(y_0 + \theta_3 \Delta y)}{\Delta x}
\]

\[
= \frac{\partial}{\partial y} f(x_0 + \Delta x, y_0 + \theta_3 \Delta y) - \frac{\partial}{\partial x} f(x_0, y_0 + \theta_3 \Delta y)
\]

\[
= \frac{\partial}{\partial y} f(x_0 + \theta_4 \Delta x, y_0 + \theta_3 \Delta y)
\]

where \(\theta_3, \theta_4 \in [0, 1]\). Then we get

\[
\frac{\partial}{\partial y} \frac{\partial}{\partial x} f(x_0 + \theta_1 \Delta x, y_0 + \theta_2 \Delta y) = \frac{\partial}{\partial x} \frac{\partial}{\partial y} f(x_0 + \theta_4 \Delta x, y_0 + \theta_3 \Delta y).
\]

Now let \(\Delta x, \Delta y \to 0\) and use the fact \(\frac{\partial}{\partial x} \frac{\partial}{\partial y} f\) are continuous to finish the proof. □

**Functions of Bounded Variation**

**Def.(10.4.3.9) [Absolute Continuity].** For \(a, b \in [-\infty, \infty]\), \(f \in C([a, b])\) is called **absolutely continuous** on \([a, b]\) if for any \(\varepsilon > 0\), there exists \(\delta < 0\) s.t. for any f.m. disjoint intervals \((a_i, b_i), i \leq N,\)

\[
\sum_{i=1}^{N} (b_i - a_i) < \delta \implies \sum_{i=1}^{N} |F(b_i) - F(a_i)| < \varepsilon.
\]

**Prop.(10.4.3.10).** For \(a < b \in [-\infty, \infty]\), \(f \in C([a, b])\) is differentiable and \(F^n\) is bounded, then \(F\) is absolutely continuous.

**Proof:** This follows from the fact \(|F(b_i) - F(a_i)| \leq (\sup |F'|)|b_i - a_i|\) by mean value theorem(10.4.3.6). □

**Thm.(10.4.3.11)[Fundamental Theorem of Calculus for Lebesgue Measure].** If \(a, b \in \mathbb{R}\) and \(F \in C([a, b])\), then the following are equivalent:

- \(F\) is absolutely convergent on \([a, b]\).
- \(F(x) - F(a) = \int_a^x f(t)dt\) for some \(f \in L^1([a, b], m)\).
- \(F\) is differentiable a.e. on \([a, b]\), \(F^n \in L^1([a, b], m)\), and \(F(x) - F(a) = \int_a^x F^n(t)dt\).

In particular, this is the case for \(F\) everywhere differentiable and \(F^n\) bounded, by(10.4.3.10).

**Proof:** Cf.[Fol99]P106.
4 Power Series

Prop. (10.4.4.1) [Cauchy-Hadamard]. For any power series \( a_0 + a_1 x + \ldots + a_n x^n + \ldots \) in \( \mathbb{R} \), take \( 1/R = \lim_{n \to \infty} |a_n|^{1/n} \), where we assume \( 1/0 = \infty \) and \( 1/\infty = 0 \), then

- The series converges absolutely for every \( |x| < R \), and if \( \rho < R \), then the convergence is uniform for \( |x| \leq \rho \).

- If \( |x| > R \), the terms are unbounded, and the series diverges.

And \( R \) is called the radius of convergence of the sequence.

\[ \text{Proof:} \quad 1: \text{For } 0 < \rho < R, \text{ take } \rho_1 \in (\rho, R), \text{ then the definition of } R \text{ implies that for some } N \in \mathbb{Z}_+, \text{ and any } n \geq N, |a_n| \leq R^{-n} < \rho_1^{-n}, \text{ so } |a_n x^n| \leq (\rho/\rho_1)^n, \text{ so } \sum_{n \in \mathbb{N}} a_n x^n \text{ converges absolutely and uniformly for } |x| \leq \rho. \]

2: For \( R < |x| \), the definition of \( R \) implies that for any \( N \in \mathbb{Z}_+ \), there exists \( n \geq N \) s.t. \( a_n \geq R^{-n} \), so \( |a_n x^n| \geq |x/R|^n \geq 1, \) so this sequence cannot be convergent. \( \square \)

Lemma (10.4.4.2). For a sequence \( (a_n)_{n \in \mathbb{N}} \) in \( \mathbb{R}_+ \),

\[ \lim_{n \to \infty} \frac{a_{n+1}}{a_n} \leq \lim_{n \to \infty} a_n^{1/n} \leq \lim_{n \to \infty} a_n^{1/n} \leq \lim_{n \to \infty} \frac{a_{n+1}}{a_n}. \]

\[ \text{Proof:} \quad \text{Let } \lim_{n \to \infty} a_n^{1/n} = R. \text{ If } R > 0, \text{ then by definition, for any } \varepsilon > 0 \text{ and } M \in \mathbb{Z}_+, \text{ there exists some } m \geq M \text{ s.t. } a_m^{1/m} < R + \varepsilon. \text{ Then for such } M, a_m/a_1 \leq (R + \varepsilon)^m/a_1. \text{ So for some } k \leq m, a_k/a_{k-1} \leq ((R + \varepsilon)^m/a_1)^{m-1}. \text{ Then if } M \text{ is very large, } a_k/a_{k-1} \leq R + 2\varepsilon. \text{ Thus } \lim_{n \to \infty} \frac{a_{n+1}}{a_n} \leq R. \]

Then \( \lim_{n \to \infty} a_n^{1/n} \leq \lim_{n \to \infty} \frac{a_{n+1}}{a_n} \) follows from this by considering the sequence \( b_n = a_n^{-1} \). The other inequality is trivial. \( \square \)

Prop. (10.4.4.3). For any power series \( a_0 + a_1 x + \ldots + a_n x^n + \ldots \) in \( \mathbb{R} \), if \( \lim_{n \to \infty} \frac{a_{n+1}}{a_n} = \rho \in [0, \infty] \), then the radius of convergence (10.5.3.1) \( R = 1/\rho \), where we assume \( 1/0 = \infty \) and \( 1/\infty = 0 \).

5 \( L^p \) space

Lemma (10.4.5.1) [Hölder]. If \( \sum x_i = 1, x_i \geq 0 \), then for any \( a_i \geq 0 \)

\[ \prod a_i^{x_i} \leq \sum a_i x_i. \]

\[ \text{Proof:} \]

Prop. (10.4.5.2) [Holder’s Inequality]. Let \( (S, \Omega, \mu) \) be a measure space, and \( 1 \leq p, q \leq \infty \) satisfies \( 1/p + 1/q = 1 \), then

\[ ||fg||_1 \leq ||f||_p ||g||_q \]

More generally, if \( \sum_{i=1}^n 1/p_i = 1 \), then

\[ ||\prod f_i||_1 \leq \prod ||f_i||_{p_i} \]

\[ \text{Proof:} \quad \text{The both sides are homogenous for } f_i, \text{ so we may assume } ||f_i||_{p_i} = 1, \text{ then use Hoder’s Lemma (10.4.5.1) for } x_i = q/p_i. \]

Prop. (10.4.5.3) [Dual of \( L^p(\mu) \)]. For a \( \sigma \)-finite measurable space \( (X, \mathcal{M}, \mu) \), for \( 1 \leq p < \infty \)

\[ L^p(X, \Omega, \mu)^* = L^q(X, \Omega, \mu). \]
Proof: Firstly, Holder inequality (10.4.5.2) shows that a \( g \in L^q(X, \Omega, \mu) \) defines a functional by \( f \mapsto \int fgd\mu \). Conversely, if given a functional \( F \), define a measure \( v(E) = F(\chi_E) \) for all measurable set \( E \in \Omega \). It is countably additive: first it is finitely additive, and if \( E_n \) is a descending sequence of measurable sets that \( \cap E_n = \emptyset \), then

\[
v(E_n) \leq ||F|| ||\chi_{E_n}||_{L^p} = ||F|| \mu(E_n)^{\frac{1}{p}} \to 0.
\]

(where we used the fact \( p < \infty \)). And it is clearly absolutely continuous w.r.t. \( \mu \).

So by Radon-Nikodym (10.4.1.8), there is a measurable function \( g \) that \( v(E) = \int_E g \, d\mu \). So for all simple function \( f \), \( F(f) = \int f(x)g(x) \). Next we want to prove \( ||g||_q \leq ||F|| \), because any measurable function \( f \) can be approximated by simple functions \( f_i \) in \( L^p \) norm (10.4.6.5), so

\[
\int |f(x) - f_i(x)||g(x)|d\mu \leq ||f - f_i||_p ||g||_q \leq ||f - f_i||_p ||g||_q
\]

So \( F(f) = \lim F(f_i) = \lim \int f_i g d\mu = \int f g d\mu \).

To prove this, if \( 1 < p \), then let \( E_t = \{ x \mid |g(x)| \leq t \} \), and \( f = \chi_{E_t} |g|^{q-2}g \), then

\[
\int_{E_t} |g|^q d\mu = \int fgd\mu = F(f) \leq ||F|| ||f||_{L^p} = ||F|| \left( \int_{E_t} |g|^q d\mu \right)^{\frac{1}{q}}
\]

which is equivalent to \( ||g\chi_{E_t}||_{L^q} \leq ||F|| \). Let \( t \to \infty \), then the monotone convergence theorem (10.4.2.4) gives us the result.

If \( p = 1 \), then \( q = \infty \). For any \( \varepsilon > 0 \), let \( A = \{ x \mid |g(x)| > ||F|| + \varepsilon \} \), \( E_t = \{ x \mid |g(x)| \leq t \} \), and let \( f = \chi_{E_t \cap A} \text{ sgn}(g) \), then \( ||f||_{L^1} = \mu(E_t \cap A) \), and

\[
\mu(E_t \cap A)(||F|| + \varepsilon) \leq \int_{A \cap E_t} |g| d\mu = \int fgd\mu \leq ||F|| \mu(E_t \cap A)
\]

If \( \mu(A) \neq 0 \), then let \( t \to \infty \), this is a contradiction. So \( ||g||_\infty \leq ||F|| \). \( \square \)

Prop.(10.4.5.4)|Hilbert Basis for Products|. For two \( \sigma \)-finite measure spaces \( M, N \) and Hilbert basis (10.6.4.9) \( \{e_i\} \) of \( L^2(M) \) and \( \{f_j\} \) of \( L^2(N) \), \( \{e_i \otimes f_j\} \) gives a Hilbert basis for \( L^2(M \times N) \). (Use Fubini).

Proof: It is easily verified that \( e_i \otimes f_j \) are mutually orthogonal, and if some \( f \in L^2(M \times N) \) satisfies \( (f, e_i \otimes f_j) = 0 \) for all \( i, j \), then

\[
\int_M e_i(x) \int_N f(x, y) f_j(y) = 0
\]

for all \( i \). But \( f_N f(x, y) f_j(y) \in L^2(M) \) for a.e. \( x(f(x, y) \in L^2(N) \) a.e. \( x \) by Fubini-Tonelli), thus it vanishes. So \( f(x) = f(x, y) = 0 \in L^2(N) \) for a.e. \( x \), so by Fubini-Tonelli again, \( ||f||_{L^2(M \times N)} = 0 \), thus \( f = 0 \). \( \square \)

Prop.(10.4.5.5)|Minkowski’s Inequality|. Let \( (X, \mathcal{M}, \mu), (Y, \mathcal{N}, \nu) \) be \( \sigma \)-finite measure spaces, and \( f \) a \( (\mathcal{M} \otimes \mathcal{N}) \)-measurable function on \( X \times Y \).

- If \( f \geq 0 \) and \( 1 \leq p < \infty \), then

\[
\left( \int \left( \int f(x, y) d\nu(y) \right)^p d\mu(x) \right)^{1/p} \leq \int \left( \int f(x, y)^p d\mu(x) \right)^{1/p} d\nu(y).
\]
\[ \text{Proof:} \quad \text{1: If } p = 1, \text{ then this is just Tonelli's theorem(10.4.2.7), and when } 1 < p < \infty, \text{ let } q^{-1} + p^{-1} = 1, \text{ and } g \in L^q(\mu), \text{ then by Tonelli's theorem and Holder's inequality(10.4.5.2),} \]

\[ \int [\int f(x,y)d\nu(y)]|g(x)|d\mu(x) = \int \int f(x,y)|g(x)|d\mu(x)d\nu(y) \leq ||g||_q \int [f(x,y)^pd\nu(y)]^{1/p}d\nu(y). \]

So we finish by(10.4.5.3).

2 follows from 1 and Fubini’s theorem. And when \( p = \infty \), this is trivial. \( \square \)

**L^2-Space**

**Def.(10.4.5.6).** Let \( X \) be a measure space, then there is a map

\[
\star : L^2(X \times X) \times L^2(X \times X) \rightarrow L^2(X \times X) : (K_1 \star K_2)(u,v) = \int_X K_1(u,x)K_2(x,v)dx.
\]

By Schwarz inequality, \( ||K_1 \star K_2||_2 \leq ||K_1||_2 \star ||K_2||_2 \), thus \( \star \) makes \( L^2(G \times G) \) into a Banach algebra(without a unit).

This Banach algebra can left and right act on \( L^2(X) \), also denoted by \( \star \), then for \( K \in L^2(X \times X) \), \( P,Q \in L^2(X) \),

\[
(P \otimes Q) \star K = P \otimes (Q \star K), \quad K \star (P \otimes Q) = (K \star P) \otimes Q.
\]

And also for \( S,T \in L^2(X) \),

\[
(P \otimes Q) \star (S \otimes T) = (Q,S)_{L^2}P \otimes T.
\]

**Prop.(10.4.5.7).**

- An element \( K \in L^2(X \times X) \) has the form \( P \otimes Q \) iff \( K \star K' \star K \) is proportional to \( K \) for all \( K' \in L^2(X \times X) \).
- Let \( K_1 = P_1 \otimes Q_1 \) and \( K_2 = P_2 \otimes Q_2 \), then \( P_1 \) and \( P_2 \) are proportional iff \( K_1 \star K \) and \( K_2 \star K \) are proportional for all pure tensors \( K \in L^2(X \times X) \). Similarly, \( Q_1 \) and \( Q_2 \) are proportional iff \( K \star K_1 \) and \( K \star K_2 \) are proportional for all pure tensor \( K \).
- For any uniform transformation \( s : L^2(X \times X) \rightarrow L^2(X \times X) \) respecting \( \star \), there exists a unitary transformation \( s_0 : L^2(X) \rightarrow L^2(X) \) s.t. \( s(P \otimes Q) = s_0(P) \otimes s_0(Q) \). And it can be chosen to be invertible iff \( s \) is.

**Proof: ** Cf.[Bump, P527]. \( \square \)

6 Approximations

**Prop.(10.4.6.1)[Stone-Weierstrass Approximation].** If a unital \( C^* \)-algebra \( A \) of continuous functions on a compact Hausdorff space separates points, then it is dense in \( C(X) \).
Proof: This is a consequence of Bishop theorem (10.7.3.18) because in this case the real functions in A separate points, so all A-antisymmetric sets consists of one point. □

Cor. (10.4.6.2). The polynomial functions are dense in $C[−1, 1]$.

Prop. (10.4.6.3) [Simple Function Approximation]. Let $E$ be a measure space,
- If $f(x)$ is a non-negative measurable function on $E$, then there is an ascending sequence of simple functions $(\varphi_n(x))$ that converges to $f$ point-wise.
- If $f(x)$ is a measurable function on $E$, then there is a sequence of simple functions $\varphi_n$ that $|\varphi_k(x)| \leq |f(x)|$, and converges to $f$ pointwise.
- If $f(x)$ is bounded, then the convergence can be chosen to be uniform.

Proof: Cf. [实变函数周明强 P110]. □

Estimations

Prop. (10.4.6.4). $\lim_{n \to \infty} n^{1/n} = 1$.

Proof: Let $n^{1/n} = 1 + \delta_n$, $\delta_n > 0$, then $n = (1 + \delta_n)^n \geq 1 + \frac{n(n−1)}{2}\delta_n^2$, so $\delta_n \leq \sqrt{2/n}$, and $\lim_{n \to \infty} \delta_n = 0$. □

$L^p$-Approximation

Prop. (10.4.6.5) [Simple Function Approximation]. Any function in $L^p$ can be approximated by compactly supported simple functions in $L^p$ norm.

Proof: □

Prop. (10.4.6.6). For $1 \leq p < +\infty$, $C_c(X)$ are dense in $L^p(X)$ for a Radon measure, but not for $p = \infty$.

Proof: Use compactly supported simple function approximation (10.4.6.5) and then use outer regular approximation (10.4.1.9) and then Tietz extension. □

Prop. (10.4.6.7) [Lusin]. If $f$ is almost everywhere finite on $E$, then for any $\delta > 0$, there is a closed subset $F \subset E$ that $f$ is continuous function on $F$.

Proof: First if $f$ is a simple function $f = \sum^n_{i=1} c_i \chi_{E_i}$, then for each $E_i$, choose a closed subset $F_i \subset E_i$ that $m(E_i - F_i) < \frac{\delta}{n}$, and then $\cup F_i$ satisfies the required condition.

Now if $f$ is arbitrary, let $g(x) = \frac{f(x)}{1+|f(x)|}$ to make it bounded, then by (10.4.6.3), there is a sequence of simple functions $\varphi_k$ converging to $f$, and for each $k$, we choose a closed subset $F_k$ that $m(E - F_k) < \frac{\delta}{2^k}$, so if we let $F = \cap F_k$, then $\varphi_k$ are all continuous on $F$, so by the uniform convergence, $f$ is also continuous on $F$. □

Cor. (10.4.6.8). If $f$ is measurable function on $E$ that is a.e. finite, then for any $\delta$, there is a continuous function $g$ that $m(\{x \in E | f(x) \neq g(x)\}) < \delta$. And if $E$ is bounded, $g$ can be chosen to be compactly supported.

Proof: Now that there is a closed subset $F$ that $m(E - F) < \delta$ and $f$ is continuous on $F$, we can use Tietze extension (3.6.6.3), there is a function $g$ that equals $f$ on $F$.

If $E \subset B(0, R)$, the we can choose a bump function to multiply with $g$. □
Prop. (10.4.6.9). For $1 \leq p < +\infty$, trigonometric polynomials are dense in $L^p(\mathbb{T})$ and $C(\mathbb{T})$, but not for $p = \infty$. So $e^{2\pi inx}$ forms an orthogonal basis in $L^2(\mathbb{T})$.

Thus, the Parseval’s identity holds.

Proof: Just use the fact that Fejer kernels are an approximate identity.

Prop. (10.4.6.10). For an integrable function $u$ that has compact support, $u_\delta = j_\delta * u$ is a smooth function of compact support that $||u_\delta - u||_{C^k} \to 0$ when $u \in C^k$. Where $j_\delta$ is the scaling of a smooth function of compact support. So Smooth function of compact support are dense in $C^k_0$.

Prop. (10.4.6.11). $D(\mathbb{R}^n)$ is dense in $W^{m,p}(\mathbb{R}^n)$.

Proof: Use the fact that $C_0$ are dense in $L^p$ by (10.4.6.10). And $f_\delta \to f$ in $L^p$ norm for $f \in C_0$. So we can use the three-part argument applied to $D_\alpha u$ to get $D_\alpha(u_\delta) \to D_\alpha u$ in $L^p$ norm for $|\alpha| \leq m$. Thus the result.

7 Convolutions

Prop. (10.4.7.1). Convolution with a smooth function makes the function smooth, in particular, $\frac{\partial}{\partial x} (f * g) = \frac{\partial f}{\partial x} * g$.

Prop. (10.4.7.2)[Young’s Inequality]. $||f * g||_r \leq ||f||_p ||g||_q$ for all $1 \leq r, p, q \leq \infty$ and

$$1 + \frac{1}{r} = \frac{1}{p} + \frac{1}{q}.$$ 

In particular, $||K * f||_p \leq ||K||_1 ||f||_p$.

Proof: By Riesz representation (10.9.1.10), it suffices to show that: for $\frac{1}{p} + \frac{1}{q} + \frac{1}{r} = 2$,

$$\int \int f(x)g(y-x)h(y) \leq ||f||_p ||g||_q ||h||_r.$$ 

write the LHS as

$$\int \int (f^p(x)g(y-x)q)^{1-\frac{1}{r}}(f^p(x)h^r(y))^{1-\frac{1}{r}}(g^q(y-x)h^q(y))^{1-\frac{1}{r}}$$

and use Holder inequality for three functions (10.4.5.2).

8 Examples of Calculations

Prop. (10.4.8.1). Assume $\text{Re}(s) > 1/2$, then

$$\int_{-\infty}^{\infty} (1 + x^2)^{-s} e^{ik \arctan -\frac{1}{2} x} dx = (-i)^k \sqrt{\pi} \frac{\Gamma(s)\Gamma(s - \frac{1}{2})}{\Gamma(s + \frac{1}{2})\Gamma(s - \frac{k}{2})}.$$ 

Proof: Cf. [Bump, Automorphic Forms and Representations, P230].
10.5 Complex Analysis

Basic References are [Ahl79], [S-S03], [谭-伍06] and [李04].

1 Basics

Def. (10.5.1.1) [Regions]. A region is a nonempty connected open set of \( \mathbb{C} \).

Def. (10.5.1.2) [Conjugations]. The non-zero element in \( \text{Gal}(\mathbb{C}/\mathbb{R}) \) is denoted by \( e \). And for \( z \in \mathbb{C} \), \( e(z) \) is also denoted by \( \overline{z} \).

For \( z \in \mathbb{C} \), denote \( \text{Re}(z) = \frac{z + \overline{z}}{2}, \text{Im}(z) = \frac{z - \overline{z}}{2i} \), called the real part and complex part of \( z \) resp. So \( z = \text{Re}(z) + i \text{Im}(z) \).

Prop. (10.5.1.3) [\( \mathbb{C} \) is Complete]. The natural extended value from \( \mathbb{R} \) to \( \mathbb{C} \) is of the form \( |x + iy| = \sqrt{x^2 + y^2} \). In particular, it is easy to prove that \( \mathbb{C} \) is a complete valued field.

Def. (10.5.1.4) [Derivatives]. We introduce the following notations:

\[
\frac{\partial}{\partial z} = \frac{1}{2} \left( \frac{\partial}{\partial x} - i \frac{\partial}{\partial y} \right), \quad \frac{\partial}{\partial \overline{z}} = \frac{1}{2} \left( \frac{\partial}{\partial x} + i \frac{\partial}{\partial y} \right), \quad dz = dx + i dy \quad d\overline{z} = dx - i dy.
\]

Then \( dz \) is dual to \( \frac{\partial}{\partial z} \) and \( d\overline{z} \) is dual to \( \frac{\partial}{\partial \overline{z}} \). And for any function \( f \),

\[
df = \frac{\partial f}{\partial x} dx + \frac{\partial f}{\partial y} dy = \frac{\partial f}{\partial z} dz + \frac{\partial f}{\partial \overline{z}} d\overline{z}.
\]

Def. (10.5.1.5) [Cross Ratios]. For any three pts \( z_1, z_2, z_3 \in \mathbb{C} \), there is a unique linear transformation that maps them to \( 1, 0, \infty \). In fact, the linear transformation is just \( Sz = \frac{z - z_3}{z - z_4} \).

Then for any for point \( z_1, z_2, z_3, z_4 \), the cross ratio \( (z_1, z_2, z_3, z_4) \) is the image of \( z_1 \) under the linear transformation that carries \( z_2, z_3, z_4 \) to \( 1, 0, \infty \).

Prop. (10.5.1.6). The cross ratio is invariant under linear transformation, and it is real iff \( z_1, z_2, z_3, z_4 \) are colinear or cocycle.

Proof: The first is because there is only one linear transformation that maps \( z_2, z_3, z_4 \) to \( 1, 0, \infty \).

For the second, notice by (10.5.1.5), \( \arg(z_1, z_2, z_3, z_4) = \arg \frac{z_1 - z_3}{z_1 - z_4} - \arg \frac{z_2 - z_4}{z_3 - z_4} \), and this is real iff \( \angle z_4z_2z_3 = \angle z_4z_1z_3 \) or \( \pi - \angle z_4z_1z_3 \), which is equivalent to cocycle. For other degenerate cases, we need some other argument. \( \square \)

Cor. (10.5.1.7). A linear transformation maps colinear/cocycle points to colinear/cocycle points.

Lemma (10.5.1.8) [Invariant Factor]. If \( a, b, c, d \in \mathbb{R} \), then

\[
\text{Im}(\frac{az + b}{cz + d}) \overset{=}{\underset{\text{Im}(z)}{\iff}} \frac{ad - bc}{|cz + d|^2} \text{Im}(z).
\]
**Analytic Functions**

**Def.(10.5.1.9)** [Analytic Functions]. For an open subset \( \Omega \subset \mathbb{C} \), a complex-valued function \( f \) on \( \Omega \) is called **analytic** or **holomorphic** if \( \frac{\partial}{\partial z} f(z) = 0 \) for any \( z \in \Omega \). Equivalently,

\[
\frac{\partial}{\partial x} f = -i \frac{\partial}{\partial y} f, \quad \text{i.e.} \quad \begin{cases} 
\frac{\partial}{\partial x} \Re(f) = \frac{\partial}{\partial y} \Im(f) \\
\frac{\partial}{\partial x} \Im(f) = -\frac{\partial}{\partial y} \Re(f) 
\end{cases}
\]

i.e. \( f \) has the same derivative vertically and horizontally, hence in every direction.

The space of analytic functions on \( \Omega \) is denoted by \( \mathcal{O}(\Omega) \). More generally, if \( \Omega \subset \mathbb{C} \) is any subspace, \( \mathcal{O}(\Omega) = C(\Omega) \cap \mathcal{O}(\Omega^o) \).

For \( f \in \mathcal{O}(\Omega) \), denote

\[
f'(z) = \frac{\partial}{\partial z} f(z) = \frac{\partial}{\partial x} f(z) = -i \frac{\partial}{\partial y} f(z).
\]

and for \( n \in \mathbb{N} \), denote inductively

\[
f^{(0)} = f, \quad f^{(1)} = f', \quad f^{(n+1)} = (f^{(n)})'.
\]

**Lemma(10.5.1.10).** Let \( \Omega \subset \mathbb{C} \) be a region and \( f \in \mathcal{O}(\Omega) \) s.t. \( f' = 0 \), then \( f \) is a constant function.

*Proof:* This follows from the fact any two points in \( \Omega \) can be connected by a path consisting of vertical or horizontal segments, and use the fundamental theorem of calculus(10.4.3.11). \( \square \)

**Conformal Mapping**

**Prop.(10.5.1.11).** Any \( C^1 \) conformal map in \( \mathbb{C} \) is holomorphic or anti-holomorphic. In higher dimension, conformal is equivalent to \( \langle df_p(v_1), df_p(v_2) \rangle = \lambda^2(p) \langle v_1, v_2 \rangle \).

*Proof:* Cf.[Ahlfors P74]. \( \square \)

**2 Complex Integration**

**Lemma(10.5.2.1).** If \( f \) is analytic on a rectangle \( R \) minus f.m. points \( \zeta_i \) and if \( \lim_{z \to \zeta_i} (z - \zeta_i)f(z) = 0 \), then \( \int_{\partial R} f(z)dz = 0 \).

*Proof:* We consider first the case that no points are omitted. Cut the rectangle \( R \) into 4 rectangles \( R^1, R^2, R^3, R^4 \) that is similar to \( R \), then

\[
\int_{\partial R} f(z)dz = \sum_{i=1}^{4} \int_{\partial R^i} f(z)dz.
\]

Let \( |\int_{\partial R} f(z)dz| = T \), then there exists some \( R^i \) that \( |\int_{\partial R^i} f(z)dz| \geq \frac{1}{4} T \). Denote this \( R^i \) by \( R_1 \).

Then we can do the same for \( R_1 \) to find an \( R_2 \) s.t. \( |\int_{\partial R_2} f(z)dz| \geq \frac{1}{8} T \). Continuing this process, we find a sequence \( R_1 \supset R_2 \supset \ldots \supset R_n \supset \), and their intersection is a single point \( z_0 \) as \( R \) is compact.

Now as \( f \) is analytic, for any \( \varepsilon > 0 \), for \( n \) sufficiently large, for any \( z \in \partial R_n \),

\[
\left| \frac{f(z) - f(z_0)}{z - z_0} - f'(z_0) \right| \leq \varepsilon.
\]
Notice also by direct calculating that
\[ \int_{\partial R_n} dz = 0, \quad \int_{\partial R_n} z dz = 0, \]
we have
\[ \frac{T}{4^n} \leq |\int_{\partial R_n} f(z)dz| = |\int_{\partial R_n} [f(z) - f(0) - f'(0)(z - 0)]dz| \leq \varepsilon \int_{\partial R_n} |z - 0||dz| \leq \varepsilon \frac{dL}{4^n} \]
where \( d, L \) are the length of the diagonal and the perimeter of \( R \). So \( T \leq \varepsilon \). As \( \varepsilon \) is arbitrary, this means \( T = 0 \).

In general, by cutting into several rectangles, it suffices to prove for the case that only one point is omitted, and in this case, we can use what we have proved and the hypothesis to reduce the rectangle to any small enough rectangle \( R_0 \) around \( \zeta_1 \) s.t. for any \( z \in \partial R_0 \),
\[ f(z) \leq \frac{\varepsilon}{|z - \zeta_1|}. \]
And then
\[ |\int_{\partial R_0} f(z)dz| \leq \varepsilon \int_{\partial R_0} \frac{|dz|}{|z - \zeta_1|} \leq 8\varepsilon \]
by elementary estimation. As \( \varepsilon \) is arbitrary, this means \( \int_{\partial R_0} f(z)dz = 0 \).

**Thm. (10.5.2.2) [Cauchy]**. If \( \Omega \subset C \) is a simply-connected region and \( \Omega' \) is the region obtained from \( \Omega \) by omitting f.m. points \( \zeta_i \). Suppose \( f \in \mathcal{O}(\Omega') \), and \( \lim_{z \to \zeta_i} (z - \zeta_i)f(z) = 0 \), then \( \int_{\gamma} f(z)dz = 0 \) for any closed piecewise \( C^1 \) curve \( \gamma \subset \Omega' \).

Moreover, if \( f \in \mathcal{O}(\overline{\Omega}) \), then \( \int_{\gamma} f(z)dz = 0 \) for any closed piecewise \( C^1 \) curve \( \gamma \subset \overline{\Omega} \setminus \{\zeta_1, \ldots, \zeta_i\} \).

**Proof**: Fix a \( z_0 \in \Omega \), then for any \( z \in \Omega \), choose a path \( \gamma \) from \( z_0 \) to \( z \) consisting of vertical or horizontal segments, and let \( F(z) = \int_{\gamma} f(z)dz \). Then this \( F \) is well-defined: if there are two paths \( \gamma, \gamma' \), \( \gamma - \gamma' \) is a sum oriented boundary of rectangles, and these rectangles must be contained in \( \Omega \) because \( \Omega \) is simply-connected. Thus the above lemme(10.5.2.1) shows that \( F(z) \) is independent of the path chosen, and it is clear that \( F(z) \) has the same derivative in both directions so analytic by definition(10.5.1.9). So clearly \( \int_{\gamma} f(z)dz = F(z)\big|_{\gamma(0)}^{\gamma(1)} = 0 \).

For the last assertion, any such a closed piecewise \( C^1 \) curve \( \gamma \subset \overline{\Omega} \setminus \{\zeta_1, \ldots, \zeta_i\} \) can be uniformly approximated by a path in \( \Omega' \). \( \square \)

**Cor. (10.5.2.3)**. If \( \Omega \subset C \) is a simply connected region and \( f \in \mathcal{O}(\Omega) \), then there exists a function \( F \in \mathcal{O}(\Omega) \) s.t. \( F' = f \).

**Proof**: Take \( z_0 \in \Omega \) and take \( F(z) = \int_{\gamma} f(z)dz \) for any path \( \gamma \) from \( z_0 \) to \( z \). \( F \) is well-defined by the Cauchy theorem(10.5.2.2). \( \square \)

**Prop. (10.5.2.4) [Generating Analytic Functions]**. If \( \varphi(\zeta) \) is continuous on an arc \( \gamma \), then the function
\[ F_n(\zeta) = \int_{\gamma} \frac{\varphi(\zeta)}{(\zeta - z)^n} d\zeta \]
is analytic on each connected component of \( C \setminus \gamma \), and its derivative is \( F'_n(z) = nF_{n+1}(z) \).
Then we see by induction hypothesis that in this case, hence

thus $F_1$ is continuous. Moreover, the above argument applied to the function $\Phi(\zeta) = \varphi(\zeta)/(\zeta - z_0)$ implies that

\[
\frac{F_1(z) - F_1(z_0)}{z - z_0} = \frac{1}{z - z_0} \int_{\gamma} \frac{\varphi(\zeta)}{(\zeta - z)(\zeta - z_0)} d\zeta = \frac{1}{z - z_0} \int_{\gamma} \frac{\Phi(\zeta)}{\zeta - z_0} d\zeta = \frac{1}{z - z_0} \int_{\gamma} \frac{\Phi(\zeta)}{\zeta - z_0} d\zeta = F_2(z_0),
\]

hence $F_1 = F_2$.

For $n > 1$, suppose we have shown $F_{n-1} = (n-1)F_n$, then with notations as above, we have

\[
F_n(z) - F_n(z_0) = \left[ \int_{\gamma} \frac{\varphi(\zeta)}{(\zeta - z)^{n-1}(\zeta - z_0)} d\zeta - \int_{\gamma} \frac{\varphi(\zeta)}{(\zeta - z_0)^n} d\zeta \right] + (z-z_0) \int_{\gamma} \frac{\varphi(\zeta)}{(\zeta - z)^n(\zeta - z_0)} d\zeta
\]

Then we see by induction hypothesis that $\lim_{z \to z_0} F_n(z) - F_n(z_0) = 0$ and $F_n$ is continuous for any $\varphi$. Moreover,

\[
\lim_{z \to z_0} \frac{F_n(z) - F_n(z_0)}{z - z_0} = \lim_{z \to z_0} \frac{1}{z - z_0} \left[ \int_{\gamma} \frac{\Phi(\zeta)}{(\zeta - z)^{n-1}} d\zeta - \int_{\gamma} \frac{\Phi(\zeta)}{(\zeta - z_0)^n} d\zeta \right] + \int_{\gamma} \frac{\Phi(\zeta)}{z - z_0} d\zeta
\]

\[
= n \int_{\gamma} \frac{\Phi(\zeta)}{(\zeta - z_0)^n} d\zeta + \int_{\gamma} \frac{\Phi(\zeta)}{(\zeta - z)^n} d\zeta = (n+1)F_{n+1}(z)
\]

\[\square\]

**Prop. (10.5.2.5)** [Index of a Point w.r.t a Curve]. If $\gamma$ is a piecewise $C^1$ curve that doesn’t pass a point $a$, then $\frac{1}{2\pi i} \int_{\gamma} \frac{dz}{z-a}$ is an integer $n(\gamma, a)$, called the index of a w.r.t. $\gamma$.

And this index function is constant on each connected component of $\mathbb{C} \setminus \gamma$, and 0 on the unbounded component. In particular, if $\gamma$ is a circle and $a$ is contained in the interior of this circle, then $n(\gamma, a) = 1$.

**Proof:** Cf. [Ahl79]P115.?

this index function is constant on each connected component of $\mathbb{C} \setminus \gamma$, and 0 on the unbounded component by the continuity of the integral by (10.5.2.4).

For the last assertion, it suffices to show for $\gamma = \partial D(0, R)$ and $a = 0$, by what we just said. And in this case,

\[
\frac{1}{2\pi i} \int_{\gamma} \frac{dz}{z-a} = \frac{1}{2\pi i} \int_{0}^{2\pi} \frac{Re^{i\theta}}{Re^{i\theta}} d\theta = 1
\]

\[\square\]

**Cor. (10.5.2.6)** [Cauchy Integral Formula]. if $\Omega \subset \mathbb{C}$ is a simply-connected region, $f \in \mathcal{O}(\Omega)$, then for any piecewise $C^1$ closed curve $\gamma \subset \Omega$ and $a \notin \gamma$,

\[
\frac{1}{2\pi i} \int_{\gamma} \frac{f(\xi)}{\xi - a} d\xi = n(\gamma, a) f(a)(10.5.2.5).
\]
In particular, if \( \gamma \) is the boundary of a disk \( D \) contained in \( \mathbb{C} \), then for any \( a \in D \),

\[
\frac{1}{2\pi i} \int_{\gamma} \frac{f(\xi)}{\xi - a} \, d\xi = f(a).
\]

Moreover, if \( f \in \mathcal{O}(\Omega) \), then this is true for any piecewise \( C^1 \) closed curve \( \gamma \subset \Omega \) and \( a \notin \gamma \).

**Proof:** Consider the function \( F(z) = \frac{f(z) - f(a)}{z - a} \), then it is analytic for \( z \neq a \), and at \( a \) it satisfies the condition of Cauchy theorem (10.5.2.2), so \( \int_{\gamma} F(z) \, dz = 0 \) which is \( \int_{\gamma} \frac{f(z) \, dz}{z - a} = f(a) \int \frac{dz}{z - a} \), and use (10.5.2.5). \( \square \)

**Cor. (10.5.2.7) [Higher Derivations].** For any region \( \Omega \), if \( a \in \Omega \) and \( \gamma \) is a small circle \( \gamma \) in \( \Omega \) centered at \( a \),

\[
f(a) = \frac{1}{2\pi i} \int_{\gamma} \frac{f(\zeta)}{\zeta - a} \, d\zeta
\]

by Cauchy integral theorem (10.5.2.6). So derivatives of \( f \) are all analytic, and satisfy:

\[
f^{(n)}(z) = \frac{n!}{2\pi i} \int_{\gamma} \frac{f(\zeta)}{(\zeta - z)^{n+1}} \, d\zeta.
\]

In particular, \( \mathcal{O}(\Omega) \subset C^\infty(\Omega) \).

**Cor. (10.5.2.8) [Morera].** If \( f \) is continuous on a region \( \Omega \) and if \( \int_{\gamma} f(z) \, dz = 0 \) for any piecewise closed curve \( \gamma \subset \Omega \) consisting of vertical or horizontal segments, then \( f(z) \in \mathcal{O}(\Omega) \).

**Proof:** There is an analytic function \( F \) that \( F' = f \), by the same method of the proof of (10.5.2.2), so \( f \) is analytic, by (10.5.2.7). \( \square \)

**Cor. (10.5.2.9) [Cauchy Estimate].** If \( f \in \mathcal{O}(\overline{D}(a,r)) \), and \( |f| \leq M \) on the boundary, then \( |f^{(n)}(a)| \leq M n! r^{-n} \) for any \( a \in D \).

**Cor. (10.5.2.10) [Liouville].** Any bounded holomorphic function on \( \mathbb{C} \) is constant.

**Proof:** if \( |f(z)| \leq M \), then the Cauchy estimate shows that \( |f'(a)| \leq M r^{-1} \), letting \( r \) tends to \( \infty \), then \( f'(a) = 0 \) for all \( a \), thus \( f \) is constant. \( \square \)

**Cor. (10.5.2.11) [Mean Value Property].** If \( f \in \mathcal{O}(\mathbb{D}) \), then \( |f(0)| \leq \int_{\mathbb{D}} |f(z)| \, dx \, dy \).

**Proof:** \( |f(0)| \leq \frac{1}{2\pi} \int f(re^{i\theta}) \, d\theta \), so if multiplied by \( r \, dr \) and integrate, then

\[
|f(0)| \leq \int \int f(re^{i\theta}) \, r \, dr \, d\theta = \int \int f(z) \, dx \, dy.
\]

\( \square \)

**Prop. (10.5.2.12).** For any \( f \in \mathcal{O}(\overline{D}(0,R)) \), for \( z \in \mathbb{D}(0,R) \):

\[
f(z) = \frac{1}{2\pi i} \int_{|\zeta| = R} \frac{\text{Re}(\zeta + z) f(\zeta)}{\zeta - z} \frac{d\zeta}{\zeta}.
\]
Proof: Let \( F(\zeta) = \frac{f(\zeta)}{\zeta - R^2/\overline{z}} \), then \( F \in \mathcal{O}(\overline{D}(0, R)) \), and by Cauchy’s theorem (10.5.2.2),
\[
\int_{|\zeta|=R} \frac{f(\zeta)}{\zeta - R^2/\overline{z}} d\zeta = 0.
\]
And by Cauchy’s integral formula,
\[
\frac{1}{2\pi i} \int_{|\zeta|=R} \frac{f(\zeta)}{\zeta - z} d\zeta = f(z).
\]
so
\[
f(z) = \frac{1}{2\pi i} \int_{|\zeta|=R} \frac{f(\zeta)}{\zeta - z} [f(\zeta) - \frac{\zeta}{\zeta - z}] d\zeta = \frac{1}{2\pi i} \int_{|\zeta|=R} \frac{f(\zeta)}{\zeta - z} d\zeta = \frac{1}{2\pi i} \int_{|\zeta|=R} \text{Re}(\zeta + z)f(\zeta) d\zeta
\]
\( \square \)

Constructing Analytic Functions

Prop. (10.5.2.13)[Holomorphic Function Defined by Integrations]. Let \((X, M, \mu)\) be a \(\sigma\)-finite measure space and \(\Omega \subset \mathbb{C}\) be a region. For any \(F \in L^1(\Omega \times X)\), if
- \(F(z, x)\) is analytic in \(z\) for any \(x \in X\).
- \(z \mapsto \int_X |F(z, x)| dx\) is uniformly convergent on compact subsets.
then \(f(z) = \int_X F(z, x) dx\) is an analytic function on \(\Omega\).

In particular, item 2 holds if \(F \in C(\Omega \times X)\) and \(X\) is compact.

Proof: This follows from Morera’s theorem (10.5.2.8) and Fubini-Tonelli theorem (10.4.2.7). \( \square \)

Local Properties of Analytic Functions

Prop. (10.5.2.14) [Analytic Functions are Open]. Let \(\Omega \subset \mathbb{C}\) be a region, then any \(f \in \mathcal{O}(\Omega)\) defines an open map \(\Omega \to f(\Omega)\).

Proof: Cf.[Ahlfors, P132] . \( \square \)

Prop. (10.5.2.15) [Taylor Expansions]. Let \(\Omega \subset \mathbb{C}\) be a region and \(f \in \mathcal{O}(\Omega)\), then if \(D \subset \Omega\) be a closed disk with center \(z_0\), then for any \(z \in D\),
\[
f(z) = \sum_{n \in \mathbb{N}} \frac{f^{(n)}(z_0)}{n!} (z - z_0)^n.
\]

Proof: By Cauchy’s integral formula (10.5.2.6), if \(C\) is the boundary of \(D\), then
\[
f(z) = \frac{1}{2\pi i} \int_C \frac{f(\xi)}{\xi - z} d\xi
\]
But
\[
\frac{1}{\xi - z} = \frac{1}{\xi - z_0} \frac{1}{1 - \frac{\xi - z}{\xi - z_0}} = \sum_{n \in \mathbb{N}} \frac{(\xi - z)^n}{(\xi - z_0)^{n+1}}
\]
and the convergence is uniform on \(C\), so by (10.5.2.7),
\[
f(z) = \int_C \left( \frac{1}{2\pi i} \int_C \frac{f(\xi)}{(\xi - z_0)^{n+1}} \right) (\xi - z)^n = \sum_{n \in \mathbb{N}} \frac{f^{(n)}(z_0)}{n!} (z - z_0)^n.
\]
\( \square \)
Cor. (10.5.2.16). For any region $\Omega \subset \mathbb{C}$ and $f \in \mathcal{O}(\Omega)$. If $z_0 \in \Omega$ and $f^{(n)}(z_0) = 0$ for any $n \in \mathbb{N}$, then $f = 0 \in \mathcal{O}(\Omega)$.

Proof: The subset $E = \{z_0 \in \Omega | f^{(n)}(z_0) = 0, \forall n \in \mathbb{N}\}$ is an open subset by the Taylor expansion (10.5.2.15), and the complement is also an open subset as all the derivatives are continuous. So $E = \Omega$, and $\Omega$ is connected.

Def. (10.5.2.17) [Orders of Vanishing]. For any region $\Omega \subset \mathbb{C}$ and $f \neq 0 \in \mathcal{O}(\Omega)$, then for any $z_0 \in \Omega$, there exists some $n$ s.t. $f^{(n)}(z_0) \neq 0$. So by (10.5.3.3) and (10.5.2.15),

$$f(z) = (z-z_0)^n f_n(z)$$

on a nbhd of $z_0$, where $f_n \in \mathcal{O}(\Omega')$ and $f_n(z_0) \neq 0$ for some nbhd $\Omega'$ of $z_0 \in \Omega$. Such an $n$ is called the order of vanishing of $f$ at $z_0$.

In particular, if $n > 0$, $f_n(z) \neq 0$ on a nbhd of $z_0$, so $f(z) \neq 0$ on nbhd of $z_0$, thus the vanishing point of $f$ is isolated in $\Omega$.

Cor. (10.5.2.18) [Uniqueness]. If the zeros of a holomorphic function $f$ has a convergent point in the domain of definition, then $f = 0$. In particular, if $f, g \in \mathcal{O}(\Omega)$ satisfies $f(z) = g(z)$ for any $z \in E$, where $E \subset \Omega$ is a subset with convergence points in $\Omega$, then $f = g \in \mathcal{O}(\Omega)$.

Prop. (10.5.2.19) [Removable Singularities]. Let $\Omega \subset \mathbb{C}$ and $\Omega'$ is the region obtained from $\Omega$ by omitting f.m. points $\zeta_i$, $f \in \mathcal{O}(\Omega')$, then $f$ can be extended to an analytic function $f \in \mathcal{O}(\Omega)$ iff $\lim_{z \to \zeta_i} (z-\zeta_i) f(z) = 0$ for each $i$.

Proof: The necessary is clear. For the other direction, choose for each $\zeta_i$ a disk $D(\zeta_i, \delta)$ contained in $\Omega$ with boundary $\gamma$, then for any $z_0 \in D(\zeta_i, \delta)$, by Cauchy theorem (10.5.2.2) applied to the analytic function $F(z) = \frac{f(z)-f(z_0)}{z-z_0}$ on $D(z_0, \delta') \setminus \{z_0, \zeta_i\}$, we see

$$\int_{\gamma} \frac{f(\xi)}{\xi-z_0} d\xi = \int_{\gamma} \frac{f(z_0)}{\xi-z_0} = f(z_0)(10.5.2.5).$$

But by (10.5.2.4), $z \mapsto \int_{\gamma} \frac{f(\xi)}{\xi-z_0} d\xi$ is a holomorphic function on $D(\zeta_i, \delta)$, and it extends $f(z_0)$. So $f$ can be extended to an analytic function $f \in \mathcal{O}(\Omega)$.

Prop. (10.5.2.20) [Singularities]. If $\Omega \subset \mathbb{C}$ is region and $\Omega'$ is the region obtained from $\Omega \setminus E$ where $E = \{\zeta_1, \ldots, \zeta_n, \ldots\} \subset \Omega$ is a discrete subset. Suppose $f \in \mathcal{O}(\Omega')$, then $f$ is said to have a singularity at $\zeta_i$. For each $i$, let $\zeta = \zeta_i$, the following are the all the cases:

- $\lim_{z \to \zeta} |z-\zeta|^\alpha |f(z)| = 0$ for any $\alpha \in \mathbb{R}$. In this case, $f = 0 \in \mathcal{O}(\Omega)$.
- there exists $h \in \mathbb{R}$ s.t. $\lim_{z \to \zeta} |z-\zeta|^\alpha |f(z)| = \begin{cases} 0, & \alpha < h \\ \infty, & \alpha > h \end{cases}$. In this case, $h \in \mathbb{Z}$, and $z_0$ is called a zero of $f$ if $h > 0$ and pole of $f$ if $h < 0$. And if $h = 0$, it is called a removable singularity, which is discussed in (10.5.2.19).
- Neither of the above holds. In this case, $z_0$ is called a essential singularity of $f$.

Proof: In case 1, $f$ can be extended to a function on $\Omega' \cup \{\zeta\}$ with $f(\zeta) = 0$ by (10.5.2.19), and at this point, all the derivatives of $f$ vanish by (10.5.2.17), so $f = 0 \in \mathcal{O}(\Omega)$ by (10.5.2.18).

In case 2, $|z-\zeta|^m |f(z)| = 0$ for some $m \in \mathbb{Z}$ larger than $h$, so $(z-\zeta)^m f(z)$ can be extended to a function on $\Omega' \cup \{\zeta\}$. As $f$ is not identically zero, $(z-\zeta)^m f(z)$ has a finite order of vanishing at $\zeta$, so $(z-\zeta)^m f(z) = (z-\zeta)^k f_k(z)$ for some $k \in \mathbb{Z}$ on a nbhd of $\zeta$ by (10.5.2.17), so $f(z) = (z-\zeta)^{k-m} f_k(z)$, so clearly $h$ is an integer.
Def. (10.5.2.21). Situation as in (10.5.2.20), if all the singularities of $f$ on $\Omega$ are zeros or poles, $f$ is called a meromorphic function on $\Omega$. Notice the poles and zeros of $f$ are discrete. The space of meromorphic functions on $\Omega$ is denoted by $\mathcal{M}(\Omega)$. $\mathcal{M}(\Omega)$ is a field.

Prop. (10.5.2.22) [Maximum Principle]. Let $f(z)$ be analytic and non-constant on a region $\Omega$, then its absolute value attains no minimum or maximum on $\Omega$.

Proof: This follows easily from Cauchy’s integral formula (10.5.2.6).

Prop. (10.5.2.23) [Schwartz Lemma]. If $f \in \mathcal{O}(\mathbb{D})$ and satisfies $|f(z)| \leq 1$, $f(0) = 0$, then $|f(z)| \leq |z|$, and $|f'(0)| \leq 1$. Moreover, if $|f(z)| = |z|$ for some $z$ or $|f'(0)| = 1$, then $f(z) = cz$ where $|c| = 1$.

Proof: The function $g(z) = f(z)/z$ is analytic on $0 < |z| < 1$ with a removable singularity at $0$ (10.5.2.19) and extends to an analytic function on $|z| < 1$ with $g(0) = f'(0)$, and $\lim_{|z| \to 1} |g(z)| \leq 1$, thus by maximal principle (10.5.2.22), $|g(z)| \leq 1$ for any $|z| < 1$, thus we are done. The last assertion also follows from (10.5.2.22).

Residues

Def. (10.5.2.24) [Residues]. If $\Omega \subset \mathbb{C}$ is a simply-connected region and $f$ is a function on $\Omega$ analytic except for isolated singularities $\{a_j\}$, then for each $i$, if $\mathcal{D}(a_i, \delta)$ is a nbhd of $a_i$ contained in $\Omega$ and contains no other singularities of $f$, then define

$$\text{res}_{z=a_i} f = \frac{1}{2\pi i} \int_\gamma f(z) dz,$$

where $\gamma = \partial \mathcal{D}(a_i, \delta)$. This quantity is invariant of the nbhd chosen by Cauchy’s theorem (10.5.2.2), and is called the residue of $f$ at $a_i$.

Thm. (10.5.2.25) [Residue theorem]. If $\Omega \subset \mathbb{C}$ is a simply-connected region and $f$ is a function on $\Omega$ analytic except for isolated singularities $\{a_j\}$, then for any piecewise $C^1$ closed curve $\gamma \subset \Omega$ not passing through the singularities,

$$\frac{1}{2\pi i} \int_\gamma f(z) dz = \sum_i n(\gamma, a_i) \text{res}_{z=a_i} f,$$

where the RHS is a finite sum.

Proof: This is because the interior of $\gamma$ contains only f.m. singularity points, and $\gamma$ is homologous to a linear combination of cycles around each singularity with multiplicity $n(\gamma, a_i)$.

Prop. (10.5.2.26). If $\Omega \subset \mathbb{C}$ is a region and $f$ is a function on $\Omega$ analytic with singularities. If $f$ is analytic around $z_0 \in \Omega$, then for $n \in \mathbb{Z}_+$, by (10.5.2.7),

$$\text{res}_{z=z_0} f(z) (z-z_0)^{-n} = \frac{f^{(n-1)}(z_0)}{(n-1)!}.$$

Prop. (10.5.2.27) [Argument Principle]. If $\Omega \subset \mathbb{C}$ is a simply-connected region and $f \in \mathcal{M}(\Omega)$ with zeros $\{a_i\}$ and poles $\{b_j\}$, then for any piecewise $C^1$ closed curve $\gamma \subset \Omega$ not passing through zeros or poles,

$$\frac{1}{2\pi i} \int_\gamma \frac{f'(z)}{f(z)} dz = \sum_i n(\gamma, a_i) - \sum_j n(\gamma, b_j)$$
where the RHS is a finite sum, and counted with multiplicity by the order.

Notice if $\Gamma$ is the closed curve $f \circ \gamma$, then

$$\frac{1}{2\pi i} \int_{\gamma} \frac{f'(z)}{f(z)} \, dz = \frac{1}{2\pi i} \int_{\Gamma} \frac{1}{z} \, dz = n(\Gamma, 0).$$

**Proof:** Notice if $z_0 \in \Omega$ and $f(z) = (z - z_0)^h f_h(z)$ near $z_0$ where $h \in \mathbb{Z}$, $f_h(z)$ is analytic on a nbhd of $z_0$ and $f_h(z_0) = 0$, then

$$\frac{f'(z)}{f(z)} = \frac{h}{z - z_0} + f_h'(z),$$

so $\text{res}_{z=z_0} \frac{f'}{f} = h$ by (10.5.2.2) and (10.5.2.5). Thus the assertion follows from the residue formula (10.5.2.25) applied to the meromorphic function $F = f'/f \in \mathcal{M}(\Omega)$. □

**Cor. (10.5.2.28) [Rouché].** If $\Omega \subset \mathbb{C}$ is a region and $\gamma \subset \Omega$ is a piecewise $C^1$ closed curve that is a boundary of a subset of $\Omega$ homeomorphic to a $\mathbb{D}$. Suppose $f, g \in \mathcal{O}(\Omega)$ satisfies $|f(z) - g(z)| < |f(z)|$ for $z \in \gamma$, then $f(z)$ and $g(z)$ have the same number of zeros or poles on the boundary of $\gamma$.

**Proof:** This follows from the argument principle (10.5.2.27) applied to the meromorphic function $F = f/g \in \mathcal{M}(\Omega)$. Notice that $n(\gamma, a) = 1$ for any $a$ in the interior of $\gamma$, and $n(F \circ \gamma, 0) = 0$ because $|F(z) - 1| < 1$ for $z \in \gamma$ by hypothesis. □

### 3 Series and Product Developments

**Prop. (10.5.3.1) [Abel-Hadamard].** For any power series $a_0 + a_1 z + \ldots + a_n z^n + \ldots$ in $\mathbb{C}$, take $1/R = \lim_{n\to\infty} |a_n|^{1/n}$, where we assume $1/0 = \infty$ and $1/\infty = 0$,

- The series converges absolutely for every $|z| < R$, and if $\rho < R$, then the convergence is uniform for $|z| \leq \rho$.

- If $|z| > R$, the terms are unbounded, and the series diverges.

And $R$ is called the radius of convergence of the sequence. Notice the radius of convergence is the same as that of $|a_0| + |a_1| |z| + \ldots + |a_n| |z^n| + \ldots$ in $\mathbb{R}$ (10.4.4.1).

**Proof:** 1: For $0 < \rho < R$, take $\rho_1 \in (\rho, R)$, then the definition of $R$ implies that for some $N \in \mathbb{Z}^+$ and any $n \geq N$, $|a_n| \leq R^{-n} < \rho_1^{-n}$, so $|a_n z^n| \leq (\rho/\rho_1)^n$, so $\sum_{n \in \mathbb{N}} a_n z^n$ converges absolutely and uniformly for $|z| \leq \rho$.

2: For $R < |z|$, the definition of $R$ implies that for any $N \in \mathbb{Z}^+$, there exists $n \geq N$ s.t. $|a_n| \geq R^{-n}$, so $|a_n z^n| \geq |z/R|^n > 1$, so this sequence cannot be convergent. □

**Cor. (10.5.3.2).** By (10.4.4.3) and (10.5.3.1), for any power series $a_0 + a_1 x + \ldots + a_n x^n + \ldots$ in $\mathbb{R}$, if

$$\lim_{n \to \infty} \frac{|a_{n+1}|}{|a_n|} = \rho \in [0, \infty],$$

then the radius of convergence (10.5.3.1) $R = 1/\rho$, where we assume $1/0 = \infty$ and $1/\infty = 0$.

**Prop. (10.5.3.3).** The power series $a_0 + a_1 z + \ldots + a_n z^n + \ldots$ defines an analytic function $f(z)$ on its disk of convergence. And also

$$f'(z) = \sum_{n \in \mathbb{N}} n a_n z^{n-1}.$$

In particular, $f(z)$ is infinite differentiable in its disk of convergence.
Proof: The sequence $\sum_{n \in \mathbb{N}} n a_n z^{n-1}$ has the same radius of convergence $R$ as $\sum_{n \in \mathbb{N}} a_n z^n$ by (10.5.3.1) and the fact $\lim n^{1/n} = 1$ (10.4.6.4). Denote $g(z) = \sum_{n \in \mathbb{N}} n a_n z^{n-1}$ for $|z| < R$.

For $|z_0| < \rho < R$, let $f(z) = s_N(z) + r_N(z)$, where

$$s_n(z) = \sum_{n=0}^{N} a_n z^n, \quad r_N(z) = \sum_{n=N+1}^{\infty} a_n z^n,$$

then for $|h| < \rho - |z|$,

$$\frac{f(z_0 + h) - f(z_0)}{h} - g(z_0) = \left[ \sum_{n=N+1}^{\infty} a_n \right] \frac{\left( z_0 + h \right)^n - z_0^n}{h} - \left[ s_N(z_0) + r_N(z_0) \right],$$

and

$$\frac{r_N(z_0 + h) - r_N(z_0)}{h} \leq \sum_{n=N+1}^{\infty} |a_n| \left| \frac{\left( z_0 + h \right)^n - z_0^n}{h} \right| \leq \sum_{n=N+1}^{\infty} n |a_n| r^{n-1}.$$ 

As $g(z)$ is absolutely convergent on $|z| < R$ by (10.5.3.1), $\lim_{N \to \infty} \frac{r_N(z_0+h) - r_N(z_0)}{h} = 0$.

Also we have $s'_N(z_0) \to g(z_0)$, so for any $\varepsilon > 0$, we can find $N \in \mathbb{Z}$ s.t.

$$\left| \frac{r_N(z_0 + h) - r_N(z_0)}{h} \right| \leq \varepsilon, \quad |s'_N(z_0) - g(z_0)| < \varepsilon.$$

Then for this $N$, if $|h|$ is small, then $|s_N(z_0 + h) - s_N(z_0)| < \varepsilon$, so when $|h|$ is small,

$$\left| \frac{f(z_0 + h) - f(z_0)}{h} - g(z_0) \right| < 3\varepsilon,$$

which proves that $f'(z) = g(z)$.

□

Prop. (10.5.3.4) [Infinite Products]. For $(b_n) \in \mathbb{C} \setminus \{-1\}$, the infinite product $\prod_{n \in \mathbb{Z}^+} (1 + b_n)$ is said to converge if the sequence

$$\Pi_m = \prod_{n=1}^{m} (1 + b_n)$$

converges. It is said to converge absolutely if $\prod_{n \in \mathbb{Z}^+} (1 + |b_n|)$ converges.

Then $\prod_{n \in \mathbb{Z}^+} (1 + b_n)$ converges absolutely iff $\sum_{n \in \mathbb{Z}^+} b_n$ converges absolutely.

Proof: Notice

$$1 + \sum_{n=1}^{m} |b_n| \leq \prod_{n=1}^{m} (1 + |b_n|) \leq \exp\left( \sum_{n=1}^{m} |b_n| \right)$$

□

Prop. (10.5.3.5). Any holomorphic function $f$ defined on the punctured disk $0 < |z| < 1$ is of the form

$$f(z) = \sum_{n \in \mathbb{Z}} a_n z^n$$

where $\lim_{n \to \infty} |a_n|^{1/n} \leq 1$, and $\lim_{n \to \infty} |a_{-n}|^{1/n} = 0$.

Proof:

□
Prop. (10.5.3.6). If \( f \in C((0, 1]) \) has an expansion
\[
f(x) = \sum_{\nu \in \Sigma} a(\nu) x^\nu
\]

near \( x = 0 \), where \( \Sigma \subset \mathbb{R} \) is a discrete subset bounded from below, then
\[
\int_0^1 f(x) x^s \frac{dx}{x}
\]

has meromorphic continuation to all \( s \in \mathbb{C} \), and has only simple poles at \( s \in -\Sigma \), and the residue at \( s = -\nu \) is \( a(\nu) \). Moreover, for any \( N \in \mathbb{R} \), \( f \) is essentially bounded on \( \text{Re}(s) > -N \).

**Proof:** For any \( N \in \mathbb{R} \), let
\[
f(x) = \sum_{\nu \in \Sigma, \nu < N} a(\nu) x^\nu + R(x), \quad R(x) = O(x^N),
\]

then
\[
\int_0^1 f(x) x^s \frac{dx}{x} = \sum_{\nu \in \Sigma, \nu < N} \frac{a(\nu)}{s + \nu} + \int_0^1 R(x) x^s \frac{dx}{x}.
\]

\( \square \)

Prop. (10.5.3.7) [Trigonometric Functions]. The exponential function
\[
\exp(z) = \sum_{n \in \mathbb{N}} \frac{z^n}{n!} (7.5.1.5)
\]
is convergent and analytic on \( \mathbb{C} \), by (10.5.3.1), and it is also denoted by \( e^z \). We can also define the trigonometric functions
\[
cos(z) = \frac{e^{iz} + e^{-iz}}{2} = \sum_{n \in \mathbb{N}} (-1)^n \frac{z^{2n}}{(2n)!}, \quad \sin(z) = \frac{e^{iz} - e^{-iz}}{2i} = \sum_{n \in \mathbb{N}} (-1)^n \frac{z^{2n+1}}{(2n+1)!},
\]
which are analytic on \( \mathbb{C} \).

Prop. (10.5.3.8). If \( \Omega \) is a simply-connected region and \( f \in O(\Omega) \) is non-vanishing, then it is possible to define single-valued holomorphic functions \( \log f \) and \( \sqrt[n]{f} \) on \( \Omega \).

**Proof:** By (10.5.2.3), there exists a function \( F \in O(\Omega) \) s.t. \( F'(z) = f'(z)/f(z) \). Then \( f(z)e^{-F(z)} \) has derivative 0 and thus a constant function by (10.5.1.10). Choose \( z_0 \in \Omega \) and choose one of the values of \( \log f(z_0) \), then
\[
e^{F(z)-F(z_0)+\log f(z_0)} = f(z)
\]
so we can choose \( \log f = F - F(z_0) + \log f(z_0) \). And then we can define \( \sqrt[n]{f} = \exp(\frac{1}{n} \log f) \). \( \square \)

Prop. (10.5.3.9) [Eulerian Identity]. The smallest positive real number \( \rho \) that \( e^{i\rho} + 1 = 0 \) is \( \pi \). In particular, the Eulerian identity \( e^{\pi i} + 1 = 0 \) holds.

**Proof:**
Entire Functions

Def. (10.5.3.10) [Bernoulli Numbers]. The Bernoulli numbers $B_k$, $k \geq 0$ are defined to be

$$\frac{x}{e^x - 1} = \sum_{k=0}^{\infty} B_k \frac{x^k}{k!}.$$  

Then $B_k$ are all rational numbers, and

$$B_0 = 1, B_1 = -\frac{1}{2}, B_{2k+1} = 0 (k \geq 1), B_2 = \frac{1}{6}, B_4 = -\frac{1}{30}, B_6 = \frac{1}{42}, B_8 = -\frac{1}{30}.$$  

More numbers can be found at [https://oeis.org/wiki/Bernoulli_numbers](https://oeis.org/wiki/Bernoulli_numbers).

Prop. (10.5.3.11).

$$\sin(z) = z \prod_{n=1}^{\infty} \left(1 - \frac{z^2}{n^2 \pi^2}\right).$$  

Proof: □

Cor. (10.5.3.12).

$$z \cot(z) = 1 + 2 \sum_{n=1}^{\infty} \frac{z^2}{n^2 \pi^2} = 1 - 2 \sum_{k=1}^{\infty} \zeta(2k) \frac{z^{2k}}{\pi^{2k}}.$$  

Proof: Taking the logarithmic derivative of the equation in (10.5.3.11). □

4 Analytic Continuations

Lemma (10.5.4.1) [Symmetry Principle]. If $\Omega \subset \mathbb{C}$ is a region s.t. $e(\Omega) = \Omega$, denote $\Omega^+ = \Omega \cap \mathcal{H}$, $\Omega^- = e(\Omega^+)$, $I = \Omega \cap \mathbb{R}$. Suppose $f^+ \in \mathcal{O}(\Omega^+), f^- \in \mathcal{O}(\Omega^-)$, and $f^+(z) = f^-(z)$ for $z \in \mathbb{R}$, then the function

$$f : \Omega \to \mathbb{C} : z \mapsto \begin{cases} f^+(z), & z \in \overline{\Omega^+} \\ f^-(z), & z \in \Omega^- \end{cases}$$

is analytic on $\Omega$.

Proof: $f$ is clearly continuous. Thus it is easily seen to be analytic by Morera’s theorem (10.5.2.8). □

Prop. (10.5.4.2) [Schwarz Reflection Principle]. If $\Omega \subset \mathbb{C}$ is a region s.t. $e(\Omega) = \Omega$, denote $\Omega^+ = \Omega \cap \mathcal{H}$, $\Omega^- = e(\Omega^+)$, $I = \Omega \cap \mathbb{R}$. Suppose $f^+ \in \mathcal{O}(\Omega^+)$ satisfies $f(I) \subset \mathbb{R}$, then $f^+$ can be analytically extended to an analytic function on $\Omega$.

Proof: For $z \in \Omega^-$, define $f(z) = \overline{f(\overline{z})}$, then $f$ is a continuous function on $\Omega$, because for $z \in I$, $f(z) = \overline{f(\overline{z})}$. To show that $f$ is analytic, by (10.5.4.1), it suffices to show that $f$ is analytic on $\Omega^-$. For any $z_0 \in \Omega^-$, if $z$ is close to $z_0$, then $\overline{z}, \overline{z_0} \in \Omega^+$. By Taylor expansion of $f$ around $\overline{z}_0$ (10.5.2.15)

$$f(z) = \overline{f(\overline{z})} = \sum_{n \in \mathbb{N}} a_n (\overline{z} - \overline{z}_0)^n = \sum_{n \in \mathbb{N}} \overline{a_n} (z - z_0)^n.$$  

And this is a power series around $z_0$ with the same radius of convergence as that of $\overline{z}_0$, thus $f$ is analytic around $z_0$. Because $z_0$ is arbitrary, $f$ is analytic on $\Omega^-$. □
Cor. (10.5.4.3). If $\Omega \subset \mathbb{C}^x$ is a region that is stable under the involution $\iota : z \mapsto \overline{z}^{-1}$, denote $\Omega^+ = \Omega \cap \mathcal{H}$, $\Omega^- = \iota(\Omega^+)$, $I = \Omega \cap \partial \mathbb{D}$. Suppose $f^+ \in \mathcal{O}(\Omega^+)$ satisfies $f(I) \subset \mathbb{R}$, then $f^+$ can be analytically extended to an analytic function on $\Omega$.

Proof: For $z \in \Omega^-$, define $f(z) = \overline{f(\iota(z))}$, then $f$ is a continuous function on $\Omega$, because for $z \in I$, $f(z) = \overline{f(\iota(z))}$. To show that $f$ is analytic, by a similar lemma as (10.5.4.1), it suffices to show that $f$ is analytic on $\Omega^-$: For any $z_0 \in \Omega^-$, if $z$ is close to $z_0$, then $\iota(z), \iota(z_0) \in \Omega^+$. By Taylor expansion of $f$ around $\iota(z_0)$ (10.5.2.15)

$$f(z) = f(\iota(z)) = \sum_{n \in \mathbb{N}} a_n(\iota(z) - \iota(z_0))^n = \sum_{n \in \mathbb{N}} \overline{a_n} \frac{(z - z_0)^n}{z^n} = g\left(\frac{1}{z}\right),$$

where $g(z) = \sum_{n \in \mathbb{N}} (-1)^n a_n (z - \frac{1}{z_0})^n$ is a power series around $z_0$ with the same radius of convergence as that of $\overline{z}_0$, so analytic around $\overline{z}_0^{-1}$. Thus $f$ is analytic around $z_0$. Because $z_0$ is arbitrary, $f$ is analytic on $\Omega^-$.

5 Theorems

Prop. (10.5.5.1) [Uniformization Theorem]. Any connected Riemann Surface is the quotient by a discrete subgroup of $\mathbb{C}, \mathcal{H}$ or $\mathbb{P}^1$.

Proof: □

Prop. (10.5.5.2) [Runge’s Theorem]. Let $K$ be a compact subset of $\overline{\mathbb{C}}$ and let $f$ be a function which is holomorphic on an open set containing $K$. If $A$ is a set containing at least one complex number from every bounded connected component of $\overline{\mathbb{C}} \setminus K$, then there exists a sequence of rational functions which converges uniformly to $f$ on $K$ and all the poles of the functions are in $A$.

Proof: □

Prop. (10.5.5.3) [Mergelyan’s theorem]. If $K$ is compact in $\mathbb{C}$ and $f$ is a continuous function on $K$ that is holomorphic in $\text{int}(K)$, then $f$ can be uniformly approximated by polynomials.

Prop. (10.5.5.4) [Weierstrass Theorem]. For a ascending sequence of regions $\Omega_1 \subset \Omega_2 \subset \ldots$, $\cup_n \Omega_n = \Omega$, and $f_n$ is analytic on $\Omega_n$, and $f_n(z)$ converges to a function $f(z)$ in the compact-open topology, then $f(z)$ is also analytic, and moreover, $f'(z)$ converges to $f'(z)$ in the compact-open topology.

Proof: The analyticity follows from Morera’s theorem (10.5.2.8) as the integration on a closed curve commutes with uniform convergence, the same argument applied to the limit of equations

$$f_n'(z) = \frac{1}{2\pi i} \int_{\partial D(0, r)} \frac{f_n(\zeta)d\zeta}{(\zeta - z)^2}$$

shows that the derivative also converges, and uniformly on $\overline{D(0, \rho)}$ for $\rho < r$. □

Cor. (10.5.5.5) [Hurwitz]. Cf. [Ahlfors P178].

Prop. (10.5.5.6) [Montel’s Theorem]. Sets of holomorphic functions bounded in the topology of $H(\Omega)$, inter convex uniform convergence, is sequentially compact.
Proof:

Thm. (10.5.5.7) [Little Picard Theorem]. The image of a non-constant entire function \( f : \mathbb{C} \to \mathbb{C} \) is either \( \mathbb{C} \) or \( \mathbb{C} \) with one point omitted.

Proof: The modular curve \( Y(2) \) is the sphere minus three points(15.11.2.4)(15.11.4.16)(15.11.4.17), and the linear transformations of \( S^1 \) is triply transitive, thus we can assume \( f \) is an analytic map \( \mathbb{C} \to \mathbb{C} \). As \( \mathbb{C} \) is simply connected, we can lift this map to the covering of \( Y(2) \), which is \( \mathcal{H} \). But \( \mathcal{H} \) is biholomorphic to the open disk, but a bounded entire function is constant(10.5.2.10), so \( f \) is constant.

Thm. (10.5.5.8) [Great Picard Theorem]. If an analytic function \( f \) has an essential singularity at a point \( w \), then on any punctured nbhd of \( w \), \( f \) takes any value infinitely often, except for at most one single exception.

Proof:

Prop. (10.5.5.9) [Phragmén-Lindelöf Principle]. Let \( f \) be a function that is holomorphic in the upper part of a strip \( \sigma_1 \leq \text{Re}(s) \leq \sigma_2, \text{Im}(s) > c \), such that \( f(\sigma + it) = O(e^{\alpha t}) \) for some \( \alpha > 0 \) uniformly for any \( \sigma_1 < \sigma < \sigma_2 \). Suppose further that \( f(\sigma + it) = O(t^b) \) for some \( b \) and \( \sigma = \sigma_1 \) or \( \sigma_2 \), then \( f(\sigma + it) = O(t^b) \) uniformly for \( \sigma_1 \leq \sigma \leq \sigma_2 \).

Proof: First assume that \( b = 0 \), thus there exists \( M \) that \( |\varphi(s)| \leq M \) for \( \text{Re}(s) = \sigma \). Now let \( m \equiv 2 \mod 4 \) and \( m > \alpha \), then \( \text{Re}((\sigma + i\tau)m) \) is a polynomial of \( \sigma \) and \( \tau \) with highest term of \( \tau \) being \(-\tau^m\), so we have

\[
\text{Re}(s^m) = -\tau^m + O(|\tau|^{m-1}), |\tau| \to \infty
\]

uniformly on the strip. So \( \text{Re}(s^m) \) has an upper bound \( N \) on the strip. Thus for any \( \varepsilon > 0 \),

\[
|\varphi(s)e^{\varepsilon s^m}| \leq Me^{\varepsilon N}
\]
on the boundary of the strip and

\[
|\varphi(s)e^{\varepsilon s^m}| = O(e^{\alpha|\tau|^n - \varepsilon \tau^m})
\]
uniformly on the strip, thus converges uniformly to 0 as \( |\text{Im}(s)| \to \infty \).

Then we can use maximum principle to see that

\[
|\varphi(s)e^{\varepsilon s^m}| \leq Me^{\varepsilon N}
\]
on the strip. Let \( \varepsilon \to 0 \), we get \( |\varphi(s)| \leq M \), thus the theorem.

In general, if \( b \neq 0 \), define \( \psi(s) = (s - \sigma_1 + 1)^b \), then \( |\psi(s)| = |s - \sigma_1 + 1|^b \sim |\tau|^b \) when \( |\tau| \to \infty \). Thus \( \varphi_1(s) = \varphi(s)/\psi(s) \) satisfies the same condition as \( \varphi \) with \( b = 0 \), so \( \varphi(s)/\psi(s) \) is bounded on the strip, and thus \( |\varphi(s)| = O(|\tau|^b) \).

Remark (10.5.10). Some condition on the growth rate of \( |f(\sigma + it)| \) is necessary, otherwise we can consider \( e^{it} \) on the strip \(-\frac{\pi}{2} \leq \text{Re}(z) \leq \frac{\pi}{2} \), then it is bounded for \( \text{Re}(z) = \pm \frac{\pi}{2} \), but not bounded for \(-\frac{\pi}{2} < \text{Re}(z) < \frac{\pi}{2} \).
6 Harmonic Functions

Def. (10.5.6.1) [Harmonic Functions]. A real-valued function on a region \( \Omega \subset \mathbb{C} \) is called harmonic if it is \( C^1 \) and has second order derivatives and \( \Delta u = (\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2})u = 0 \) holds. This is an elliptic differential operator, so \( u \) is automatically smooth, by (10.11.8.4).

The vector space of Harmonic functions on \( \Omega \) is denoted by \( H(\Omega) \subset C^\infty(\Omega) \).

Prop. (10.5.6.2). If \( \Omega \subset \mathbb{C} \) is a region and \( z \in \Omega \), \( f \in \mathcal{O}(\Omega) \), \( f(z) \neq 0 \), then \( \log |f| \in H(\Omega) \).

Proof: \( \square \)

Prop. (10.5.6.3) [Schwarz’s Theorem]. Cf. [Ahlfors P169].

Def. (10.5.6.4) [Mean-Value Property]. A real valued function \( u \) on a region \( \Omega \) is said to have the mean-value property iff

\[
\frac{1}{2\pi} \int_0^{1\pi} u(z_0 + re^{i\theta})d\theta
\]

whenever \( D(z_0, r) \subset \Omega \).

Lemma (10.5.6.5) [Harmonic Mean Value]. If \( u \) is a Harmonic function between two concentric circles, then the arithmetic mean of it over circles \( |z| = r \) is a linear function of \( \log r \):

\[
\frac{1}{2\pi} \int_{|z|=r} ud\theta = \alpha \log r + \beta.
\]

In particular, if \( u \) is harmonic in the disk, then by continuity, \( \alpha = 0 \), and the mean value is a constant.

Proof: Cf. [Ahlfors P165]. \( \square \)

Prop. (10.5.6.6) [Harmonicity and Mean-Value Property]. A harmonic function satisfies the mean-value property, and conversely, and continuous function satisfying the mean-value property is harmonic.

Proof: Harmonic function satisfies the mean-value property by (10.5.6.5). Conversely, for any \( z_0 \), by Schwarz’s theorem (10.5.6.3), there is a harmonic function \( v(z) \) that is harmonic in \( D(z_0, \rho) \) and equals \( u(z) \) on \( \partial B(z_0, \rho) \). Now the maximal and minimal principles apply to \( u - v \), thus \( u = v \) is harmonic. \( \square \)

Cor. (10.5.6.7) [Maximum Principle]. If \( u \) is a harmonic function, then it attains neither maximum nor minimum at its region of definition.

Prop. (10.5.6.8) [Harmonic Functions as the Real Parts of Analytic Functions]. Let \( \Omega \subset \mathbb{C} \) be a simply-connected region, \( u \in H(\Omega) \), then there exists \( f \in \mathcal{O}(\Omega) \) s.t. \( \text{Re} f = u \). And any two such \( f \) differ by a purely imaginary constant.

Proof: Let \( g(z) = 2\frac{\partial}{\partial x}u \), then \( \frac{\partial}{\partial x}g = 2\frac{\partial}{\partial x}\frac{\partial}{\partial z}u = \frac{1}{2}\Delta u = 0 \), so \( g \in \mathcal{O}(\Omega) \). Then by (10.5.2.3), there exists \( f \in \mathcal{O}(\Omega) \) s.t. \( \frac{\partial}{\partial z}f = g = 2\frac{\partial}{\partial x}u \). So

\[
2\frac{\partial}{\partial x}f = \frac{\partial}{\partial x}\text{Re} f + \frac{\partial}{\partial y}\text{Im} f = 2\frac{\partial}{\partial x}\text{Re} f, \quad 2\frac{\partial}{\partial y}u = \frac{\partial}{\partial y}\text{Re} f - \frac{\partial}{\partial x}\text{Im} f = 2\frac{\partial}{\partial y}\text{Re} f.
\]

So \( u - \text{Re} f \) is a constant function. And we may modify \( f \) to make \( \text{Re} f = u \). For the last assertion, use the Cauchy-Riemann equations to show that \( \frac{\partial}{\partial x}(\text{Im} f - \text{Im} f') = \frac{\partial}{\partial y}(\text{Im} f - \text{Im} f') = 0 \), so \( \text{Im} f - \text{Im} f' \) is a constant function. \( \square \)
Prop.(10.5.6.9)[Poisson Formula]. For \( u \in \mathcal{H}(\overline{D}(0,R)) \),
\[
 u(z) = \frac{1}{2\pi} \int \frac{R^2 - |z|^2}{|Re^i\theta - z|^2} u(\rho e^{i\theta})d\theta = \text{Re} \left[ \frac{1}{2\pi i} \int_{|\zeta|=R} \frac{\zeta + z}{\zeta - z} u(\zeta) \frac{d\zeta}{\zeta} \right].
\]
for \( z \in \mathbb{D}(0,R) \).

In particular, for any \( f \in \mathcal{O}(\overline{D}(0,R)) \), for \( z \in \mathbb{D}(0,R) \):
\[
f(z) = \frac{1}{2\pi i} \int_{|\zeta|=\rho} \frac{\zeta + z}{\zeta - z} \text{Re}(f(\zeta)) \frac{d\zeta}{\zeta} + iC.
\]

Proof: This follows from (10.5.6.8) and (10.5.2.12).

Prop.(10.5.6.10)[Hadamard’s Three Circle Theorem]. Let \( f(z) \) be analytic in the annulus \( r_1 < |z| < r_2 \), and continuous on the boundary, if \( M(r) \) denotes the maximum of \( |f(z)| \) for \( |z| = r \), then:
\[
 M(r) \leq M(r_1)^\alpha M(r_2)^{1-\alpha}
\]
where \( \alpha = \log(r_2/r) : \log(r_2/r_1) \).

Proof: Apply the maximum principle (10.5.6.7) for
\[
g(z) = \log |f(z)| - \log(M(r_1)(\log(r_2/|z|) : \log(r_2/r_1)) - \log(M(r_2))(1 - \log(r_2/|z|) : \log(r_2/r_1)),
\]
it is harmonic by (10.5.6.2), then \( g(z) \leq 0 \) on \( |z| = r_1 \) and \( |z| = r_2 \), so \( g(z) \leq 0 \) on all the annulus.

Cor.(10.5.6.11). Let \( f(z) \) be analytic in the annulus \( r_1 < |z| < r_2 \), then the function
\[
s \mapsto \max_{|z|=e^s} |f(z)|
\]
is convex on the interval \([\log(a), \log(b)]\).

Prop.(10.5.6.12)[Reflection Principle].

Prop.(10.5.6.13)[Harnack’s Inequality]. For a positive harmonic function \( u \) on \( B(0,\rho) \),
\[
\frac{\rho - |z|}{\rho + |z|} u(0) \leq u(z) \leq \frac{\rho + |z|}{\rho - |z|} u(0).
\]

Proof: By Poisson formula,
\[
u(z) = \frac{1}{2\pi} \int \frac{\rho^2 - |z|^2}{|\rho e^{i\theta} - z|^2} u(\rho e^{i\theta})d\theta
\]
for \( |z| < \rho \), so the conclusion follows from the obvious inequality
\[
\frac{\rho - |z|}{\rho + |z|} \leq \frac{\rho^2 - |z|^2}{|\rho e^{i\theta} - z|^2} \leq \frac{\rho + |z|}{\rho - |z|}
\]
and Mean-value property (10.5.6.6).

□
Cor. (10.5.6.14). If $E$ is a compact subset of a region $\Omega$, there is a constant $M$, depending on $E, \Omega$ that for any positive harmonic function $u(z)$ on $\Omega$, $u(z_2) \leq Mu(z_1)$ for any $z_1, z_2 \in E$.

Proof: This is an easy consequence of Harnack inequality and the compactness of $E$. □

Cor. (10.5.6.15) [Harnack’s Principle]. Consider a sequence of functions $u_n(z)$, each harmonic in a region $\Omega_n$, and there is a region $\Omega$ that every point has a nbhd that is contained in all but f.m. $\Omega_n$, and in this nbhd $u_n(z) \leq u_{n+1}(z)$ for $n$ large, then either $u_n(z)$ tends to $+\infty$ in the compact open topology, or they tends to a harmonic function in compact open topology.

Proof: The uniform continuity follows easily from Harnack’s inequality, and for the harmonicity of the limit function $u(z)$ is a consequence of the Poisson formula. □

**Dirichlet Problem**

**Miscellaneous**

Def. (10.5.6.16) [L²(\mathbb{D}, \nu_k) Unit Disc]. Define a density $\nu_k = \frac{4(1-|w|^2)^{k-2}dudv}{|1-w|^2}$ (k ≥ 2) on $\mathbb{D}$ and define $L^2(\mathbb{D}, \nu_k)$ to be the space of holomorphic functions on $\mathbb{D}$ that is $L^2(\nu_k)$ bounded. Then the space $L^2(\mathbb{D}, \nu_k)$ is complete.

Proof: By (10.5.2.11), the uniform norm is bounded by the local $L^1$-norm hence also the local $L^2$-norm. Hence for a compact subset $K$, the uniform norm is also bounded by $L^2(\nu_k)$-norm. Thus any Cauchy sequence in $L^2(\mathbb{D}, \nu_k)$ converges to a holomorphic function by Weierstrass theorem (10.5.5.4). □

Prop. (10.5.6.17). The space $L^2(\mathbb{D}, \nu_k)$ has an orthogonal basis consisting of holomorphic functions

\[ \{ \psi_n = w^n(1 - w)^k \}_{n \geq 0}. \]

Proof: Firstly, $\psi_n$ is convergent: In the polar coordinate, $\nu_k = \frac{4(1-r^2)^{k-2}rdrd\theta}{|1-w|^2}$, so

\[ ||\psi_n||^2 = 4 \int_0^{2\pi} \int_0^1 r^{2n}(1 - r^2)^{k-2}drd\theta < \infty. \]

And if $m \neq n$,

\[ \int_\mathbb{D} \psi_m(w)\overline{\psi_n}(w)dw = 4 \int_\mathbb{D} w^m(\overline{w})^n(1 - r^2)^{k-2}drd\theta = 4 \int_0^1 r^{m+n}(1 - r^2)^{k-2} \int_0^{2\pi} e^{i(m-n)\theta}d\theta = 0. \]

Def. (10.5.6.18) [Upper Half Plane \( \mathcal{H} \)]. On the upper half plane $\mathcal{H}$, we can define a density $\mu_k = y^k \frac{dxdy}{y}(k \geq 2)$, and define $L^2(\mathcal{H}, \mu_k)$ to be the space of holomorphic functions on $\mathcal{H}$ that is $L^2(\mu_k)$ bounded. Then under the Cayley map $z \mapsto w = \frac{z-i}{z+i}$, this density is mapped to the density $\nu_k$ of $\mathbb{D}$ and induces an isomorphism of spaces

\[ L^2(\mathcal{H}, \mu_k) \cong L^2(\mathbb{D}, \nu_k). \]

In particular, $L^2(\mathcal{H}, \mu_k)$ is complete, and it has an orthogonal basis

\[ \{ \varphi_n = (\frac{z-i}{z+i})^n \frac{(2i)^k}{(z+i)^k} \}. \]

by (10.5.6.16) and (10.5.6.17).
7 Elliptic Functions

Main references are [Ahl79]Chap7, [Sil99], [Sil16].

Def. (10.5.7.1) [Doubly Periodic Function]. Let \( \Lambda \) be a lattice of \( \mathbb{C} \), then a meromorphic function \( f \) on \( \mathbb{C} \) is called doubly periodic w.r.t. \( \Lambda \) if it is invariant under \( \Lambda \).

Prop. (10.5.7.2). Let \( f \) be a periodic function for \( \Lambda \), not identically zero, and let \( D \) be a parallelogram for \( \Lambda \) that \( f \) has no zeros or poles on the boundary of \( D \). Then

- \( \sum_{P \in D} \text{ord}_P(f) = 0 \).
- \( \sum_{P \in D} \text{Res}_P(f) = 0 \).
- \( \sum_{P \in D} \text{ord}_P(f) \cdot P = 0 \).

Proof: \( f \) can be realized as meromorphic functions on the Riemann surface \( \mathbb{C}/\Lambda \), so 1, 2 are direct consequences of (5.11.11.6) 1, 2. 3 is 2 applied to the meromorphic function \( zf'(z)/f(z) \).

Def. (10.5.7.3) [Order]. The order of an elliptic function \( f \) is defined to be the number of poles of \( f \) in \( D \). Equivalently, it is the number of zeros of \( f \) in \( D \)(10.5.7.2).

Prop. (10.5.7.4). The order of a non-constant elliptic function \( \geq 2 \).

Proof: If its order is 0, then it is bounded on \( D \) and also on \( \mathbb{C} \) thus constant by Liouville’s theorem. If its order is 1, then it has a simple pole \( z_0 \), but then \( \text{Res}_{z_0}(f) \neq 0 \), contradicting (10.5.7.2).

Def. (10.5.7.5) [Weierstrass Function \( \wp \)]. For a lattice \( \Lambda \subset \mathbb{C} \), consider the function

\[
\wp(z) = \frac{1}{z^2} + \sum_{\omega \in \Lambda \setminus \{0\}} \left( \frac{1}{(z - \omega)^2} - \frac{1}{\omega^2} \right)
\]

Then it is a doubly periodic meromorphic function that has a double pole at 0, and so does its derivative \( \wp' \), having a triple pole at 0. Hence they descend to a rational function on \( \mathbb{C}/\Lambda \).

If \( \Lambda = \Lambda_\tau \), then the function \( \wp(z; \tau) = \wp(z) \) is called the Weierstrass \( \wp \)-function.

Prop. (10.5.7.6). Let \( G_k(\Lambda) \) be given by (15.11.5.5),

\[
\wp(z) = \frac{1}{z^2} + \sum_{k \geq 1} (2k + 1)G_{2k+2}(\Lambda)z^{2k}.
\]

Proof: This follows from (7.5.2.1).

Prop. (10.5.7.7) [Fields of Elliptic Functions]. The field of doubly periodic functions for \( \Lambda \) is just \( \mathbb{C}(\wp, \wp') \). And \( \wp, \wp' \) also satisfies the following equation:

\[
\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z)^2 - g_3\wp(z)
\]

where \( g_2 = 60G_4(\Lambda), g_3 = 140G_6(\Lambda)(15.11.5.5) \).

Proof: For the equational function, just notice we can calculate directly that the difference of the two sides is a holomorphic function in \( z \) without constant terms, and they are both doubly periodic, thus is zero.
For the first statement, notice that any function is a sum of an odd function and an even function. \( \Psi' \) is odd, thus an odd function is \( \Psi' \) times an even function. Thus it reduces to show that any even doubly periodic function is a rational function of \( \Psi \).

For any even periodic function \( f \), \( f \) has the same order at \( z_0 \) and \( -z_0 \), also if \( z_0 \equiv -z_0 \mod \Lambda \), the order of \( f \) at \( z_0 \) must be odd. Now consider \( \Psi(z) - \Psi(z_0) \), then it is a function with two poles at 0, so it has two zeros. If \( z_0 \equiv -z_0 \mod \Lambda \), then \( \Psi(z) - \Psi(z_0) \) has a zero of order 2 at \( z_0 \), and otherwise it has simple zeros at \( z_0 \) and \( -z_0 \).

So for any even doubly periodic function \( f \), we can use the product \( \prod (\Psi(z) - \Psi(z_0))^{m_i} \) to get a function with the same order of poles and zeros as \( f \), which implies it equals \( f \). \( \square \)

**Prop. (10.5.7.8) [Uniformization Theorem]**. For any complex numbers \( A, B \in \mathbb{C} \) that \( A^3 - 27B^2 \neq 0 \), there exists a unique lattice \( \Lambda \in \mathbb{C} \) that \( g_2(\Lambda) = A, g_3(\Lambda) = B \) (10.5.7.7).

**Proof**: The \( j \)-function (15.11.5.10) is surjective, thus there is a \( z \in \mathbb{C} \) s.t.
\[
1728 \frac{1}{1 - \frac{E_6}{E_4}} = \frac{A^3}{A^3 - 27B^2}.
\]

And if we assume \( A, B \neq 0 \), then by (15.11.5.5)(16.2.3.27) and (10.5.3.10), assume this implies
\[
\left( \frac{B}{g_3(\tau)} \right)^2 \left( \frac{g_2(\tau)}{A} \right)^3 = 1.
\]
Then we can scale \( \Lambda \) by \( \Lambda' = \alpha \Lambda \) s.t. \( g_3(\Lambda') = B, \ g_2(\Lambda) = A \).

The case that \( A = 0 \) or \( B = 0 \) is similar.

The uniqueness follows from (13.5.8.6). \( \square \)

8 Special Functions

**Gamma Function**

**Def. (10.5.8.1) [Gamma Function]**. For a complex number \( s \) that \( \text{Re}(s) > 0 \), the **Gamma function** is defined to be
\[
\Gamma(s) = \int_0^\infty e^{-x} x^s \frac{dx}{x},
\]
which is convergent for any \( \text{Re}(s) > 0 \) thus an analytic function on the right half plane.

**Prop. (10.5.8.2)**. \( \Gamma(s + 1) = s\Gamma(s) \).

**Proof**: \( \square \)

**Prop. (10.5.8.3) [Special Values]**.
\[
\Gamma(1) = 1, \Gamma \left( \frac{1}{2} \right) = \sqrt{\pi}.
\]

**Proof**: \( \square \)

**Prop. (10.5.8.4) [Duplication Formula]**.
\[
\Gamma(2s - 1) = \frac{4^{s-1}}{\sqrt{\pi}} \Gamma(s - \frac{1}{2})\Gamma(s).
\]
Prop. (10.5.8.5).

\[ \Gamma(u)\Gamma(1-u) = \frac{\pi}{\sin(\pi u)}. \]

Proof:

\[ \square \]

Cor. (10.5.8.6) [Analytic Extensions]. This formula extends \( \Gamma \) to a meromorphic function at whole plane. It has simple poles at \( s = -n \), where it has residues \( \frac{(-1)^n}{n!} \), for \( n \geq 0 \).

Prop. (10.5.8.7) [Mellin Inversion Formula]. By (10.10.2.16) applied to \( f(x) = e^{-x} \), for any real \( c > 0 \),

\[ e^{-x} = \frac{1}{2\pi i} \int_{c-i\infty}^{c+i\infty} \Gamma(s)x^{-s}ds, \quad x > 0. \]

Prop. (10.5.8.8) [Stirling’s Formula]. \(|\Gamma(\sigma + it)| \sim \sqrt{2\pi|t|^{\sigma-1/2}}e^{-\pi|t|/2} .\)

Proof:

\[ \square \]

Bessel Function

Def. (10.5.8.9) [Bessel Function]. The Bessel function is defined to be

\[ B(r, s) = \int_0^1 (1 - y)^{r-1}y^{s-1}dy. \]

Prop. (10.5.8.10).

\[ B(x, y) = \frac{\Gamma(x)\Gamma(y)}{\Gamma(x + y)}. \]

K-Bessel Function

Def. (10.5.8.11). The K-Bessel function is defined to be

\[ K_s(y) = \frac{1}{2} \int_0^\infty e^{-y(t+\frac{1}{2})/2}t^sdt/t, \quad y > 0. \]

it satisfies \( K_{-s}(y) = K_s(y) \).

Prop. (10.5.8.12). \(|K_s(y)| \leq e^{-y/2}K_{Re(s)}(2) \) when \( y > 4 \).

Proof: This is because \( e^{-ab} < e^{-a}e^{-b} \) when \( a, b > 2 \).

\[ \square \]

Prop. (10.5.8.13).

\[ \frac{\partial}{\partial y}K_s(y) = \frac{1}{2} \int_0^\infty (-t + \frac{1}{2})/2e^{-y(t+\frac{1}{2})/2}t^sdt/t = -\frac{1}{2}(K_{s+1}(y) + K_{s-1}(y)) \]

Prop. (10.5.8.14). If \( Re(s) > 1/2 \) and \( r \in \mathbb{R} \),

\[ \left(\frac{y}{\pi}\right)^s\Gamma(s)\int_{-\infty}^{\infty} (x^2 + y^2)^{-s}e^{2\pi i rx}dx = \begin{cases} 
\pi^{1/2-s}\Gamma(s - \frac{1}{2})y^{1-s} & r = 0 \\
2|y|^{s-1/2}\sqrt{y}K_{s-1/2}(2\pi|y|) & r \neq 0 
\end{cases} \]
Proof: By (10.5.8.1), the LHS equals
\[ \int_{-\infty}^{\infty} \int_{0}^{\infty} e^{-t \left( \frac{ty}{\pi(x^2 + y^2)} \right)^s} e^{2\pi irx} \frac{dt}{t} dx = \int_{0}^{\infty} \int_{-\infty}^{\infty} e^{-\pi t(x^2 + y^2)/yt} e^{2\pi irx} dx \frac{dt}{t} \]
where we interchanged the order of integration because it is absolutely convergent, and made a change of variable. Also notice
\[ \int_{-\infty}^{\infty} e^{-t\pi x^2/y} e^{2\pi irx} dx = \sqrt{\frac{y}{t}} e^{-y\pi r^2/t} \]
by Fourier inversion (10.10.2.3), so we get the final answer. \(\square\)

Prop. (10.5.8.15). If \(\text{Re}(s) + k/2 > 1/2\) and \(r\) is real,
\[ \frac{y}{\pi} s(\pi) \int_{-\infty}^{\infty} \frac{1}{(x + yi)^k(x^2 + y^2)^s} e^{-2\pi irx} dx = \begin{cases} \pi^{1/2-s} \Gamma(s - \frac{k}{2}) y^{1-s} & r = 0 \\ 2r|s-1/2| \sqrt{y} K_{s-1/2}(2\pi |r|) & r \neq 0 \end{cases} \]
Proof: By (10.5.8.1), the LHS equals
\[ \int_{-\infty}^{\infty} \int_{0}^{\infty} e^{-t \left( \frac{ty}{\pi(x^2 + y^2)} \right)^s} e^{2\pi irx} \frac{dt}{t} dx = \int_{0}^{\infty} \int_{-\infty}^{\infty} e^{-\pi t(x^2 + y^2)/yt} e^{2\pi irx} dx \frac{dt}{t} \]
where we interchanged the order of integration because it is absolutely convergent, and made a change of variable. Also notice
\[ \int_{-\infty}^{\infty} e^{-t\pi x^2/y} e^{2\pi irx} dx = \sqrt{\frac{y}{t}} e^{-y\pi r^2/t} \]
by Fourier inversion (10.10.2.3), so we get the final answer. \(\square\)

9 Multi-Variable case

Basics

Should cover the part from [Complex Analytic and Differential Geometry Demailly], [Principle of Algebraic Geometry Griffith/Harris] and [Complex Geometry Daniel].

Def. (10.5.9.1). A function is called **holomorphic** in several variables iff it is holomorphic for each indeterminate.

Def. (10.5.9.2). For \(a \in \mathbb{C}^n\), the polydisc \(B(a, \varepsilon) \subset \mathbb{C}^n\) is defined to be the set \(\{z||z_i - a_i| < \varepsilon_i\}\).

Prop. (10.5.9.3) [Hartog’s Extension Theorem]. If \(K\) is a compact subset in an open domain \(\Omega\) of \(\mathbb{C}^n (n \geq 2)\) and \(\Omega - K\) is connected, then any holomorphic function on \(\Omega - K\) extends to a holomorphic function on \(\Omega\).

Proof: \(\square\)

Prop. (10.5.9.4). Let \(\varepsilon = (\delta, \ldots, \delta)\) and \(f\) be a holomorphic function on the polydisc \(B_\varepsilon(0)\). Then if \(f\) vanishes of order \(k\) at the origin and \(|f(z)| \leq C\), then
\[ f(z) \leq C \left( \frac{|z|}{\delta} \right)^k \]
for all \(z \in B_\varepsilon(0)\).

Proof: Fix \(z \in B_\varepsilon(0) \neq 0\), consider the one-variable function \(g_\varepsilon(w) = w^{-k} f(w \cdot \frac{z}{|z|})\), then \(g_\varepsilon\) is holomorphic and \(|g_\varepsilon(w)| \leq \delta^{-k} C\) for \(|w| = \delta\). So maximal principle implies that \(g_\varepsilon(w) \leq \delta^{-k} C\) for all \(|w| \leq \delta\). Hence \(|z|^{-k} |f(z)| = |g_\varepsilon(z)| \leq \delta^{-k} C\). \(\square\)
10.6 General Functional Analysis

Basic references are [Rudin Functional Analysis],[Nonarchimedean Functional Analysis].

This section only contains theorems that are applicable to both Archimedean and non-Archimedean valuations. For theorems specialized to non-Archimedean valuations, See 12.1, for theorems specialized to Archimedean valuations, See 10.7. Many propositions in Functional Analysis can be transplanted in the general case, but I haven’t finish yet.

The major problem is convex is not definable, so Hahn-Banach fail, causing many to fail.

1 Topological Vector Space

Def.(10.6.1.1)[Topological Vector Spaces]. A topological vector space (TVS) over a complete valued field $k$ is a $k$-vector space that the addition and scalar multiplication is continuous.

Remark(10.6.1.2). If the field $k$ is not of char 0, then we fix a sequence of elements $\{a_n\}$ that $\lim |a_n| = \infty$. This will be applied for example in the proof of Banach-Steinhaus theorem, but we will just write $n$ instead of $a_n$.

Prop.(10.6.1.3). For subsets $K, C$ of a TVS $X$ that $K$ is compact and $C$ is closed, there is a nbhd $V$ that $(K + V) \cap (C + V) = \emptyset$.

Proof: For each $x \in K$, there are symmetric nbhd $V_x$ that $(x + V_x + V_x + V_x) \cap C = \emptyset$. Then $(x + V_x + V_x) \cap (C + V_x) = \emptyset$. Because $K$ is compact, there are f.m. $x_i$ that $K \subset \cup (x_i + V_x)$. So let $V = \cap V_{x_i}$, then $(K + V) \cap (C + V) = \emptyset$. □

Cor.(10.6.1.4)[Closed Subbasis]. Every nbhd of 0 in a TVS contains a closure of another nbhd of 0. (Apply the above proposition for $K = \{0\}$.

Def.(10.6.1.5). A subset containing 0 is called balanced iff $kU = U$ for each $|k| = 1$.

Prop.(10.6.1.6)[Balanced Subbasis]. Every nbhd $U$ of 0 in a TVS contains a balanced nbhd of 0. By (10.6.1.4), we can even assume $V \subset U$.

Proof: Since scalar multiplication is continuous, there is a $\delta > 0$ and a nbhd $V$ that $\alpha V \subset U$, for each $|\alpha| < \delta$. Then let $W = \cup_{|\alpha|<\delta} \alpha V$. □

Def.(10.6.1.7)[F-Space and Fréchet space]. A space is called a F-space if its topology is induced by a complete invariant metric. F-space is of second Baire category by (3.6.9.2)

A locally convex F-space is called a Fréchet space.

A TVS is said to satisfy Heine-Borel iff every closed and bounded subset of $X$ is compact.

Def.(10.6.1.8)[Norm]. A seminorm on a vector space $X$ is a real-valued function $p$ that $p(x+y) \leq p(x) + p(y)$, and $p(\alpha x) = |\alpha|p(x)$ for $\alpha \in k$. It is called a norm if moreover $p(x) = 0 \iff x = 0$.

A family of seminorms $\{p_i\}$ on $X$ is called separating iff for each $x$, at least one $p_i$ satisfies $p_i(x) \neq 0$.

Prop.(10.6.1.9). A TVS is metrizable by a translation-invariant metric iff it has a countable basis.

Proof: One direction is trivial, for the other, Cf.[Rudin P18]. □

Prop.(10.6.1.10). If a subspace $Y$ of a TVS $X$ is a F-space, then it is closed in it.
2 Completeness

Prop. (10.6.2.1)[Banach-Steinhaus]. \( \Gamma \) is a collection of continuous linear mapping between two TVS, if the set \( B \) of \( x \) that \( \Gamma(x) \) is bounded is a second category set in \( X \), then \( B = X \) and \( \Gamma \) is equicontinuous (thus maps bounded sets to bounded sets).

Proof: For an open balanced nbhd \( W \) of 0, choose a balanced nbhd \( U \) s.t. \( U + U \subset W \). Let \( E = \bigcap_{\lambda \in \Gamma} \lambda^{-1}(U) \), then \( E \subset \bigcup_{n \geq 1} nE \), so by Baire theorem (3.6.9.2), \( E \) has a interior point thus \( E \) has a nbhd \( V \) s.t. \( \Gamma(V) \subset U + U \subset W \). Thus we are done.

Cor. (10.6.2.2)[Uniform Boundedness Theorem]. If a set \( E \) in a TVS is called totally bounded if for every nbhd \( V \) of 0, there is a finite set \( F \) that \( E \subset F + V \).

Prop. (10.6.2.4)[Open Mapping theorem]. If a continuous linear mapping \( T \) from a F-space \( X \) to \( Y \) satisfies \( R(T) \) is of second category, then it is a surjective open mapping and \( Y \) is a F-space.

Proof: V \( n = T(B(0, \frac{r}{2n})) \) are all of second category, because \( \bigcup_{n} nV_n = R(T) \), so \( V_n \) has an interior by definition. Then also it contains a nbhd of 0 because \( V_{n+1} \subset V_n \).

Now we show \( V_{n+1} \subset V_n \), this will show \( T \) is open. for a \( y \in V_n \), since \( T(V_{n+1}) \) contains a nbhd of 0, we can consecutively choose \( x_i \in B(0, \frac{r}{2n+i}) \) s.t. \( y - \sum_{i=1}^{n} T(x_i) \in T(B(0, \frac{1}{2n+i+1})) \). So by completeness of \( X \) and closedness, \( \sum x_i \) converges to some \( x \in D(T) \), and \( Tx = y \in V_n \).

And an open linear mapping must be surjective. hence \( Y \cong X/N(T) \), so \( Y \) is also a F-space.

Cor. (10.6.2.5)[Banach Theorem]. If a continuous map \( T \) between F-spaces is a bijection, then it has a continuous inverse.

Cor. (10.6.2.6). If a F-space is complete w.r.t two different topologies and one is stronger than the other, then they are equivalent.

Cor. (10.6.2.7). For every operator between F-spaces that has closed image, we have \( X/N(T) \cong R(T) \).
Cor. (10.6.2.8) [Closed Graph Theorem]. If $T$ is a closed linear mapping between two F-spaces, i.e., the graph of it is closed, then it is continuous, because the metric induced by the graph is stronger than the original one, and use Banach (10.6.2.5).

The graph is closed is equivalent to if $x_i \to x$ and $Tx_i \to y$, then $y = Tx$. This is very useful when proving some map is continuous.

Cor. (10.6.2.9). If $A, B, C$ are F-spaces, and $f : A \to B, g : B \to C$, if $gf, g$ is continuous and $g$ is injective, then $F$ is continuous.

Proof: Use closed graph theorem, if $x_i \to x, f(x_i) \to z$, then $gf(x_i) \to g(z)$, so $gf(x) = g(z)$, so $f(x) = z$. □

Cor. (10.6.2.10) [Finite Codimensional Image]. If the image of a continuous linear mapping $T$ between F-spaces has finite codimensional image, then the image is closed and complemented.

Proof: It has finite codimension, so we can construct $K^n \oplus X/N(T) \to Y$, by Banach theorem (10.6.2.5) it is a homeomorphism, and the image of $X/N(T)$ corresponds to the image, so the image is closed. □

Prop. (10.6.2.11) [Separate Continuous]. If a bilinear map $B : X \times Y \to Z$ where $X$ is a F-space is separately closed, then $B(x_n, y_n)$ converges to $B(x_0, y_0)$.

Proof: Use Banach-Steinhaus to prove $B_{y_n}(x)$ is equicontinuous, then use $B(x_n - x_0, y_n) + B(x_0, y_n - y_0)$.

□

3 Dual Space

Prop. (10.6.3.1) [Operator Space]. If $X, Y$ are normed spaces then $L(X, Y)$ is also a normed space with the metric $||A|| = \sup\{||Ax|| | x| \leq 1\}$. And if $Y$ is Banach, then $L(X, Y)$ is also Banach. The proof is easy.

In particular, if $Y = K$, then $X^*$ is a Banach space.

Prop. (10.6.3.2). For a bounded operator $T$,

$$\overline{R(T)} = N(T^*)^\perp, \text{ Thus } \overline{R(T^*)} = N(T)^\perp$$

In particular, using Hahn Banach, $R(T)$ is dense in $Y$ iff $T^*$ is injective, $T$ is injective iff $T^*$ is weak*-dense in $X^*$.

Prop. (10.6.3.3). Let $\Lambda_1, \ldots, \Lambda_n, \Lambda$ are linear functionals on a vector space $X$, let $N = \cap \ker f_i$, the following are equivalent:

1. $\Lambda = \sum \alpha_i \Lambda_i$.
2. $|\Lambda x| \leq \gamma |\Lambda_i x|$.
3. $\ker \Lambda \subset N$.

Proof: Only need to show 3 $\to$ 1: define $\pi : X \to k^n : x \mapsto (\Lambda_1 x, \ldots, \Lambda_n x)$, then by hypothesis $f(\pi(x)) = \Lambda(x)$ defined a linear functional on $\pi(X)$. This can be extended to a functional on $k^n : F(u_1, \ldots, u_n) = \sum \alpha_i u_i$, so $\Lambda$ is a linear combination of $\Lambda_i$. □
Weak Convergence

**Def. (10.6.3.4) [Operator Topologies].** There are three topologies on $L(X)$ for a normed space $X$:

- norm topology: $||T_i - T|| \to 0$.
- strong topology: $\forall x \in X, ||(T_i - T)x|| \to 0$.
- weak topology: $\forall x \in X, f \in X^*, \lim f(T_n x) = f(Tx)$.

**Prop. (10.6.3.5) [Weak Convergence and Bounded].** In a normed space $X$, if $x_n \to x$ weakly iff $\{x_n\}$ is bounded and $\lim f(x_n) = f(x)$ for a dense subset $f \in M^* \subset X^*$.

*Proof:* This follows from (10.6.2.3), as $X^*$ is a Banach space, by (10.6.3.1).

4 Banach Space

**Def. (10.6.4.1) [Normed (Valued) $K$-Spaces].** For a complete valued field $K$, a normed (valued) $K$-space is a TVS over $K$ with a norm that satisfies $|kv| = |k||v|$ for $k \in K$.

**Def. (10.6.4.2) [Banach Spaces].** For $K$ complete valued field, a complete normed (valued) $K$-vector space (10.6.4.1) is called a **Banach space**.

A $K$-algebra with a complete $K$-algebra norm is called a **Banach algebra**.

**Prop. (10.6.4.3).** The dual space of a Banach space is a Banach space. (Immediate from (10.6.3.1)).

**Prop. (10.6.4.4).** if $A$ is a Banach space as well as a Topological group, then there is a norm on $A$ which induce the same topology and makes $A$ into a Banach algebra.

*Proof:* embed $A$ into $L(A)$ by left multiplication, which is injective, and $||x|| = ||xe|| = ||M_x e|| \leq ||M_x||||e||$, so its inverse is continuous. Now if we show the image $\tilde{A}$ is closed in $L(A)$, then the open mapping theorem will show that $A \cong \tilde{A}$, and $\tilde{A}$ is clearly a Banach algebra.

To show it is closed, if $T = \lim T_i$, notice $T_i(y) = T_i(e)y$, so take a limit, $T(y) = T(e)y = M_{T(e)}y$.

* □

**Cor. (10.6.4.5).** Every f.d. Banach algebra is isomorphic to an algebra of matrices. In particular, if $xy = e$, then $yx = e$.

*Proof:* Embed $A$ into $L(A)$.

* □

**Remark (10.6.4.6) [Inequivalent Banach Norms].** There exists two complete norm on a vector space that is inequivalent. For this, just choose a banach space $X$, and notice if we can choose a discontinuous bijection $X \to X$, then the induced metric is also complete, and it cannot by equivalent by Banach theorem (10.6.2.5). For this, choose a infinite dimensional Banach space over $\mathbb{C}$, and choose a $\mathbb{C}$-basis $x_i$ for it, and choose a sequence $x_n$ and maps $x_n$ to $nx_n$, the rest are invariant, then this is not continuous.

Hilbert Space

**Def. (10.6.4.7).** there are different topologies in the space of operators on a Hilbert space $\mathcal{H}$.

- **Norm operator topology:** defined by the norm $||T||$.
- **Strong operator topology:** defined by the separating seminorms $T \mapsto ||Tu||, u \in \mathcal{H}$.
- **Weak operator topology:** defined by the separating seminorms $T \mapsto (Tu, v), u, v \in \mathcal{H}$. 

Prop. (10.6.4.8). The strong and weak operator topology coincides on the unitary operators on \( \mathcal{H} \).
The sets of unitary operators that is continuous in this two topology is denoted by \( U(\mathcal{H}) \).

Proof: If \( T_n \) converges to \( T \) in the weak operator topology, then
\[
||(T_n - T)u||^2 = ||Tu||^2 + ||T_n u||^2 - 2 \text{Re}(T_n u, Tu).
\]
The right hand side is clearly bounded by the weak seminorms, so the two topologies coincide. \( \square \)

Prop. (10.6.4.9) [Hilbert Basis]. If \( H \) is a Hilbert space and \( S = \{e_\alpha\} \) is an orthonormal basis in \( H \), then the following are equivalent:

1. For any \( x \), \( x = \sum (x, e_\alpha) e_\alpha \) (notice the sum are in fact infinite sum).
2. There is a no nonzero element \( x \) that is orthogonal to all \( e_\alpha \).
3. Parseval equality holds: \( ||x||^2 = \sum |(x, e_\alpha)|^2 \).

If these are true, then \( S \) is called a Hilbert basis of \( H \), a Hilbert basis always exists, by Zorn’s lemma.

Proof: 1 \( \rightarrow \) 2: if \( (x, e_\alpha) = 0 \) for all \( e_\alpha \), then by 1, \( x = \sum (x, e_\alpha) e_\alpha = 0 \).
2 \( \rightarrow \) 3: Notice \( y = x - \sum (x, e_\alpha) e_\alpha \) is orthogonal to all \( e_\alpha \), and
\[
||y|| = ||x||^2 - \sum |(x, e_\alpha)|^2,
\]
so Parseval equality holds.
3 \( \rightarrow \) 1: \( ||x - \sum (x, e_\alpha) e_\alpha|| = 0 \). \( \square \)

Prop. (10.6.4.10). Any symmetric operator on a Hilbert space is continuous.

Proof: Because \( x_n \to 0 \) implies \( Tx_n \to 0 \) weakly, so we can use closed graph theorem (10.6.2.8). \( \square \)

**Ultrannormed Banach Spaces**

The ultrannormed Banach spaces are defined in (12.1.2.4).

**Nuclear Maps and Spaces**
10.7 Archimedean Functional Analysis

Reference: [Rudin Functional Analysis]. [Rudin Functional Analysis Chap11,13] needs to be revised.
This section contains functional analysis in characteristic 0. By Ostrowski theorem (10.3.3.18),
the base field is just \( R \) or \( \mathbb{C} \).

1 Topological Vector Space

Def. (10.7.1.1). A sublinear functional is a function \( p \) that \( p(x+y) \leq p(x)+p(y) \) and \( p(\lambda x) = \lambda p(x) \)
for \( \lambda > 0 \).
A seminorm is a non-negative function \( p \) that \( p(x+y) \leq p(x)+p(y) \) and \( p(\alpha x) = |\alpha|p(x) \) for all complex \( \alpha \).

Def. (10.7.1.2). A absorbing set is a convex set \( A \) that \( \bigcup_{k>0} kA = X \). A convex nbhd of 0 is clearly absorbing.

Def. (10.7.1.3) [Minkowski Functional]. For an absorbing set \( A \), the Minkowski functional \( \mu_A \)
is defined to be \( \mu_A(x) = \inf \{ t > 0, x/t \in A \} \). It satisfies:
• \( \mu_A(x+y) \leq \mu_A(x)+\mu_A(y) \).
• \( \mu_A(kx) = k\mu_A(x) \) if \( k > 0 \).
• \( \mu_A \) is a seminorm if \( A \) is balanced.
• If \( B = \{ x|\mu(x) < 1 \} \), \( C = \{ x|\mu(x) \leq 1 \} \), then \( B \subset A \subset C \) and \( \mu_A = \mu_B = \mu_C \).

Proof: Cf. [Rudin P27].

Cor. (10.7.1.4) [Seminorm and Absorbing set]. A seminorm on \( X \) is exactly the Minkowski functional of a balanced absorbing set \( W \), but the set may not be unique and it is uniformly continuous iff 0 is an interior point.

Proof: If \( p \) is a seminorm, then \( \{ x|p(x) < 1 \} \) is convex, balanced and absorbing by definition (10.6.1.8). The converse is by (10.7.1.3). The last assertion is easy.

Prop. (10.7.1.5) [Minkowski Functional and Separating Seminorms]. If \( \mathfrak{B} \) is a convex local base in a TVS \( X \), then the Minkowski functionals of elements of \( \mathfrak{B} \) forms a separating family of seminorms.

Conversely, a separation family \( P \) of seminorms on a vector space defines a convex balanced local base for a topology \( \tau \) that is locally convex. And in this topology, a sequence converges iff \( p(x_i - x) \to 0 \) for \( p \in \mathfrak{B} \), a set is bounded if each \( p \) is bounded on it.

Proof: For any \( V \in \mathfrak{B} \), \( V = \{ x \in X|\mu_V(x) < 1 \} \), because \( V \) is open and convex. (10.7.1.3) shows each \( \mu_V \) is a seminorm, and it is continuous because it is bounded on \( V \). And they are separating because \( \mathfrak{B} \) is a local base.

Defined \( V(p,n) = \{ x \in X|p(x) < 1/n \} \), and let these be a local subbasis at 0, and make it a topology by translation. This is checked to be a locally convex TVS. For the last assertion, if \( E \) is bounded, then \( E \subset kV(p,1) \) for \( k \) large, so \( p \) is bounded on \( E \), and conversely, for each nbhd \( U \), there are \( p_i \) and \( M_i \) and \( \cap V(p_i,M_i) \subset U \), so \( E \subset kU \) for \( n \) large.

Prop. (10.7.1.6). If \( \mathfrak{B} \) is a family of countable separating family of semi-norms on \( X \), then the topology defined in (10.7.1.5) is in fact metrizable, by a metric \( d(x,y) = \sum \frac{1}{2^k} \frac{p_i(x-y)}{1+p_i(x-y)} \).
Finite Dimensional Subspace

**Prop. (10.7.1.7) [Finite Dimensional and Locally Compact].** There is only one topological vector space structure on a finite dimensional C-vector space and it is complete. A TVS is locally compact iff it is f.d.

*Proof:* Cf. [Rudin P17].

For the second assertion, if is locally compact, then 0 has a nbhd $V$ that is precompact, so bounded, hence $2^{-n}V$ forms a local basis. the compactness of $V$ shows there are f.m. $x_i$ that $V \subset \cup (x_i + \frac{1}{2} V)$. Let $Y$ be the subspace spanned by $x_i$, then it is of f.d, thus closed. Now $V \subset Y + \frac{1}{2}V$, so $\frac{1}{2}V \subset Y + \frac{1}{4}V$, hence continuing this way, $V \subset \cap (Y + 2^{-n}V)$, so $V \subset Y = Y$. But then $Y = X$. $\square$

**Cor. (10.7.1.8) [Finite Subspace Closed].** A f.d subspace in a TVS over C is closed, because it must be a F-space, hence it is closed by (10.6.1.10).

**Prop. (10.7.1.9) [Finite Subspace in Banach Space].** For a finite dimensional space $V$ in an Archimedean Banach space, there is a continuous projection onto it. In particular, any finite dimensional space in an Archimedean Banach space is complemented.

Also finite codimensional subspace in any Banach space is complemented by (10.6.2.10).

*Proof:* Choose a basis $e_i$ for $V$, consider the dual basis $f_i$. Because a finite dimensional space only has one topology (10.7.1.7), these $f_i$ are bounded on $V$. Extend them to bounded functional on $X$, then consider $p(x) = \sum f_i(x) e_i$, then this is a continuous projection onto $V$. $\square$

## 2 Various Spaces and Duality

For a bounded connected open set $\Omega$,

**Prop. (10.7.2.1) [Various Spaces and Duality].**

- **Sobolev Space** $W^{m,p}(\Omega)$ is the completion of a subspace of $C^\infty(\Omega)$ with the norm
  \[ \|u\|_{m,p} = \left( \sum_{|\alpha| \leq m} \int_{\Omega} |\partial^\alpha u(x)|^p \, dx \right)^{1/p}. \]
  for $m > 0$. And we denote $W^{m,2}(\Omega)$ by $H^m(\Omega)$. It is also a subspace of $L^p(\Omega)$ that satisfies this, without completion (10.10.3.1).

- $C^\infty_0(\Omega)$ is the subspace of $C^\infty(\Omega)$ that have compact support in $\Omega$. Its completion $W^{m,p}_0(\Omega)$ is a closed subspace of $W^{m,p}(\Omega)$. And we denote $W^{m,2}_0(\Omega)$ by $H^m_0(\Omega)$ and the dual space of $H^m_0(\Omega)$ by $H^{-m}(\Omega)$.

- $C(\Omega)$ in the topology of compact convergence is a Fréchet space. It is not locally convex.

- $H(\Omega)$ the space of holomorphic functions in $\Omega$ is a closed subspace of $C(\Omega)$ thus is a Fréchet space. Montel’s theorem says exactly that $H(\Omega)$ is Heine-Borel.

- $H^2(D)$ the space of holomorphic functions on the unit disk $D$ that is also $L^2$. It has the $L^2$ norm.

- $C^\infty(\Omega)$ in the topology defined by seminorms $p_N(f) = \max\{|D^\alpha f(x)| : x \in K_N, |\alpha| \leq N\}$, is a Fréchet space thus locally convex and it has the Heine-Borel property by Arzela-Ascoli.
• $D(K)$ is the closed subspace of smooth functions on $\Omega$ with support in $K$, thus a Fréchet space with Heine-Borel property.

• $D(\Omega)$ is the space of smooth functions with support in $\Omega$. It has the topology generated by translation of basis consisting of convex balanced sets $W$ that $W \cap D(K)$ is open for every compact $K$. This makes $D(\Omega)$ into a locally convex TVS, Cf.[Rudin P152]. It has Heine-Borel property.(10.10.1.1).

• (Schwartz Functions) The space of Schwartz functions $\mathcal{S}$ is defined as smooth functions on $\mathbb{R}^n$ that

$$\sup_{|\alpha| \leq N} \sup_{x \in \mathbb{R}^n} (1 + |x|^2)^N |(D_\alpha f)(x)| < \infty$$

for any $N > 0$. And it is a Fréchet space define by these seminorms.

### Dual Spaces

**Prop. (10.7.2.2).** For a $\sigma$-finite measure $\mu$ on a measurable space $X$, for $1 \leq p < \infty$

$$L^p(X, \Omega, \mu)^* = L^q(X, \Omega, \mu).$$

(10.4.5.3)

• $C[0,1]^* = BV[0,1]$ and $C[X]^* = M(X)$, the space of complex measure on compact $X$ with the norm of total variance, by Riesz representation theorem(10.9.1.10).

### 3 Convexity

**Prop. (10.7.3.1).** Every convex nbhd of 0 contains a balanced convex nbhd of 0. By(10.6.1.4), we can even assume $V \subset U$.

**Proof:** If $U$ is convex, choose $W$ as in(10.6.1.6), then $W \subset A = \cap_{|\alpha|=1} \alpha U$ because it is balanced. Then $W \subset A^0$ and $A^0$ is open and balanced, satisfying the requirement. \hfill $\square$

**Prop. (10.7.3.2).** For a compact convex set $K$ in a TVS $X$, if a set $\Gamma$ of continuous linear mapping is bounded for every $x \in K$, then $\Gamma$ is equicontinuous on $K$.

**Proof:** The proof is similar to that of Banach-Steinhaus(10.6.2.1). For $K$ compact convex, the same argument shows that there is a nbhd $V$ that $K \cap (x_0 + V) \subset nE$, fix $p > 1$ that $K \subset x_0 + pV$, then for any $x \in K$, consider $z = (1 - p^{-1})x_0 + p^{-1}x$, then $z \in K$ as $K$ is convex and $z - x_0 = p^{-1}(x - x_0) \in V$, so $z \in nE$, and since $x = pz - (p - 1)x_0$, $\Lambda x \in pnW$ for each $\Lambda \in \Gamma$, so $\Gamma$ is equicontinuous. \hfill $\square$

### Hahn-Banach

**Prop. (10.7.3.3)[Real Hahn].** For a sublinear functional $p$ on a real linear space $X$ and a subspace $X_0$, if a functional $f$ satisfies $f(x) \leq p(x)$ on $X_0$, then it can be extended to a functional $\Lambda$ on $X$ that $|\Lambda(x)| \leq |p(x)|$.

**Proof:** Use Zorn’s lemma, if the maximum extension is not on the whole space but on $M$, choose $x_1 \in X - M$, we want to define $f(x_1)$. Now let $M_1 = \{x + tx_1| x \in M\}$. Since for $x, y \in M$, $f(x) + f(y) = f(x + y) \leq p(x + y) \leq p(x - y) + p(x_1 + y)$, so

$$f(x) - p(x - x_1) \leq p(y + x_1) - f(y)$$
for $x, y \in M$. Let the maximum of the left side be $\alpha$, and define $f(x_1) = \alpha$, then it is clear $f(z) \leq p(z)$ still. □

**Prop. (10.7.3.4)[Complex Hahn].** For a seminorm $p$ (i.e. it can attain 0) on a complex linear space $X$ and a subspace $X_0$, if a functional $f$ satisfies $|f(x)| \leq p(x)$ on $X_0$, then it can be extended to a functional on $X$ with the same condition.

**Proof:** Let $g(x) = \text{Re } f(x)$ and extend it by Hahn and set $f(x) = g(x) - ig(ix)$, then $f$ is complex linear, and for any $x$, for some $|\alpha| = 1$, $|f(x)| = f(\alpha x) = g(\alpha x) \leq p(\alpha x) = p(x)$. □

**Cor. (10.7.3.5)[Hahn].** In a normed space $X$, a bounded linear functional on a subspace $X_0$ can be extended to a bounded functional on $X$ with the same norm.

**Cor. (10.7.3.6)[Extending Functional Preserving Norm].** If $X$ is a normed space and $N$ is a closed subspace, if $x_0$ satisfies $d = d(x_0, M) > 0$, then here is a continuous functional $f$ that $f(x) = 0$ and $f(x_0) = d$ and $|f|| = 1$.

**Proof:** Define $f(m + \alpha x) = |\alpha|d$ on span{$M, x$}, then $f(m + \alpha x) = |\alpha|d = |\alpha|d(x_0, M) \leq |\alpha||\frac{m}{\alpha} + x_0|| = ||x' + \alpha x|| = ||x||$. So $|f|| = 1$, so we can use Hahn-Banach to extend it to a functional on $X$. □

**Prop. (10.7.3.7)[Geometric Hahn].**

- If $E_1$ and $E_2$ are two convex set that $E_1 \cap E_2 = \emptyset$ and $E_1$ has interior point, then there is a continuous linear functional that separate them, i.e $\text{Re } f(E_1) < \text{Re } f(E_2)$. (The interior point is here to assure $f$ is continuous).

- In a locally convex TVS, if $E_1$ is convex compact and $E_2$ is convex closed, then there is a real functional that separate them, i.e. $\text{Re } f(E_1) < \gamma_1 < \gamma_2 < \text{Re } f(E_2)$. Thus for a set $E$ and a point $x, x \in \text{span}E \iff$ for all $f$ that $f(E) = 0, f(x) = 0$.

**Proof:** The complex case follows from the real case, so assume it is real. Consider $a_0 \in E_1, b_0 \in E_2$, let $x_0 = a_0 - b_0$ and let $C = E_1 - E_2 + x_0$, then $C$ is a convex nbhd of 0. Let $p$ be the Minkowski functional of $C$, then $p$ is sublinear by (10.7.1.3) and $p(x_0) \geq 1$. Let $f(tx_0) = t$ on the subspace $M$ generated by $x$, then it extends to a functional $\Lambda$ that $\leq 1$ on $C$, thus it is bounded by 1 on $C \cap (-C)$, hence continuous. For any $a \in E_1, b \in E_2$, because $\lambda(x_0) = 1$ and $a + b + x_0 \in C$ open, $\Lambda a < \Lambda b$.

For the second, There is a convex nbhd $V$ of 0 that $E_1 + V \cap B = \varphi$, so the above argument applied with $E_1 + V$ and $B$ shows that there is a $f$ that separate them. And $f(E_1 + V)$ is open and $f(E_1)$ is compact, so the conclusion follows. □

**Cor. (10.7.3.8)[Banach-Saks].** The weak closure of a convex set in a locally convex metric space equals the original closure.

Thus if a sequence $\{x_n\}$ weakly converges to $x$ in a metrizable locally convex space, then a convex combination of $\{x_n\}$ strongly converge to $x$, i.e. $x \in \overline{co}(\{x_n\})$, because metric space is first countable.

**Proof:** A weak closed set is closed, and to show the closure is weakly closed, use (10.7.3.7). □

**Prop. (10.7.3.9).** If $A_i$ are compact convex sets in a TVS $X$, then $co(A_1 \cup \ldots \cup A_n)$ is compact.
Prop. (10.7.3.10). In F-space, a closed subset is compact iff it is totally bounded by (3.6.8.6).

Prop. (10.7.3.11). In a locally convex space, if E is totally bounded, then co(E) is totally bounded. Thus in a Fréchet space, if K is compact, then K is compact.

Proof: For a nbhd U of 0, choose a convex nbhd V that V + V ⊂ U, then E ⊂ F + V for some finite set F, hence co(E) ⊂ co(F) + V. But co(F) is compact by (10.7.3.9). So co(F) ⊂ F₁ + V for some finite set F₁, then co(E) ⊂ F₁ + U.

If K is compact, then it is totally bounded, and then co(K) is totally bounded and co(K) is compact by (3.6.8.4), so it is compact by (10.7.3.10).

Prop. (10.7.3.12) [Weakly Bounded and Locally Convex]. In a locally convex space, bounded ⇐⇒ weakly bounded.

Proof: One direction is trivial, for the other, suppose E is weakly bounded and U is a closed nbhd of 0. Because X is locally convex, there is a convex, balanced nbhd of 0 that V ⊂ U (10.7.3.1). Now V = V** the polar (10.7.4.1) by (10.7.3.8).

Now V* is weak*-compact and |Λ(x)| ≤ γ(Λ) for each Λ ∈ X* for some γ(Λ) because E is weakly bounded. So we can use (10.7.3.2) to show that |Λx| ≤ γ for some γ and all Λ ∈ V*. So we have γ⁻¹E ⊂ V ⊂ U. This proves that E is bounded.

Prop. (10.7.3.13)[Markov-Kakutani Fixed Point Theorem]. For a commuting family F of continuous affine maps from K to K where K is a compact convex set in a TVS, then there is a fixed point in K for all maps in F.

Proof: Consider the semigroup F* generated by these maps together with their average, it is also commutative because they are all affine. For any f, g ∈ F*, f(K) ∩ g(K) ⊂ f o g(K), so by finite intersection property, there is a point in p ∈ K in all f(K).

For this p, consider p = 1/ₙ(I + T + T² + ... + Tⁿ⁻¹)(x), then p - Tp = 1/ₙ(x - Tⁿx) ∈ 1/ₙ(K - K). As K is bounded and n is arbitrary, this means that p = Tp for all T.

Cor. (10.7.3.14)[Invariant Hahn]. For a commuting family Γ of operators on a normed space and Y an invariant space, then for any Γ-invariant continuous functional f on Y, it has a Γ-invariant Hahn extension.

Proof: We may assume ||f|| = 1. Let K be all extensions of f that has norm ≤ 1. K is obviously convex, and it is weak*-compact by Banach-Alaoglu. The adjoint action of T is checked to be continuous in the weak*-topology, so by (10.7.3.13), there is some F ∈ K that is invariant under Γ.

Krein-Milman theorem

Prop. (10.7.3.15) [Krein-Milman Theorem]. For a compact convex set in a TVS that is weak-Hausdorff (X* separate points), then K = eο(Extreme(K)).

If K is a compact set in a locally convex space, then K ⊂ eο(E(K)) = eο(K).
Prop. (10.7.3.16) [Milman’s Theorem]. If $K$ is a compact set in a locally convex space $X$ and if $\sigma(K)$ is also compact (e.g., in a Fréchet space (10.7.3.11)), then every extreme point of $\sigma(K)$ lies in $K$.

Proof: The annihilator $A^\perp$ of $A$ consists of all regular complex Borel measure $\mu$ on $S$ that $\int f d\mu = 0$ for all $f \in A$ by Riesz representation (10.9.1.10). Cf. [Rudin P122].

Def. (10.7.3.17). For a compact Hausdorff space $S$ and an algebra in $C(S)$, a subset $E$ is called $A$-antisymmetric iff every $f \in A$ that is real on $E$ is constant on $E$. There are in fact maximal $A$-antisymmetric subsets of $S$.

Prop. (10.7.3.18) [Bishop Theorem]. If $A$ is a closed subalgebra of $C(S)$. If $g \in C(S)$ satisfies $g|_E \in A|_E$ for every maximal $A$-antisymmetric set $E$, then $g \in A$. This theorem is a generalization of Stone-Weierstrass approximation.

Proof: The annihilator $A^\perp$ of $A$ consists of all regular complex Borel measure $\mu$ on $S$ that $\int f d\mu = 0$ for all $f \in A$ by Riesz representation (10.9.1.10). Cf. [Rudin P122].

Prop. (10.7.3.19) [Schauder Fixed Point Theorem]. If $C$ is a closed convex subset in a metrizable TVS and continuous $T : C \to C$ has sequentially compact image (e.g., $C$ is compact and $X$ is locally convex hence $X^*$ separate points), then $T$ has a fixed point.

Proof: As $T(C)$ is sequentially compact, for each $n$, there is a $1/n$-net $N_n = \{y_i\} \subset T(C)$, let $E_n = \text{span}\{N_n\}$.

Define a map $T(C) \to \text{co}(N_n) : I_n(y) = \sum y_i \lambda_i(y)$, where $\lambda_i(y) = \frac{m_i(y)}{\sum m_i(y)}$ and $m_i(y) = 1 - n||y - y_i||$ if $y \in B(y_i, 1/n)$, and 0 otherwise.

Now $||I_n(y) - y|| = ||\sum (y_i - y) \lambda_i(y)|| \leq \sum ||y_i - y|| \lambda_i(y) \leq \frac{1}{n}$ for each $y \in T(C)$. As $C$ is convex, $\text{co}(N_n) \subset C$, if we let $T_n = I_n \circ T$, then $T_n$ has a fixed pt $x_n$ in $\text{co}(N_n)$ by Brower fixed pt theorem (3.10.4.2).

As $T(C)$ is sequentially compact and $C$ is closed, there is a subsequence $T x_{n_k}$ that converges to $x \in C$. And then

$$||x_{n_k} - x|| = ||I_n T x_{n_k} - x|| \leq ||I_n T x_{n_k} - T x_{n_k}|| + ||T x_{n_k} - x|| < \frac{1}{n} + ||T x_{n_k} - x||$$

so $x_{n_k} \to x$, and then by continuity, $T x = x$. \qed
Vector-valued Integration

Def. (10.7.3.20) [Vector-Valued Integration]. Given a measure space \((Q, \mu)\) and \(X\) is an Archimedean TVS on which \(X^*\) separate points. If \(f\) is a function from \(M\) to \(X\) that \(\Lambda \circ f\) are integrable w.r.t \(\mu\) for any \(\Lambda \in X^*\). The integration \(\int_M f d\mu\) w.r.t \(Q\) is an element \(y\) that

\[ \Lambda y = \int_Q (\Lambda f) d\mu \]

for any \(\Lambda \in X^*\).

Prop. (10.7.3.21). If \(X\) is an Archimedean TVS on which \(X^*\) separate points, \((Q, \mu)\) is a Radon measure on a locally compact Hausdorff space that \(\mu\) is compactly supported, and \(f\) is continuous that \(\text{co} (f(Q))\) is compact(e.g. when \(X\) is Fréchet(10.7.3.11)), then the integral \(y = \int_Q f d\mu\) exists, and belongs to the closed linear span of the range of \(H\). Moreover if \(\mu\) is positive and \(\mu(Q) = 1\), then \(y \in \text{co} (f(Q))\).

Proof: Cf.[Rudin P78]. □

Cor. (10.7.3.22). If \(Q\) is Hausdorff, \(d\mu\) is compactly supported, \(X\) is Archimedean Banach and \(f : Q \rightarrow X\) is continuous, then

\[ ||\int_Q f d\mu|| \leq \int_Q ||f|| d\mu \]

Proof: Let \(y = \int_Q f d\mu\). By(10.7.3.6), there is a \(||\Lambda|| \leq 1\) that \(\Lambda y = ||y||\), so

\[ \Lambda y = ||y|| = \int_Q \Lambda f d\mu = |\int_Q \Lambda f d\mu| \leq \int_Q |\Lambda f| d\mu \leq \int_Q ||f|| d\mu \]

□

Prop. (10.7.3.23). If \(X\) is an Archimedean TVS on which \(X^*\) separate points, \(Q\) is a compact subset of \(X\), and \(\text{co}(Q)\) is compact, then \(y \in \text{co}(Q)\) iff there is a regular Borel measure \(\mu\) on \(Q\) that \(y = \int_Q x d\mu(x)\).

Proof: Cf.[Rudin P79]. □

Prop. (10.7.3.24)[Continuous Action Extends to Measure]. For a fixed map \(f : Q \rightarrow X\), assume \(X\) is a Fréchet space, then the integration functor in(10.7.3.21) induces a continuous map

\[ Meas_x(Q) \rightarrow X : \mu \mapsto \int_\mu f \]

that maps \(\delta_x\) to \(f(x)\).

Proof: It suffices to verify continuity: for any seminorm \(\rho\), by convexity,

\[ \rho(\int_\mu f) \leq (\mu, \rho(f)) \]

thus for \(\mu \in U\) satisfying \((\mu, \rho(f)) < 1\), \(\rho(\int_\mu f) < 1\). This proves continuity. □
Prop. (10.7.3.25) [Vector Valued Integration Stronger]. If $V$ is a Banach space and $\mu$ is a Radon measure on a locally compact Hausdorff space $X$. If $g \in L^1(\mu)$ and $H : X \to V$ is bounded and continuous, then $\int gHd\mu$ exists and belongs to the closed linear span of the range of $H$, and

$$||\int gHd\mu|| \leq \sup_{x \in X} ||H(x)|| \int |g(x)|\mu(x)$$

Proof: Clearly $\varphi(gH) \in L^1(\mu)$ for all $\varphi \in V^*$. And $\mu$ is Radon, so there is a sequence $\{g_n\} \in C_c(X)$ that converges to $g$ in $L^1$, so $\int g_nHd\mu$ is integrable by (10.7.3.21), and

$$\int ||g_n(x)H(x) - g_m(x)H(x)dx||d\mu(x) \leq \int |g_n(x) - g_m(x)|d\mu(x) \to 0$$

thus this is a Cauchy sequence, converging to some $y$. Now for any $\varphi \in V^*$,

$$\varphi(y) = \lim \varphi(\int g_nHd\mu(x)) = \lim \int \varphi \circ (g_nH)d\mu = \int \varphi \circ (gH)d\mu$$

The last equality uses boundedness again.

Moreover, each $\int g_nHd\mu$ belongs to the closed range of $H$ by (10.7.3.21), hence so does $\int gHd\mu$. And last assertion is also from (10.7.3.21).

□

Holomorphic Functions

Def. (10.7.3.26) [Holomorphic Functions]. Let $\Omega$ be an open set in $\mathbb{C}$, and $X$ be a TVS over $\mathbb{C}$, then A function $f : \Omega \to X$ is called:

- weakly holomorphic if $\Lambda f$ is holomorphic for any $\Lambda \in X^*$.
- strongly holomorphic if $\lim_{w \to z} \frac{f(w) - f(z)}{w - z}$ exists for every $z \in \Omega$.

A strongly holomorphic function is clearly weakly holomorphic, and the converse is true when $X$ is Fréchet space, by the following proposition (10.7.3.27).

Prop. (10.7.3.27) [Weak and Strong Holomorphic]. Let $\Omega$ be an open set in $\mathbb{C}$, and $X$ be a Fréchet space over $\mathbb{C}$, then $f$ is strongly continuous, and the Cauchy integral formula (10.5.2.6) holds for $f$, and $f$ is strongly holomorphic.

Proof: We may assume $0 \in \Omega$, then let $B(0, 2r) \subset \Omega$ and $\Gamma$ the boundary of $B(0, 2r)$, since $\Lambda f$ is holomorphic,

$$\frac{(\Lambda f)(z) - (\Lambda f)(0)}{z} = \frac{1}{2\pi i} \int_{\Gamma} \frac{(\Lambda f)(\zeta)}{(\zeta - z)\zeta} d\zeta \quad 0 < |z| < 2r.$$ 

Therefore $\{ \frac{f(z) - f(0)}{z} | 0 < |z| \leq r \}$ is weakly bounded, so it is also bounded by (10.7.3.12), so $f$ is strongly continuous.

The integral exists by (10.7.3.21), so $f$ satisfies Cauchy integral formula because it satisfies this when acting with any functional $\Lambda$, and $X^*$ separate points.

For the last assertion, Cf. [Rudin P84].

□

Prop. (10.7.3.28) [Liouville’s Theorem]. If $X$ is a TVS over $\mathbb{C}$ on which $X^*$ separate points and $f : \mathbb{C} \to X$ is weakly holomorphic and $f(\mathbb{C})$ is weakly bounded, then $f$ is constant.

Proof: Immediate from Liouville’s theorem (10.5.2.10).

□
4 Duality Theory

Prop. (10.7.4.1) [Banach-Alaoglu]. For a nbhd $V$ of 0 in a TVS $X$, the set

$$K = \{ f | |f x| \leq 1, \forall x \in V \}$$

is weak*-compact in $X^*$, which is called the polar $V^*$ of $V$.

Proof: Consider the Minkowski function $\gamma$ of $V$, then for each $\Lambda \in K$, $|\Lambda x| \leq \gamma(x)$. If we consider the space $P = \prod_{x \in X} |\gamma(x) - \gamma(x)|$, then $P$ is compact by Tychonoff (3.6.2.5).

The point is that the weak*-topology coincides with the pointwise convergence topology on $K$, because they have the same generating subbasis. If we show $K$ is a closed subspace of $P$, this will finish the proof that $K$ is weak*-compact. For this, consider any $f_0$ in its closure, then for each $x, y \in X, \alpha, \beta \in K$, there is a $f \in K$ that is close to $f_0$ at $x, y$ and $\alpha x + \beta y$. So $f_0$ is linear. Similarly we can show $|f_0(x)| \leq 1$ for $x \in V$, so $f_0 \in K$. □

Prop. (10.7.4.2). If $X$ is a TVS that $X^*$ separate points (e.g. locally convex), then the weak topology $X_w$ is a locally convex space, and $(X_w)^* = X^*$.

Proof: If $\Lambda$ is a functional that is continuous in $X_w$-topology, then $|\lambda x| < 1$ for some set defined by elements in $X^*$, so by (10.6.3.3), $\Lambda = \sum_\alpha \lambda \Lambda_i$, which is continuous w.r.t the original topology. □

Prop. (10.7.4.3) [Hahn Weak Topology case]. If $X$ is a TVS that $X^*$ separate points, then if $A, B$ are disjoint nonempty, compact convex sets in $X$, then there is a $\Lambda \in X^*$ that separate $A$ and $B$, i.e. $\Re f(E_1) < \gamma_1 < \gamma_2 < \Re f(E_2)$.

Proof: Let $X_w$ be $X$ with the weak topology, then the sets $A$ and $B$ are compact in $X_w$ as it’s weaker. And they are also closed because $X_w$ is Hausdorff. $X_w$ is convex, so we can use geometric Hahn (10.7.3.7). Now $(X_w)^* = X^*$, so the chosen functional is also continuous in the original topology. □

Prop. (10.7.4.4) [Dual Banach Space]. For a normed space $X$, $x \in X$ can be seen as functional on $X^*$, of norm exactly $||x||$. And the closed ball $B^*$ of the dual space $X^*$ is weak*-compact.

Proof: The first assertion is because of (10.7.3.6), the last assertion is because of Banach-Alaoglu (10.7.4.1). □

Prop. (10.7.4.5) [Adjoint Norm]. For $X, Y$ normed, the adjoint of $T : X \to Y$ satisfies $||T^*|| = ||T||$.

Proof: Use (10.7.4.4), $||T|| = \sup\{ ||(Tx, y^*)|| | ||x|| \leq 1, ||y^*|| \leq 1 \} = ||T^*||$. □

Prop. (10.7.4.6) [Closed Range Theorem]. Let $T$ be continuous mapping between Banach spaces $X$ and $Y$, let $U, V$ be open balls of $X, Y$ particularly. then the following are equivalent:

1. $||T^* y^*|| \geq \delta ||y^*||$ for some $\delta$.
2. $\delta V \subset T(U)$.
3. $\delta V \subset T(U)$, i.e. $T^{-1}$ is continuous.
4. $T(X) = Y$.
5. $T^*$ is one-to-one and $R(T^*)$ is closed in $X$. 

Proof: 1 → 2: If $||T^* y^*|| \geq \delta ||y^*||$, first prove $\delta V \subset \overline{T(U)}$. If $y_0 \notin \overline{T(U)}$, since $\overline{T(U)}$ is convex closed and balanced, geometric Hahn shows that there is a $y^*$ that $|y^*(y)| \leq 1$ for every $y \in T(U)$, and $|y^*(y_0)| > 1$. Then if follows $||T^* y^*|| \leq 1$. So

$$\delta < \delta |y^*(y_0)| \leq \delta ||y_0|| ||y^*|| \leq ||y_0|| ||T^* y^*|| \leq ||y_0||$$

This shows $\delta V \subset \overline{T(U)}$.

2 → 3: may assume $\delta = 1$. Then $V \subset \overline{T(U)}$. Then for every $y \in Y$ and every $\varepsilon > 0$, there is a $x$ that $||x|| \leq ||y||$ and $|y - Tx| < \varepsilon$. For any $y_1 \in V$, pick $\varepsilon > 0$ that $\sum \varepsilon_n < 1 - ||y_1||$, then choose $||x_n|| \leq ||y_n||$ that $||y_n - Tx_n|| < \varepsilon_n$, and let $y_{n+1} = y_n - Tx_n$. Then it is verified that $x = \sum x_n \in U$ and $Tx$.

3 → 1: $||T^* y^*|| = \sup \{\langle x, T^* y^* \rangle | x \in U \} = \sup \{\langle y, y^* \rangle | y \in V \} = \delta ||y^*||$.

3 $\iff$ 4: By Open mapping theorem.

4 $\iff$ 5: $T^*$ is injective by (10.6.3.2). By open mapping theorem, $T^*$ is a multiple of a dilation, so $R(T^*)$ is closed by (3.6.8.9).

5 $\iff$ 4: $R(T)$ is dense in $Y$ by (10.6.3.2), and it is closed by the proposition (10.7.4.7) below. □

**Prop. (10.7.4.7) [Closed Range Theorem].** If $X, Y$ are Banach spaces and $T \in L(X, Y)$, the following are equivalent:

1. $R(T)$ is closed in $Y$.
2. $R(T^*)$ is weak*-closed in $X^*$.
3. $R(T^*)$ is closed in $X$.

**Proof:** 1 $\rightarrow$ 2: As $N(T)^\perp$ is the weak*-closure of $R(T^*)$, it suffices to prove $N(T)^\perp \subset R(T^*)$. As $R(T)$ is complete, the open mapping theorem applies to $X \rightarrow R(T)$, showing that each $y \in R(T)$ corresponds to an element $x \in X$ that $Tx = y$ and $||x|| \leq K ||y||$.

For $x^* \in N(T)^*$, define a functional $\Lambda$ on $R(T)$ by $\Lambda T x = \langle x, x^* \rangle$, this is well-defined, and $|\Lambda y| = \Lambda T x \leq K ||y|| ||x^*||$. So it is continuous and by Hahn=Banach some continuous functional $y^* \in Y^*$ extends $\Lambda$. Then $\langle Tx, y^* \rangle = \Lambda T x = \langle x, x^* \rangle$, so $x^* = T^* y^*$ is in the image of $T^*$, so we are done.

3 $\rightarrow$ 1: let $Z = \overline{R(T)}$. $RT$ is dense in $Z$, so (10.6.3.2) shows $T^* : Z^* \rightarrow X^*$ is injective. And for each $z^* \in Z^*$, there is an extension $y^*$ by Hahn-Banach, and then $\langle x, T^* y^* \rangle = \langle Tx, y^* \rangle = \langle Tx, z^* \rangle = \langle x, T^* z^* \rangle$, so $T^* (Y^*) = T^* (Z^*)$, which is closed by hypothesis.

Now use open mapping theorem for $Z^* \rightarrow R(T^*)$, then there is a $c$ that $c ||z^*|| \leq ||T^* z^*||$. So $T : X \rightarrow Z$ is surjective, by (10.7.4.6). So $R(T) = Z$ is closed. □

**Prop. (10.7.4.8).** In a normed space, if $x_n \rightarrow x$ weakly, then $\lim |x_n| \geq ||x||$.

**Proof:** Choose a functional that $||f|| = 1$ and $|f(x)| = 1$ by (10.7.3.6), then use the definition of weak convergence. □

**Prop. (10.7.4.9) [Eberlein-Smulian].** For a set $A$ in a Banach space $X$, $A$ is weak*–sequentially compact if its weak precompact.

**Proof:** We prove here that the case that the closed unit ball of a reflexive Banach space is weakly*–self sequentially compact.

To prove this, first we show that a bounded sequence has a subsequence that is weak*–convergent in $X$. Let $X_0 = \text{span} \{x_n\}$, then $X_0$ is reflexive by (10.7.4.13), and it is separable, so $X_0$ is separable by (10.7.4.11). Then the result follows from (10.7.4.14).

Finally, the weak limit $x$ is in the closed unit ball, by (10.7.4.8). □
Reflexive and Separable

Def. (10.7.4.10) [Reflective Banach Space]. If $X$ is a Banach space, there is an isometric immersion of $X$ onto a closed subspace of $X^{**}$ (closed because $X$ is complete). $X$ is called reflexive iff $X \cong X^{**}$.

Prop. (10.7.4.11) [Separability Banach]. For a normed space $X$, if $X^*$ is separable, then $X$ is separable.

Proof: Choose a countable dense set in $X^*$, then their projection to the unit sphere $S^*$ $\{g_n\}$ are dense in $S^*$ (easily checked), and choose for each of them a $x_n$ that $||x_n|| = 1$ and $g_n(x_n) > \frac{1}{2}$.

Now I claim $x_n$ are dense in $X$, i.e. $X_0 = \text{span}\{x_n\} = X$. If this is not the case, then there is a $||x|| = 1$ not in $X_0$, so by (10.7.3.6), there is a $f$ that $f(X_0) = 0$ and $||f|| = 1$ and $f(x) = 1$. Then $||g_n - f|| = \sup_{||x|| = 1} |g_n(x) - f(x)| \geq |g_n(x_n) - f(x_n)| = |g_n(x_n)| \geq 1/2$, contradicting the fact $g_n$ is dense in $S^*$.

□

Prop. (10.7.4.12) [Duality Exact]. If $X$ is a closed subspace of a normed space $Y$, and $Y/X$ is the quotient field, then $(Y/X)^*$ is a closed subspace of $Y^*$, and $X^*$ is the quotient.

Proof: $(Y/X)^* \to Y^*$ is clearly injective, and the $X^*$ are all functionals on $Y$ modulo the functionals that vanish on $X$.

□

Cor. (10.7.4.13) [Pettis]. Closed subspace and quotient space of a reflexive normed space is reflexive.

Proof: Use the fact that $0 \to X \to Y \to Z \to 0$ induces an exact sequence $0 \to X^{**} \to Y^{**} \to Z^{**} \to 0$, and there is a map $X \to X^{**}$, so we can use snake lemma (as modules).

□

Prop. (10.7.4.14) [Separable Ball Weak*-Sequentially Compact]. If a normed space $X$ is separable, then the closed unit ball of $X^*$ is weak*-sequentially compact.

Proof: Let $x_n$ be a countable dense subset of $X$, then by diagonal method, for each bounded sequence of $f_n \in X^*$, there is a subsequence $f_{nk}$ that $f_{nk}(x_m)$ converges for each $x_m$. Then by (10.6.2.3), $f_{nk}$ converges to some $f \in X^*$. So the theorem is finished.

□

Prop. (10.7.4.15) [Reflexive Ball Weak*-Sequentially Compact]. In a reflexive Banach space $X$, then a set in $X$ is bounded iff it is weak*-sequentially compact.

Proof: If it is reflexive, then the unit ball is weak*-compact by Alaoglu, so it is weak*-sequentially compact by Eberlein (10.7.4.9). Conversely, if it is weak*-sequentially compact, then its closure is weak*-compact, thus bounded.

□

Prop. (10.7.4.16). A closed convex set of a reflexive Banach space attains minimal norm.

Proof: By Hahn, a closed convex set is weakly closed. Let $d = \inf \{||x||\}$, then if $d \leq ||x_n|| < d + q/n$, then $\{x_n\}$ is bounded, so by (10.7.4.15) it is weak-sequentially compact (10.7.4.9), thus some $x_n \to x$ weakly. and use (10.7.4.8), $x$ must attains minimal norm $d$.

□

5 Compact Operator & Fredholm Operator

Def. (10.7.5.1) [Compact Operators]. A compact operator is an operator between Banach spaces that maps bounded set to sequentially compact (equivalently precompact or totally bounded (3.6.8.6)) set. It is necessarily continuous because the norm function is continuous thus $||Tx||$ is bounded on the unit ball. The set of compact operators between $X,Y$ is denoted by $\mathcal{C}(X,Y)$.
Prop. (10.7.5.2) [Examples of Compact Operators].
- Let $X$ be a compact measure space and $Lu(x) = \int_X K(x,y)u(y)\,dy$ for $K \in C(X \times X)$. This is a compact operator on $C(X)$ by Arzela-Ascoli (3.6.8.7).
- Let $\Omega$ be a $\sigma$-finite measure space and $Lu(x) = \int_{\Omega} K(x,y)u(y)\,dy$ for $K(x,y) \in L^2(\Omega \times \Omega)$. This is a compact operator on $L^2(\Omega)$, as it is Hilbert-Schmidt (10.8.5.5) (10.8.5.3).

Prop. (10.7.5.3) [Properties of Compact Operators].
1. For a continuous operator, it has f.d. image iff it is compact and the image is closed.
2. The space of compact operator is a closed subspace of $L(X,Y)$. Thus the limit of f.d. operators is compact.
3. If one of $A$ or $B$ is compact and the other is continuous, then $AB$ is compact, because continuous maps bounded to bounded and compact to compact.

Proof:
1. A finite dimensional space is closed by (10.7.1.8), and a finite dimensional space is Heine-Borel (3.6.5.2), so it maps closed ball to precompact set, as it is continuous. Conversely, if it is compact and the image is closed, then it is an open map to its image, by open mapping theorem, and the image is locally compact because $T$ is compact, so it has finite dimension (10.7.1.7).
2. $S + T$ is continuous because sum of precompact set is precompact. To show it is closed subspace, Use totally bounded definition, for $T$ is the closure, let $||S - T|| < r$, then if $S(x_i)$ is a $r$-net for $S(B(0,1))$, then $T(x_i)$ is a $3r$-net for $T(B(0,1))$.
3. Because continuous function preserves both boundedness and (pre)compactness.

Prop. (10.7.5.4) [Compact and Totally Convergence]. Let $x_n \to x$ weakly, if $T$ is compact, then $T x_n \to T x$ strongly. The converse is true when $X$ is reflexive. In particular, this applies to Hilbert space.

Proof: Assume the contrary, if $T x_n$ doesn’t converge to $T x$, there is a subsequence $x_{n_k}$ that $||T x_{n_k} - T x|| \geq \varepsilon_0$. Now $\{x_n\}$ is bounded by (10.6.3.5), so by $T$ compact, there is a subsubsequence $T x_{n_{k_l}} \to z$ strongly. But because $x_{n_i} \to x$ weakly, $T x_{n_i} \to T x$ weakly because $T$ is continuous, and thus $z = T x$.

The converse is by Eberlein (10.7.4.9), because the bounded $x_n$ has a weak convergent subsequence, and it is mapped to convergent sequence by $T$.

Prop. (10.7.5.5). $T$ is compact $\iff T^*$ is compact.

Proof: We need only to show that $T^* y_n^*$ has a uniformly convergent subsequence on the unit sphere, but for this it suffice to prove $y_n^*$ is sequentially compact in $C(T(B(0,1)))$. And we use Arzela-Ascoli because $\overline{T(B(0,1))}$ is compact. For the other half, use the double dual space.

Lemma (10.7.5.6). If there is a chain of closed subspaces $M_1 \subset M_2 \subset \ldots$ that $T(M_n) = M_n$ and $(T - \lambda_n I) M_n \subset M_{n-1}$ for some $\lambda_n \in \sigma(A) - B(0,r)$, then $T$ is not compact.

Proof: There are $y_n \in M_n$ that $||y_n|| \leq 1$ and $||y_n - x_n|| \geq 1/2$ for $x \in M_{n-1}$, so if $m < n$, $||T y_m - T y_n|| = ||\lambda y_n - (T y_m - (T - \lambda_n) y_n)|| \geq \frac{||y_n||}{2} \geq \frac{r}{2}$, so $T y_n$ has no convergent subsequence.
Lemma (10.7.5.7). If $A$ is compact and $T = 1 - A$, then if $T$ is not injective, then it is not surjective. And for any $r > 0$, $\sigma_p(A) - B(0, r)$ is a finite set.

Proof: We use (10.7.5.6). If $R(T) = X$, then let $M_n = N(T^n)$, then $M_0 \neq 0$ because there is a $Tx_0 = 0$, and $M_n \subset M_{n+1}$ because there is a $T^n x_{n+1} = x_0$, so $x_{n+1} \in M_{n+1} - M_n$.

If $\sigma_p(A) - B(0, r)$ is infinite, then choose $M_n$ to be generated by $n$ eigenvectors, then it is clear that a chain like above will be found.

Lemma (10.7.5.8). If $A$ is compact and $T = 1 - A$, then $R(T)$ is closed.

Proof: it suffices to show $T^{-1} : R(T) \to X/N(T)$ is continuous, if this is not the case, then there is a sequence $\|x_n\| = 1$ but $Tx_n \to 0$. But $A$ is compact, so there is a subsequence that $Ax_{n_k} \to z$, so $x_{n_k} \to z$. So $Tz = 0$ so $z = 0$, but then $x_{n_k} \to 0$, contradiction.

Prop. (10.7.5.9)[Riesz-Fredholm]. For a compact operator $A \in L(X)$, let $T = I - A$. Then:

1. $0 \in \sigma(A)$ if $X$ is not f.d.
2. $T$ is Fredholm of index 0 (10.7.5.17). Equivalently, $\sigma(A) \setminus \{0\} = \sigma_p(A) \setminus \{0\}$ (because either $T$ not injective or $T$ is surjective).
3. $\sigma(A)$ has at most one convergent point 0 (it must attain 0 if $X$ is a infinite-dimensional).

Hence it has at most countable spectrum.

Proof: 1: If 0 is a regular value, then $T$ is invertible, thus $T^{-1}T = \text{id}$ is compact, thus $X$ has f.d. (10.7.1.7).

2: Firstly $\dim N(T) < \infty$. This is because $T|_{N(T)} = \text{id}_{N(T)}$, so it is compact iff it is f.d. (10.7.5.3). by [Rudin P108].

3: By (10.7.5.7).

Prop. (10.7.5.10)[Lomonosov’s Invariant Subspace Theorem]. If $X$ is an infinite dimensional complex Banach space, and $T \neq 0$ is a compact operator in $L(X)$, then there is a proper closed subspace $M$ of $X$ that is invariant under $S$ for any $S$ that commutes with $T$.

In particular, if $S$ commutes with some compact operator $T$, then $S$ has an invariant closed subspace.

Proof: If $\Gamma$ is the subspace of all operators that commutes with $T$, then it is a subalgebra of $L(X)$, and for each $y \in X$, let $\Gamma(y) = \{Sy \subset \Gamma\}$, then $\Gamma(y) \subset \Gamma(y)$, then so does the closure of $\Gamma(y)$. So if the proposition is false, then $\Gamma(y)$ is dense in $X$ for each $y$.

Pick $x_0$ that $Tx_0 \neq 0$, then there is an open ball $B$ of $x_0$ that $\|Tx_0\| \geq \frac{1}{2} \|x_0\|$.

Now our assumption shows that for every $y \neq 0$, there is a nbhd $W$ of it that maps into $B$ by some $S \subset \Gamma$ (notice $\Gamma$ is a subspace).

Now $K = \overline{T(B)}$ is compact because $T$ is compact, so there are f.m. open sets $W_i$ whose union cover $K$, and $S_i(W_i) \subset B$, where $S_i \subset \Gamma$. Now let $\mu = \max\{|S_i|\}$. Consider $Tx_0 \in K$, so there is a $S_i Tx_0 \in B$, then $TS_i Tx_0 \in K$, so there is a $S_{i_2} TS_{i_1} Tx_0 \in B$. Continuing this way, we get

$$\frac{1}{2} \|x_0\| \leq \|x_N\| \leq \mu^N \|T^N\| \|x_0\|,$$

so by Gelfand theorem (10.8.1.8), $\rho(T) > 0$, so there is an eigenvalue $\lambda$ of $T$ (by (10.7.5.9)) that $N(T - \lambda I)$ is finite dimensional, so not equal to $X$, and it is clearly invariant under $\Gamma$. 

\hfill \Box
Prop. (10.7.5.11) [Jordan Decomposition for Compact Operators]. For a compact operator $A$ and all the non-zero eigenvalues $\lambda_i$, we can find a subspace
\[
\bigoplus_{i=1}^{\infty} N((\lambda_i - A)\rho_i), \quad \lambda_i \neq 0
\]
on which $A$ has a Jordan form.

Proof: Let $T = 1 - A$, By (2.2.4.5), we only have to prove there are some $m, n$ that There is a $p$ that $N(T^p) = N(T^{p+1})$ and a $q$ that $R(T^q) = R(T^{q+1})$, because then we have a decomposition $X = N((T - \lambda I)\rho) \oplus R((T - \lambda I)\rho)$, and all these $N((T - \lambda I)\rho)$ are pairwise disjoint.

Now $q < \infty$, because if $R(T) \supset R(T^2) \supset \ldots$, because $T^k$ is of the form $1 +$ compact operator, $R(T^k)$ are all closed by (10.7.5.8), so by (10.7.5.6), this is impossible.

For $p$, use Riesz-Fredholm (10.7.5.9),
\[
\dim N(T^q) = \text{codim}R(T^q) = \text{codim}R(T^{q+1}) = \dim N(T^{q+1}) < \infty
\]
So $p \leq q < \infty$. \qed

Prop. (10.7.5.12). If $X, Y$ are Banach spaces and $T, K \in L(X, Y)$, $K$ is compact and $R(A) \subset R(K)$, then $A$ is compact.

Proof: Use (10.6.2.9), then we can lift the function to a map $\tilde{T} : X \to X/N(K)$, which is also continuous, so $T = \tilde{K} \to \tilde{T}$ is also compact. \qed

Schauder Basis

Def. (10.7.5.13) [Schauder Basis]. Let $X$ be a Banach space, a sequence $e_n$ is called a Schauder basis iff for any $x \in X$, there is a unique sequence $C_n(x)$ that $x = \lim \sum_{n=1}^{N} C_n(x)e_n$. Notice in this case $X$ is automatically separable.

Prop. (10.7.5.14). If $X$ has a Schauder basis, then $C_n(x)$ are continuous functional on $X$.

Proof: Consider the module $||x||_1 = \sup ||S_n x||$. Firstly, it is complete, because $||x|| = \lim ||S_N x|| \leq ||x||_1$, so if there is a Cauchy sequence $\{x_i\}$ in $|| \cdot ||_1$, then it is a Cauchy sequence in $|| \cdot ||$, then it converges to some $x$. Now $C_n(x) = S_n(x_i) - S_{n-1}(x_i)$ are all Cauchy sequence, uniform in $N$, so they convere to some sequence $C_N$.

It is left to verify that $s_N = \sum_{j=1}^{N} c_n e_n$ converges to $x$, because then it is easy to verify that $\lim ||x_i - x||_1 = 0$. For this, choose $N_1$ large that $||x_n - x|| \leq \varepsilon$ for $n \geq N_1$, and choose $N_2$ large that $||s_k(x_n) - s_k|| \leq \varepsilon$ for all $k$ and $n \geq N_2$. Then for $x_{N_1 + N_2}$, there is a $N_3$ that $||S_n x_{N_1 + N_2} - x_{N_1 + N_2}|| \leq \varepsilon$, so $||x_k - s_k|| \leq ||x_{N_1 + N_2}|| + ||S_k(x_{N_1 + N_2} - x_{N_1 + N_2})|| + ||s_k(x_{N_1 + N_2}) - s_k|| \leq 3\varepsilon$ for $k$ large.

Now by Banach (10.6.2.6), $||x||_1 \leq M||x||$ for some $M$, so $|C_n(x)e_n| \leq 2M||x||$ and $C_n$ is continuous. \qed

Prop. (10.7.5.15). If $X$ has a Schauder basis, then any compact operator is a limit of operators of f.d. range.

Proof: Let $S_N(x) = \sum_{n=1}^{N} C_n(x)e_n$, it is continuous by (10.7.5.14). And it converges, so $||S_N|| \leq M$, by Banach-Steinhaus (10.6.2.1).

For any compact operator, we want to find f.d. range operator $T_i$ that $T_i \to T$. For this, given any $\varepsilon > 0$, because $\overline{T}(B(0, 1))$ is compact, there are operators that is a $\varepsilon/M^2$-net $y_i$, then choose $N$ large enough that $|S_N y_i - y_i| \leq \varepsilon/M^2$, then for any $x$, there is a $y_i$ that $|T x_i - y_i| < \varepsilon/M^2$, so $|S_N T x_i - S_N y_i| < \varepsilon/M$, and then $|S_N T x - T x_i| < \varepsilon$, and notice $S_N T$ has f.d. range. \qed
Prop. (10.7.5.16) [Compact Operator as Limits of F.D. Operators]. Any compact operator on a Hilbert space is a limit of f.d. operators.

Proof: Cf. [Trace Classes and Hilbert-Schmidt Operators, Thm10]. □

Fredholm Operator

Def. (10.7.5.17) [Fredholm Operator]. A bounded operator between Banach space is called a Fredholm operator if \( \dim N(T) < \infty \) and \( \text{codim} R(T) < \infty \). It necessarily has closed image by (10.6.2.10), so \( R(T) = N(T^*)^\perp \) (10.6.3.2).

The index of a Fredholm operator is defined as \( \text{ind}(T) = \dim N(T) - \text{codim} R(T) \), thus for a compact operator \( A \), \( I - A \) has index 0, by (10.7.5.9).

Prop. (10.7.5.18). For a Fredholm operator between Banach space, we have

\[
X = N(T) \oplus R(T) \quad Y = Y/R(T) \oplus R(T)
\]

and \( X/N(T) \cong R(T) \).

Proof: Because \( R(T) \) and \( N(T) \) are finite/cofinite hence closed and complemented by (10.7.1.9). If \( X = N(T) \oplus M_1 \) and \( Y = R(T) \oplus M_2 \), then \( M_1 \cong X/N(T) \), \( X/N(T) \cong R(T) \) and \( M_2 \cong Y/R(T) \) by Banach theorem. □

Prop. (10.7.5.19) [Characterizing Fredholm Operator]. \( T \) is Fredholm from \( X \) to \( Y \) iff there exist a bounded \( S_1, S_2 \) from \( Y \) to \( X \) that \( S_1T = I - A_1, TS_2 = I - A_2 \), where \( A_1, A_2 \) is compact. If this is the case, \( S_1 \) and \( S_2 \) can be chosen the same as \( S \), then \( S \) is called the regulator of \( T \), and \( S \) is Fredholm as well.

So the Fredholm operator is the set of operators invertible 'modulo compact ones'.

Proof: By (10.7.5.18) \( T : X/N(T) \cong R(T) \), and there is a projection of \( \pi : Y \to R(T) \). Thus we composed them to get a \( S = T^{-1} \circ \pi : Y \to X \). And \( ST \) and \( TS \) are both 1 minus a projection with f.d. image, hence compact (10.7.5.3).

For the converse, \( R(T) \supseteq R(1 - A_2) \) is of finite codimension because \( 1 - A_2 \) is Fredholm, and \( N(T) \subseteq N(1 - A_1) \) is of finite dimension because \( 1 - A_1 \) is Fredholm. □

Cor. (10.7.5.20). The set of Fredholm operators is closed under composition. Index is a locally constant function on it, and \( \text{ind}(T_1T_2) = \text{ind}(T_1) + \text{Ind}(T_2) \).

Proof: There is a long exact sequence (use (3.3.4.4) in the category of vector spaces)

\[
0 \to \ker T_2 \to \ker T_1T_2 \to \ker T_2 \to \text{Coker} T_2 \to \text{Coker} T_1T_2 \to \text{Coker} T_1 \to 0.
\]

which shows the composition and index is additive.

For the openness and locally constancy, use (10.7.5.19), when adding a small \( R \), \( S(T + R) = 1 - A_1 + SR \), and if when \( ||R|| < ||S||^{-1} \), \( E_1 = (I + RS)^{-1} \) is bounded, so \( E_1S(T + R) = I - E_1A_1 \), and similarly does \( (T + R)SE_2 \), so \( T + R \) is Fredholm. And \( \text{ind} E_1 + \text{ind} S + \text{ind}(T + R) = \text{ind}(1 - E_1A_1) = 0 \), and \( \text{ind} E_1 = 0 \) because it is invertible, and \( \text{ind} S + \text{ind} T = \text{ind}(1 - A_1) = 0 \), so \( \text{ind} T = \text{ind}(T + R) \). □

Cor. (10.7.5.21). If \( T \) is Fredholm and \( A \) is compact, then \( T + A \) is Fredholm, and \( \text{ind}(T + A) = \text{ind} T \), so \( \text{ind} \) is in fact defined on the quotient of \( L(X,Y) \) by compact operators.
Proof: It is Fredholm by (10.7.5.19), and we notice $S(T + A)$ and $ST$ are both 1 minus compact operators, thus (10.7.5.20) and (10.7.5.9) gives the result.

\[ \square \]

Cor. (10.7.5.22). If $T$ is Fredholm, then $T^*$ is Fredholm, and $\text{ind}(T^*) = - \text{ind}(T)$.

Proof: The first follows from (10.7.5.19) and (10.7.5.5). For the second, use the fact $R(T)$ and $N(T)$ are all closed.

\[ \square \]

6 Unbounded Operators
10.8 Archimedean Banach Algebra

Main references are [Functional Analysis, Rudin].

1 Banach Algebra

Def. (10.8.1.1) [Spectrum]. For a bounded operator \( A \in L(X) \) where \( X \) is Banach space, a \( \lambda \in \mathbb{C} \) is called a:

- **point spectrum** if \( \lambda I - A \) is not injective;
- **continuous spectrum** if it is not a point spectrum and \( R(\lambda I - A) \neq X \) but \( \overline{R(\lambda I - A)} = X \).
- **residue point** if it is not a point spectrum and \( \overline{R(\lambda I - A)} \neq X \).
- **regular point** if \( \lambda I - A \) is injective and \( R(\lambda I - A) = X \), in which case \( (\lambda I - X)^{-1} \) is continuous, by Banach.

denote \( \sigma(A) = K - \) regular points of \( A \) the **spectrum** of \( A \), and \( \rho(A) = \sup\{|\lambda| : \lambda \in \sigma(A)\} \) is called the **spectral radius** of \( A \).

Prop. (10.8.1.2). If \( A \) is a Banach algebra and \( x \) is invertible in \( A \), and \( h \in A \) satisfies \( ||h|| < \frac{1}{2}||x^{-1}||^{-1} \), then \( x + h \) is also invertible and

\[
||((x + h)^{-1} - x^{-1} + x^{-1}hx^{-1})|| \leq 2||x^{-1}||^3||h||^2
\]

*Proof:* \( x + h = x(e + x^{-1}h) \) and \( ||x^{-1}h|| < \frac{1}{2} \), so \( x + h \) is invertible by (10.8.1.14), and \( ||(x + h)^{-1} - x^{-1} + x^{-1}hx^{-1}|| = ||(e + x^{-1}h)^{-1} - e + x^{-1}h||x^{-1}|| \leq 2||x^{-1}||^3||h||^2 \) also by (10.8.1.14).

□

Cor. (10.8.1.3). If \( A \) is a Banach algebra, then the invertible elements \( G(A) \) is an open subset of \( A \), and the mapping \( x \mapsto x^{-1} \) is a homeomorphism of \( G(A) \) onto \( G(A) \).

Prop. (10.8.1.4). For \( T \in L(X) \) where \( X \) is Banach space, \( \mathbb{C} \setminus \sigma(T) \) is an open set and \( \lambda \to (\lambda I - T)^{-1} \) is a holomorphic function on \( \mathbb{C} \setminus \sigma(T) \).

Thus for every bounded operator \( T \) on a Banach space, \( \sigma(T) \) is not empty.

*Proof:* The first assertion is by (10.8.1.3), for the second, let \( f(\lambda) = (\lambda e - x)^{-1} \) is defined on \( \Omega = \mathbb{C} - \sigma(x) \) and (10.8.1.2) shows

\[
||f(\mu) - f(\lambda) + (\mu - \lambda)f^2(\lambda)|| \leq 2||f(\lambda)||^3|\mu - \lambda|^2
\]

so \( \lim_{\mu \to \lambda} \frac{f(\mu) - f(\lambda)}{\mu - \lambda} = -f^2(\lambda) \), which means that \( f \) is strongly holomorphic in \( \Omega \).

Now if \( |\lambda| > ||x|| \), then \( |f(\lambda)| = |\lambda^{-1}e + \lambda^{-2}x + \ldots | \leq |\frac{1}{|\lambda||x||} | \), so \( \sigma(x) \) cannot be empty by Liouville theorem (10.7.3.28).

□

Cor. (10.8.1.5)[Gelfand-Mazur]. If in a Banach algebra \( A \) over \( \mathbb{C} \), all the nonzero element is invertible, then it is isomorphic to \( \mathbb{C} \).

*Proof:* Any nonzero element \( x \) has a nonempty spectrum, so there is a \( \lambda(x) \) that \( x - \lambda(x)e \) is not invertible, so it must be 0. That is, the mapping \( \mathbb{C} \to A : \lambda \mapsto \lambda e \) is bijective, so is is isomorphism by Banach. □
Prop. (10.8.1.6). Notice \((I - T)\) is invertible for \(||T|| < 1\) and the inverse can be calculated by definition.

In particular, for a Banach algebra \(A\) and any \(x \in A\), when \(\lambda > ||x||\), \(e - \lambda^{-1}x\) is invertible, so the spectrum of \(x\) is bounded. Now that its complement is open as the inverse image of \(G(A)\) by \(\lambda \mapsto \lambda e - x\), so the spectrum of \(x\) is compact.

Cor. (10.8.1.7) [Spectrum is Continuous]. The spectrum of an element of a Banach algebra is continuous, i.e. if \(\sigma(x) \subset \Omega\) for some open subset \(\Omega \subset \mathbb{C}\), then there is a \(\delta > 0\) that \(\sigma(x + y) \subset \Omega\) for \(||y|| < \delta\).

Proof: As \(||(\lambda e - x)^{-1}\||\) is a continuous function of \(\lambda\) in the complement of \(\sigma\), and since the norm tends to 0 as \(\lambda \to \infty\), there is a \(M\) that \(||(\lambda e - x)^{-1}|| < M\) for all \(\lambda \notin \Omega\). Now if \(||y|| < 1/M\) and \(\lambda \notin \Omega\), then \((\lambda e - x)^{-1}y\) is invertible.

Prop. (10.8.1.8) [Gelfand]. The spectrum radius \(\rho(A) = \lim_{n \to \infty} ||A^n||^{\frac{1}{n}} = \inf ||A^n||^{\frac{1}{n}} \leq ||A||\).

This formula is remarkable, as the LHS depends only on the algebraic structure, and the RHS depends on the metric structure.

Proof: For \(r > \rho(x)\)

\[
x^n = \frac{1}{2\pi i} \int_{T_r} \lambda^n f(\lambda) d\lambda.
\]

Let \(M(r) = \max ||f(re^{i\theta})||\), then \(||x^n|| \leq r^{n+1}M(r)\), hence \(\limsup ||x^n||^{1/n} \leq r\), so \(\limsup ||x^n||^{1/n} \leq \rho(x)\).

For the converse, if \(\lambda \in \sigma(x)\), then \(\lambda^n \in \sigma(x^n)\), because \(\lambda^n e - x^n = (\lambda e - x)(\lambda^{n-1}e + \ldots + x^{n-1})\), and this two commutes. So \(|\lambda^n| \leq ||x^n||\), so \(\rho(x) \leq \inf ||x^n||^{1/n}\). □

Prop. (10.8.1.9). \(\sigma(A) = \sigma(A^*)\).

Proof: It suffices to show if \(T\) is invertible iff \(T^*\) is invertible. If \(T\) is invertible, then \(T^*\) is invertible with inverse \((T^{-1})^*\). Conversely, if \(T^*\) is invertible, then \(T^{**}\) is invertible, so, as the restriction of \(T^{**}\), \(T\) is injective and image is closed. If the image is not \(X\), then there is a \(f\) that vanish on the image, so \(T^* f = 0\), but then \(f = 0\). □

Prop. (10.8.1.10). In a Banach algebra \(A\), \(e - xy\) is invertible iff \(e - yx\) is invertible, thus \(\sigma(xy) \cup \{0\} = \sigma(yx) \cup \{0\}\).

Proof: Let \(z = (e - xy)^{-1}\), then we claim \(e + yzx\) is just the inverse of \(e - yx\): \((e - yx)(e + yzx) = e - yx + yzx - yzx = (e + yzx) - yz = e\). □

Lemma (10.8.1.11). If \(A\) is a Banach algebra and \(x_n \in G(A)\) converges to \(x \notin G(A)\), then \(||x_n^{-1}|| \to \infty\).

Proof: If \(||x_n^{-1}|| < M\), choose \(n\) that \(||x_n - x|| < 1/M\), then \(||e - x_n^{-1}x|| = ||x_n^{-1}(x_n - x)|| < 1\), so \(x_n^{-1}x\) is invertible, so \(x\) is invertible. □

Prop. (10.8.1.12). For Banach algebra \(B\) and its closed subalgebra \(A\), \(\sigma_B(x) \subset \sigma_A(x)\) by filling some holes. So when \(\sigma_B(x)\) doesn’t separate \(\mathbb{C}\) or \(\sigma(A)\) has empty interior, then \(\sigma_A(x) = \sigma_B(x)\).

Proof: Cf. [Rudin P256]. □
Prop. 10.8.1.13. If $A$ is a Banach algebra over $\mathbb{C}$ that $\|x\|\|y\| \leq M\|xy\|$ for some fixed $M$, then $A$ is isomorphic to $\mathbb{C}$.

Proof: If $y$ is a boundary pt of $G(A)$, $y = \lim y_n$, then $\|y_n^{-1}\| \to \infty$. But $\|y_n\|\|y_n^{-1}\| \leq M\|e\|$, so $y_n \to 0$, so $y = 0$.

But any boundary point of $\sigma(x)$ gives a boundary point $\lambda e - x$ of $G(A)$, so $x = \lambda e$, so $A \cong \mathbb{C}$. □

Complex Homomorphism

Prop. 10.8.1.14. Suppose $A$ is a Banach algebra over $\mathbb{C}$, $x \in A$ satisfies $\|x\| < 1$, then $||(e - x)^{-1} - e - x|| \leq \frac{\|x\|^2}{1 - \|x\|}$, and $|\varphi(x)| < 1$ for any complex homomorphism $\varphi$ on $A$. In particular, any complex homomorphism is continuous.

Proof: $||(e - x)^{-1} - e - x|| = ||x^2 + x^3 + \ldots|| \leq \sum_{n=2}^{\infty} ||x||^n = \frac{\|x\|^2}{1 - \|x\|}$.

For the second, notice $e - \lambda^{-1}x$ is invertible for each $|\lambda| \geq 1$, so $1 - \lambda \varphi(x) \neq 0$, so $\varphi(x) \neq \lambda$. □

Prop. 10.8.1.15[Gleason-Kahane-Zelazko]. If $\varphi$ is a linear functional on a Banach algebra $A$ over $\mathbb{C}$, if $\varphi(e) = 1$ and $\varphi(x) \neq 0$ for every invertible element $x \in A$, then $\varphi$ is a complex homomorphism.

Proof: Cf.[Rudin P251]. □

Symbolic Calculus

Prop. 10.8.1.16[Symbolic Calculus]. For a Banach algebra $A$. For a domain $\Omega$ in $\mathbb{C}$, define $A_\Omega$ as the set of $x$ that $\sigma(x) \in \Omega$, it is an open set by (10.8.1.7), then:

$$f \mapsto \tilde{f}(x) = \frac{1}{2\pi i} \int_{\Gamma} f(\lambda)(\lambda e - x)^{-1}d\lambda$$

for any contour $\Gamma$ that surrounds $\sigma(x)$, is a continuous algebra isomorphism of $H(\Omega)$ into the set of $A$-valued functions on $A_\Omega$ with the compact-open topology.

We have $\overline{g \circ f} = \tilde{g} \circ \tilde{f}$.

Proof: The nontrivial part is that this map is multiplicative, but for this we can use Runge’s theorem to approximate any function on $\sigma(x)$. □

This theorem makes it possible to implant complex analysis to the study of Banach Algebra.

Cor. 10.8.1.17. $\exp(x)$ is defined on $A$ and is continuous. If $\sigma(x)$ doesn’t separate 0 from $\infty$, then $\log(x)$ is defined but might not be continuous.

Prop. 10.8.1.18[Spectral Mapping Theorem]. $\tilde{f}(x)$ is invertible in $A$ iff $f(\lambda) \neq 0$ on $\sigma(x)$. Thus we have $\sigma(\tilde{f}(x)) = f(\sigma(x))$.

Prop. 10.8.1.19. If $f$ doesn’t vanish identically on any component of $\Omega$, then $f(\sigma_p(T)) = \sigma_p(\tilde{f}(T))$. Cf.[Rudin P266].
\textbf{Lemma (10.8.1.20).} For \( A \) a commutative Banach algebra, the set of maximal ideals has codimension 1 corresponds to kernels of complex homomorphisms to \( \mathbb{C} \). (Consider the quotient space and use Gelfand-Mazur). Note that a complex homomorphism is all continuous because \( \lambda e - x \) maps to nonzero.

\( \lambda \in \sigma(x) \) iff there is a complex homomorphism \( h \) s.t. \( h(x) = \lambda \). (Because \( x \) is invertible iff it is not contained in any proper ideal of \( A \).

\textit{Proof:} \qed

\textbf{Prop. (10.8.1.21)[Gelfand Transform].} The spectrum \( \Delta_A \) of a unital commutative Banach algebra \( A \) is defined to be the set \( \Delta \) of maximal ideals of \( A \). It is a locally compact Hausdorff space w.r.t to the weak*-topology and the Gelfand transform: \( x \mapsto \hat{x}(h) = h(x) \) is a continuous map of \( A \) into \( C(\Delta) \). And the range of \( \hat{x} \) equals \( \sigma(x) \), so \( ||\hat{x}|| = \rho(x) \leq ||x|| \).

\textit{Proof:} First we prove it is compact Hausdorff: As \( \sigma(A) = \{ h \in \text{closed ball of } A^* | h(e) = 1, h(xy) = h(x)h(y) \} \) which is a closed subset of the closed ball of \( A^* \), so it is compact Hausdorff. The rest is clear and follows from (10.8.1.20). \qed

\textbf{Prop. (10.8.1.22).} For \( A = C(X) \) where \( X \) is compact Hausdorff, \( \Delta \) is homeomorphic to \( X \). (Otherwise it has finite \( f_i \neq 0 \), then \( \sum |f_i|^2 \) is positive thus invertible but maps to 0). In fact, for a space \( X \), \( \Delta(C(X)) \) is the Stone-Cech compactification of \( X \).

\textbf{Prop. (10.8.1.23).} For \( A = L^\infty(m) \), the spectrum of \( f \) is just the essential range of \( f \).

\textbf{Lemma (10.8.1.24).} If \( \hat{A} \subset C(\Delta) \) with a chosen topology that makes it compact, and \( A \) separate points, then the topology of it is the same of the weak*-topology. (Compact to Hausdorff).

\textbf{Prop. (10.8.1.25).} The algebra \( L^1(\mathbb{R}^n) \oplus \delta \) with the multiplication by convolution has the spectrum \( \mathbb{R}^n \cap \{ \infty \} \). (Use \( (L^p)^* = L^q \) and see when will it be homomorphism).

\section{2 Hilbert spaces}

\textbf{Prop. (10.8.2.1)[Optimal Approximation].} A closed convex subset in a Hilbert space has a unique element that attains the minimum norm.

\textit{Proof:} Assume \( 0 \notin C \), so let \( d = \inf_{z \in C} ||z|| > 0 \), then there are \( x_n \) that \( d \leq ||x_n|| \leq d + 1/n \). It suffices to show that \( x_n \) is a Cauchy sequence, because then it has a convergent point in \( C \). Now

\[ ||x_n - x_m||^2 = 2(||x_n||^2 + ||x_m||^2) - 4||\frac{x_n + x_m}{2}||^2 \leq 2[(d + 1/n)^2 + (d + 1/m)^2] - 4d^2 \to 0. \]

For the unicity, if \( ||x_1|| = ||x_2|| = d \), then

\[ ||x_1 - x_2||^2 = 2(||x_1||^2 + ||x_2||^2) - 4\frac{x_1 + x_2}{2}||^2 \leq 4d^2 - 4d^2 = 0. \]

\textit{□}

\textbf{Cor. (10.8.2.2)[Orthogonal Decomposition].} The orthogonal complement of a closed subspace of a Hilbert space exists. and the projection on to a closed subspace exists. This is a good trait of Hilbert space.
Prop. (10.8.2.7) [Lax-Milgram Theorem]. Linear functionals on a Hilbert space over \( \mathbb{C} \) are all of the form \( x \mapsto (x,z) \) (Choose an orthogonal of the kernel). In other words, Hilbert spaces are reflexive.

Proof: Choose a \( x_0 \) orthogonal to \( N(f) \) by \ref{10.8.2.2} and \(|x_0| = 1\), then any \( x = \alpha x_0 + y \) where \( y \in N(f) \). Inner product with \( x_0 \), we get \( \alpha = (x,x_0) \), so \( f(x) = \alpha f(x_0) = (x, f(x_0)x_0) \).

\( \square \)

Cor. (10.8.2.4). For Hilbert spaces \( \mathcal{H}, \mathcal{K} \) and \( T \in \mathcal{L}(\mathcal{H}, \mathcal{K}) \), \(|T| = \sup\{(T(x,y)||x| \leq 1, ||y|| \leq 1\}\).

Proof: Use (10.7.3.6) to find for each \( x \) a functional \( f \) of norm 1 that \(|f(Tx)| = ||Tx||\), then use Riesz theorem. In particular, if we define

\( \square \)

Cor. (10.8.2.5) [Reproducing Kernel]. For a Hilbert space \( H \), if elements of \( H \) are all complex valued functions on a set \( S \), and \( J_x : f \mapsto f(x) \) is continuous functional for \( H \), then there is a function \( K(x,y) \) on \( S \times S \) that \( K_y(x) = K(x,y) \in H \), and \( f(y) = (f,K_y)_H \), called the reproducing kernel.

And if \( e_\alpha \) is a basis for \( H \), then \( K(x,y) = \sum e_\alpha(x)e_\alpha(y) \).

Proof: For any \( y \), there is a \( K_y \in H \) that \( f(y) = (f,K_y)_H \) by Riesz representation. If we let \( K(x,y) = (K_y,K_x) = K_y(x) \), then this is the desired kernel.

If \( e_\alpha \) is a basis, then \( K_x = (K_x,e_\alpha)e_\alpha = e_n(x)e_n \), so by Parseval equality, \( K(x,y) = \sum e_\alpha(x)e_\alpha(y) \).

\( \square \)

Prop. (10.8.2.6). Let \( \mathcal{H} \) be a Hilbert space, then a sequence \( x_n \) converges to \( x \) iff \( x_n \) converges to \( x \) weakly and \(|x_n| \rightarrow ||x||\).

Proof: One direction is trivial, for the other, notice that \(|x_n - x|^2 = ||x_n||^2 + ||x||^2 - 2\text{Re}(x,x_n)\) which converges to 0.

\( \square \)

Prop. (10.8.2.7) [Lax-Milgram Theorem]. If \( a(x,y) \) is a sesquilinear form on a Hilbert space \( H \) over \( \mathbb{C} \) that \(|a(x,y)| \leq M||x||||y||\), then there is a unique continuous operator \( A \in L(H) \) that \( a(x,y) = (x,Ay) \). If moreover \(|a(x,x)| \geq \delta ||x||^2\), then \( A \) is bijective and \(|A^{-1}| \leq \frac{1}{\delta}\).

Proof: For any \( y \), \( x \mapsto a(x,y) \) is a continuous functional, so by Riesz theorem (10.8.2.3), there is an element \( Ay \) that \( a(x,y) = (x,Ay) \).

Now \( Ay \) depends linearly on \( y \), and \(|Ay| = \sup |a(x,y)|/||x|| \leq M||y||\).

If \(|a(x,x)| \geq \delta ||x||^2\), then \( A \) is clearly injective, and \( R(A) \) is closed, because for any \( z = \lim Av_n \), it is easily verified that \( v_n \) is a Cauchy sequence. And \( R(A)^\perp = 0 \), because if \( (w, Av) = 0 \) for any \( v \in H \), then \( \delta ||w||^2 \leq |a(w,w)| = 0 \). \( A^{-1} \) exists by Banach theorem (10.6.2.5), and \( \delta ||x||^2 \leq |a(x,x)| = (x,Ax) \leq ||x||||Ax|| \), so \( \delta ||x|| \leq ||Ax|| \).

\( \square \)

Cor. (10.8.2.8) [Variational Inequality]. If \( H \) is a Hilbert space that \( a(x,y) \) is an anti-symmetric bilinear function that \( \delta ||x||^2 \leq a(x,x) \leq M||x||^2 \), then if \( u_0 \in H \), and \( C \) is a closed convex subset of \( X \), the function

\[ f : x \mapsto a(x,x) - \text{Re}(u_0,x) \]
attains minimum at \( C \).
Prop. (10.8.2.1). $f(x) \geq \delta ||x||^2 - ||u_0||||x||$ is bounded below on $C$. if $x_n$ is a sequence that converge to the infimum $d$, then

$$a(x_n - x_m, x_n - x_m) = 2(a(x_n, x_n) + a(x_m, x_m)) - 4a(\frac{x_n + x_m}{2}, \frac{x_n + x_m}{2})$$

$$= 2(f(x_n) + f(x_m)) - 4f(\frac{x_n + x_m}{2}) \leq 2[(d + 1/n)^2 + (d + 1/m)^2] - 4d^2 \to 0.$$ 

So $x_n$ is a Cauchy sequence by the condition, and it contains a unique minimum. □

Cor. (10.8.2.9)[Involution]. For a Hilbert space $H$ over $C$, for any $T \in L(H)$, there is an operator $T^* \in L(H)^*$ that $(Tx, y) = (x, T^*y)$, which is called the formal adjoint or involution of $T$. Notice it is defined on $H$, not on $H^*$. Moreover, $||T|| = ||T^*|| = ||T^*T||^{1/2}$.

Proof: Use Lax-Milgram for $a(x, y) = (Tx, y)$. For the last assertion, $||T|| = ||T^*||$ by (10.8.2.4). And we notice

$$||T^*T||^{1/2} = (Tx, Tx) = (T^*Tx, x) \leq ||T^*T|| ||x||^2,$$

so $||T|| \leq ||T^*T||^{1/2}$. □

Remark (10.8.2.10)[Examples]. The dual operator of the integral operators (10.7.5.2) with kernel $K(x, y)$ is also an integral operator with kernel $K^*(x, y) = K(y, x)$. This follows from Fubini-Tonelli theorem.

3 $B^*$-algebra

Def. (10.8.3.1). A $B^*$-algebra is a Banach algebra with an involution s.t. $||xx^*|| = ||x||^2$.

Any $B^*$-algebra is isomorphic to a closed subspace of $B(H)$ for some Hilbert space.

Proof: Cf. [Rudin P338]. □

Prop. (10.8.3.2). For a Hilbert space, the adjoint operation serves as an involution and makes $B(H)$ into a $B^*$-algebra by (10.8.2.9).

Prop. (10.8.3.3)[Gelfand-Naimark]. For a commutative $B^*$-algebra, the Gelfand transform $x \mapsto \hat{x}$ is an isomorphism from $A$ to $C(\Delta)$ with $||x|| = ||\hat{x}||_\infty$ and $\hat{x}^* = \overline{\hat{x}}$.

Proof: First use $||xx^*|| = ||x||^2$ to prove that a Hermitian element is mapped to real function, and use Stone-Weierstrass to show that the image is dense, then let $y = xx^*$ and $||y^{2m}|| = ||y||^{2m}$ to prove $||\hat{x}|| = ||x||$, so its image is closed. □

Cor. (10.8.3.4). If $A$ is a commutative $B^*$-algebra that contains an element $x$ s.t polynomials of $x, x^*$ are dense in $A$, then $\hat{x}$ is an isomorphism from $\Delta_A$ to $\sigma(x)$, in particular, the Gelfand transform is an isomorphism from $C(\sigma(x))$ to $A$.

Proof: Cf. [Rudin P290]. □

Now we want to apply commutative algebra methods in the non-commutative case, there are two ways.

Prop. (10.8.3.5). For a commutative set of elements $S$ in $A$, its bicommutant (10.8.3.13) $B = \Gamma(\Gamma(S))$ is commutative, closed and contains $S$. And $\sigma_B(x) = \sigma_A(x)$ for $x \in B$. 

Proof:
Prop. (10.8.3.11) [Positive Functional and Measure].

**Proof:** Because $S \subset \Gamma(S)$, $\Gamma(\Gamma(S)) \subset \Gamma(S)$, thus $\Gamma(\Gamma(S))$ is commutative. And if $xy = yx$, then $x^{-1}y = yx^{-1}$, so the inverse, if exists, are in $B$. □

Cor. (10.8.3.6). In a Banach algebra, if $x, y$ commutes, then

$$\sigma(x + y) \subset \sigma(x) + \sigma(y), \quad \sigma(xy) \subset \sigma(x)\sigma(y).$$

**Proof:** Because $\sigma(x)$ is just the range of $\hat{x}$ on $\Delta_A$ where $A = \Gamma(\Gamma(\{x, y\}))$. □

The second method applies to normal elements:

Def. (10.8.3.7) [Normal]. In a Banach algebra with an involution, a set $S$ is called normal if it is commutative and $S^* = S$. An element $x$ is called:

- **normal** if $x$ commutes with $x^*$.
- **unitary** if $x^* = x^{-1}$.
- **Hermitian** if $x^* = x$.
- **positive** if $x = x^*$ and $\sigma(x) \subset [0, \infty)$.

Prop. (10.8.3.8). A maximal normal set $B$ in $A$ is a closed subalgebra and $\sigma_B(x) = \sigma_A(x)$ for $x \in B$.

**Proof:** Cf. [Rudin P294]. □

Cor. (10.8.3.9) [Normalness and Spectra]. In a $B^*$-algebra $A$,

- Hermitian elements have real spectra.
- If $x$ is normal, then $\rho(x) = ||x||$.
- If $u, v \geq 0$, then $u + v \geq 0$.
- $yy^* \geq 0$. Thus $e + yy^*$ is invertible.

**Proof:** Cf. [Rudin P295]. □

Def. (10.8.3.10) [Positive Functional]. In a Banach algebra with an involution, a positive functional is such that $F(xx^*) \geq 0$. It has the following properties.

- $F(x^*) = \overline{F(x)}$ and $|F(xy^*)|^2 \leq F(xx^*)F(yy^*)$. (Use Swartz like trick).
- $|F(x)|^2 \leq F(e)F(xx^*) \leq F(e^2)\rho(xx^*)$, because $e = ee^*$. Thus $|F(x)| \leq F(e)\rho(x)$ for every normal $x$ by (10.8.3.9), so $||F|| = F(e)$ if $A$ is commutative.

**Proof:** Cf. [Rudin P297]. □

Prop. (10.8.3.11) [Positive Functional and Measure]. If $A$ is a commutative Banach algebra with an involution that $h(x^*) = \overline{h(x)}$, then The map

$$\mu \to F(x) = \int_\Delta \tilde{x}d\mu$$

is a one-to-one correspondence between the convex set of measures $\mu$ that $\mu(\Delta) \leq 1$ to the convex set $K$ of positive functionals on $A$ of norm $\leq 1$, i.e. $F(e) \leq 1$, so maps the extreme points, i.e. the point mass to extremes points, thus the extreme points of $K$ is exactly $\Delta$. This can be used to prove Bochner’s theorem??

**Proof:** Use the last prop to show that there is a functional on $C(\Delta)$ and use Riesz representation. It is positive and by Stone-Weierstrass, it is unique. □
von Neumann Algebras

Def.(10.8.3.12)[von Neumann Algebra]. A von Neumann Algebra is a $B^*$-algebra of operators in $L(H)$ that contains the identity and is closed in the weak operator topology (10.6.3.4).

Def.(10.8.3.13)[Bicommutant]. If $S$ is a subset of $L(H)$, then we define the commutator $\Gamma(S)$ be the algebra of operators that commutes with $S \in S$, then $\Gamma(\Gamma(S))$ contains $S$, it is called the bicommutant of $SS$.

If $A$ is a $\ast$-algebra in $L(H)$, then $\Gamma(\Gamma(A))$ is a von Neumann algebra.

Proof: If $A$ is a $\ast$-algebra, then $\Gamma(\Gamma(A))$ is clearly a $\ast$-algebra, and it is weak-closed because if $SV_i = V_i S$ and $V_i x \to V x$ for any $x$, then $SV x = VS x$ for any $x$. □

Prop.(10.8.3.14)[von Neumann Density Theorem]. Let $A$ be a non-degenerate $\ast$-subalgebra of $L(H)$, then $A$ is dense in $\Gamma(\Gamma(A))$ in the strong operator topology.

Proof: For any $S \in \Gamma(\Gamma(A))$ and any $x_1, \ldots, x_N \in H$, $\varepsilon > 0$, we need to prove there exists $A \in A$ that $\sum ||Sx_i - Ax_i|| \leq \varepsilon^2$.

For the case $N = 1$ and $x_1 = x$, consider the closure $\mathcal{X}$ of $\{Ax\}$, then the orthogonal projection $P$ onto $\mathcal{X}$ is an operator in $\Gamma(A)$. This implies $A(1 - P)x = (1 - P)Ax = 0$, thus $x = Px$ because of non-degeneracy. Then because $S$ commutes with $P$, $Sx = SPx = PSx \in \mathcal{X}$, thus there exists an $A \in A$ that $Ax$ is close to $Sx$.

For $N > 1$, we can just apply the result to $H^N$. □

4 Spectral Theory on Hilbert Spaces

The most useful tool is the general symbolic calculus for normal operators.

Resolution of Identity

Def.(10.8.4.1). A resolution of identity on a Hilbert space $H$ for a $\sigma$-algebra on a set $\Omega$ is an $E$ that:
1. $E(\emptyset) = 0, E(\Omega) = 1$.
2. $E(\omega)$ is self-adjoint projection.
3. $E(\omega' \cap \omega) = E(\omega') E(\omega)$.
4. $E(\omega \cup \omega') = E(\omega) + E(\omega')$ for disjoint $\omega, \omega'$.
5. $E_{x,y}(\omega) = (E(\omega)x, y)$ is a complex measure on $E$.

Thus for any $x, \omega \to E(\omega)x$ is a countably additive $H$-valued measure.

This will generate an isometric $\ast$-isomorphism $\Psi$ of the Banach algebra $L^\infty(E)$ onto a closed normal subalgebra $A$ of $B(H)$. (Define on simple function first).

\[ \Psi(f) = \int_\Omega f dE, \quad (\Psi(f)x, y) = \int_\Omega f dE_{x,y} \]

Proof: Cf.[Rudin P319]. □

Prop.(10.8.4.2)[Spectral Decomposition for Normal Algebra]. For any closed normal algebra $A$ of $B(H)$, there is a unique resolution $E$ of identity on the Borel subsets of $\Delta_A$ that the inverse
of Gelfand transform extends to an isometric *-isomorphism $\Phi$ of the algebra $L^\infty(E)$ to a closed subalgebra $B$ containing $A$.

In fact, $B = \Gamma(\Gamma(A))$ is normal by Fuglede theorem(10.8.4.10).

Proof: Cf.[Rudin P322].

Cor.(10.8.4.3)[Generalized Symbolic Calculus for Normal Operator]. For a normal operator $T$ and the minimal closed commutative $B^*$-algebra $A$ it generates, then the inverse of Gelfand transform gets us a map $\Psi : C(\sigma(x)) \to A$ that $\Psi(z) = x$, $\Psi(\bar{z}) = x^*$, by(10.8.3.4).

Then the above proposition says there is a resolution of identity on the Borel set of $\sigma(T)$ that $\Psi$ extends to a function that maps $L^\infty(m)$ to $B(H)$ and $||\Psi(f)|| = ||f||_\infty$.

Cor.(10.8.4.4)[Normal and Invariant Subspace]. Any closed normal algebra $A$ has many invariant subspaces, just choose a decomposition of Borel sets $\Delta_A = \omega \bigcup \omega'$, then $R(E(\omega)) \oplus R(E(\omega')) = H$.

In particular, any normal operator has an invariant subspace.

Normal Operators on Hilbert Space

Lemma(10.8.4.5). For a Hilbert space $H$ and $T \in L(H)$, $T$ is defined by values $(Tx,x)$.

Proof: If $(Tx,x) = 0$, then $(Tx,y) + (Ty,x) = 0$, so $-i(Tx,y) + i(Ty,x) = 0$, solving $(Tx,y) = 0$ for all $x,y$, so $T = 0$.

Prop.(10.8.4.6)[Normal Operators].

1. An operator is normal iff $||Tx|| = ||T^*x||$. So $N(T) = N(T^*)$ thus $\sigma_p(T^*) = \overline{\sigma_p(T)}$, and $R(T)$ is dense iff $T$ is injective. And different eigenspaces are orthogonal.

2. An operator is unitary iff $R(U) = H$ and $||Ux|| = ||x||$ for every $x$. (Because an operator is defined by its value $(Tx,y)$).

Proof: $||Tx||^2 = (T^*Tx,x)$, $||T^*x|| = (TT^*x,x)$, and they are equal iff $T,T^*$ commutes by(10.8.4.5). In particular, for different eigenvectors, $\alpha(x,y) = (Tx,y) = (xT^*y) = (x,\bar{y}) = \beta(x,y)$.

For unitary, one way is obvious, for the other, if $||Ux|| = ||x||$, then $(U^*Ux,x) = (x,x)$, so $U^*U = id$ by(10.8.4.5), and $U$ is a bijection. So it is invertible.

Cor.(10.8.4.7). For a normal operator $T$ on a Hilbert space $T$ is invertible iff there is a $\delta$ that $||Tx|| = ||T^*x|| \geq \delta ||x||$.

Proof: $T$ is injective iff $R(T)$ is dense, and if $||Tx|| = ||T^*x|| \geq \delta ||x||$, then $R(T)$ is closed by(3.6.8.9), so it is invertible by Banach theorem.

Prop.(10.8.4.8). If $T$ is normal, then

1. $||T|| = \sup\{|(Tx,x)| \ |x|| = 1\}$.

2. $T$ is self-adjoint iff $\sigma(T)$ is real.

3. $T$ is unitary iff $|\sigma(T)| = 1$. 
Proof: For $1$, $||T|| = \rho(T) = ||z_0||$ for some $z_0 \in \rho(T)$ by Naimark (10.8.3.3), then Urysohn lemma to show $E(U) \neq 0$ for an open $U$ near $x$ (because otherwise there is a continuous function supported in $U$ that are mapped to $0$), then there are $||x_0|| = 1$ that $E(U)x_0 = x_0$.

Consider now $f = (z - z_0)i_U(z)$, then $f(T)(x_0) = Tx_0 - \lambda_0x_0$, so

$$ (Tx_0, x_0) - \lambda_0 = |(f(T)x_0, x_0)| \leq ||f(T)|| = ||f|| \leq \varepsilon $$

This shows that $||T|| = \sup\{||(Tx, x)|| : ||x|| = 1\}$.

For $2$, by generalized symbolic calculus (10.8.4.3), $\hat{T} = \lambda$ on $\sigma$ and $\hat{T}*$ = $\overline{\lambda}$ on $\sigma$, so they are equal iff $\sigma(T)$ is real, and $TT^* = I$ iff $\lambda\overline{\lambda} = 1$ on $\sigma(T)$. □

Prop. (10.8.4.9)[Decomposition of Operators]. Every operator $S \in L(H)$ on a Hilbert space $H$ is a linear combination of two self-adjoint operator and a linear combination of four unitary operator.

Proof: The first assertion is easy as $S = (S + S^*)/2 + (S - S^*)/2$. Now any self-adjoint operator is a multiple of a self-adjoint operator of norm $||S|| \leq 1$, so $1 - S^2$ is positive, and we have $S = \frac{1}{2}(f_+(S) + f_-(S))$, where $f_\pm(s) = s \pm i\sqrt{1 - s^2}$.

Prop. (10.8.4.10)[Fuglede]. If $N_1$ and $N_2$ are normal operators and $A$ is a bounded linear operator on a Hilbert space such that $N_1A = AN_2$, then $N_1^*A = AN_2^*$.

Proof: For any $S \in B(H)$, $exp(S - S^*)$ is unitary thus $||exp(S - S^*)|| = 1$, $exp(N_1)A = Aexp(N_2)$. Because $exp(M)T = Texp(N)$, if we let $U_1 = exp(M^* - M), U_2 = exp(N - N^*), then$ $||exp(N_1^*)Texp(-N_2^*)|| = ||U_1TU_2|| \leq ||T||$ because $\lambda\overline{\lambda}$ is normal. Now $||exp(\lambda N_1^*)Texp(-\lambda N_2^*)|| = ||U_1TU_2|| \leq ||T||$ also holds, thus by Liouville, $exp(\lambda N_1^*)Texp(-\lambda N_2^*) = T$. Compare the coefficients of $\lambda$, we get the result. □

Prop. (10.8.4.11). An operator $T \in B(H)$ has the same spectrum w.r.t all the closed $B^*$-algebras of $B(H)$ containing it.

Proof: If $T$ is invertible, because $TT^*$ is self-adjoint thus has real spectrum (10.8.4.8) so doesn’t separate $C$ thus it is invertible in any closed $B^*$-algebra of $B(H)\{10.8.1.12\}$. so does $T^{-1} = T^*TT^*$. □

Prop. (10.8.4.12). For $T$ normal and $E$ its spectral decomposition, then if $f \in \mathcal{C}(\sigma(T))$ and $\omega_0 = f^{-1}(0)$, then $N(f(T)) = R(E(\omega_0))$.

Proof: $\chi_{\omega_0}f = 0$, so $f(T)R(E(\omega_0)) = 0$, and if we let $\omega_n = f^{-1}(\{1/(n - 1), 1/n\})$, and let $f_n(\lambda) = 1/f(\lambda)\chi_{\omega_n}$, then $f_n(T)f(T) = E(\omega_n)$, so if $f(T) = 0$, then $E(\omega_n)x = 0$, so countable additivity shows that $E(\sigma\setminus\omega_0)x = 0$, so $E(\omega_0)x = x$. These shows the desired result. □

Cor. (10.8.4.13).
1. $N(T - \lambda I) = R(\{\lambda\})$.
2. every isolated point of $\sigma(T)$ is point spectrum, because this point is open thus is $E(\{x\}) \neq 0$ by Urysohn lemma.
3. if $\sigma(T)$ is countable, then every $x \in H$ has a unique orthogonal decomposition $x = \sum E(\lambda_i)x$ and $T(E(\lambda_i)x) = \lambda_i E(\lambda_i)x$.

**Prop. (10.8.4.14) [Normal Compact Operator]**. A normal operator $T \in B(H)$ is compact iff $\sigma(T)$ has no limit point except possibly $0$ and $\dim N(T - \lambda I) < \infty$ for $\lambda \neq 0$.

In particular, a normal compact operator is a limit of f.d. operators

Proof: One direction is general, by (10.7.5.9), for the other, it is a limit of operators of finite dimensional range by general symbolic calculus (10.8.4.3). □

**Cor. (10.8.4.15) [Spectral Theorem]**. A compact normal operator (in particular a normal operator on a f.d linear space) is unitarily diagonalizable.

Proof: it suffices to find a basis of eigenvectors, but this is easy, just by (10.8.4.13). □

**Cor. (10.8.4.16) [Hilbert-Schmidt]**. For a self-adjoint compact operator $A$ on a Hilbert space $H$, there is a set of orthonormal basis that $A$ is diagonal on it. And of course, its eigenvalues are real and can only converges to $0$ (10.8.4.8).

**Prop. (10.8.4.17)**. For a normal compact operator $T \in L(H)$, then:

1. $T$ has an eigenvalue $|\lambda|$ that $|\lambda| = ||T||$. 
2. $f(T)$ is compact if $f \in C(\sigma(T))$ and $f(0) = 0$.
3. $f(T)$ is not compact if $f \in C(\sigma(T))$ and $f(0) \neq 0$ and $\dim H = \infty$.

Proof: 1: The spectrum of maximal norm is isolated (10.7.5.9) hence a point spectrum by (10.8.4.13). And $|\lambda| = ||T||$ by symbolic calculus (10.8.4.3).

2: Cf. [Rudin P330].

3: The 2 sill show that $f(0)I - f$ is compact, If $f$ is compact, then $f(0)I$ is compact, so $\dim H < \infty$ (10.7.5.3). □

**Prop. (10.8.4.18) [Freudenthal Spectral Theorem]**.

**Prop. (10.8.4.19) [Positive Equivalent Definition]**. A $T \in L(H)$ is positive, i.e. $T = T^*$ and $\sigma(T) \subset [0, \infty)$ iff $(Tx, x) \geq 0$.

Proof: If $(Tx, x) \geq 0$, then $(Tx, x) = (x, Tx) = (T^*x, x)$, so $T = T^*$ by (10.8.4.5), so $\sigma(T)$ is real (10.8.4.8), and for $\lambda > 0$,

$$\lambda||x||^2 = (\lambda x, x) \leq ((T + \lambda I)x, x) \leq ||(T + \lambda I)x||||x||,$$

so $T + \lambda I$ is invertible by (10.8.4.7), so $\sigma(T) \subset [0, \infty)$.

Conversely, if $T$ is positive, then it is normal, so $(Tx, x) = \int_{\sigma(T)} \lambda dE_{x,x} \geq 0$. □

**Prop. (10.8.4.20) [Polar Decomposition]**.

1. Every positive operator $T$ has a positive square root, which is invertible if $T$ is.
2. Polar decomposition exists in $B(H)$: Any $T \in L(H)$ invertible has a unique decomposition $T = UP$ where $U$ is unitary and $P$ is positive. And $||Px|| = ||Tx||$ for all $x$.
3. Any normal operator has commuting decomposition $UP$, where $U, P, T$ commutes.
Proof: 1: Use general symbolic calculus, then \( S = \sqrt{T} \) is the square root of \( T \). If \( T \) is invertible, then \( S^{-1} = T^{-1}S \).

2: \((T^*Tx, x) = (Tx, Tx) \geq 0\), so \( T^*T \) is positive\(^{(10.8.4.19)}\), so let \( P = \sqrt{T} \), then it is also invertible, and \( U = TP^{-1} \) is unitary.

3: Use general symbolic calculus, let \( p(\lambda) = |\lambda| \), \( u(\lambda) = \lambda/|\lambda| \) if \( \lambda \neq 0 \), and \( u(0) = 0 \). Then \( T = UP \), and they are commutative. \( \square \)

Cor.\(^{(10.8.4.21)}\) [Similar Normal Operator]. Similar normal operators are unitarily equivalent.

Proof: It suffices to show that if \( M = TNT^{-1} \), and \( T = UP \) is the polar decomposition, then \( M = UNU^{-1} \). Fuglede\(^{(10.8.4.10)}\) shows \( M^*T = TN^* \), so \( NP^2 = NT^*T = T^*MT = T^*TN = P^2N \), so \( N \) commutes with any functions \( f(P) \), in particular \( P \). Hence \( M = (UP)N(U^P)^{-1} = UNU^{-1} \). \( \square \)

5 Hilbert-Schmidt Operators and Trace Classes

Main references are [Trace Classes and Hilbert-Schmidt Operators].

Def.\(^{(10.8.5.1)}\) [Hilbert-Schmidt Operator]. Let \( \mathcal{H}, \mathcal{K} \) be Hilbert spaces and \( T \in L(\mathcal{H}, \mathcal{K}) \). Then for any orthonormal basis \( \{e_k\} \) of \( \mathcal{H} \) and \( \{f_k\} \) of \( \mathcal{K} \),

\[
\sum_j ||Te_j||^2_\mathcal{K} = \sum_j ||T^*f_j||^2_\mathcal{H}.
\]

Thus we can say \( T \) is Hilbert-Schmidt iff

\[
||T||_{HS} = (\sum_j ||Te_j||^2_\mathcal{K})^{1/2} < \infty
\]

for some/all basis \( e_j \) of \( \mathcal{H} \). The space of all Hilbert-Schmidt between \( \mathcal{H}, \mathcal{K} \) is denoted by \( S_2(\mathcal{H}, \mathcal{K}) \).

Proof:

\[
\sum_i ||Te_k||^2 = \sum_i \sum_j |(Te_k, f_j)|^2 = \sum_i \sum_j |(T^*f_j, e_i)|^2 = \sum_j ||T^*f_j||^2
\]

\( \square \)

Cor.\(^{(10.8.5.2)}\) [Properties of \( S_2(\mathcal{H}, \mathcal{K}) \)].

- If \( A \in S_2(\mathcal{H}, \mathcal{K}) \) then \( A^* \in S_2(\mathcal{K}, \mathcal{H}) \) with the same HS-norm.
- For \( A \in S_2(\mathcal{H}, \mathcal{K}) \), \( ||A|| \leq ||A||_{HS} \).
- \( S_2(\mathcal{H}, \mathcal{K}) \) is a Banach space in the HS-norm.
- If \( \mathcal{H}_1, \mathcal{K}_1 \) are separable Hilbert spaces and \( T \in S_2(\mathcal{H}, \mathcal{K}), A \in L(\mathcal{H}_1, \mathcal{H}), B \in L(\mathcal{K}, \mathcal{K}_1) \), then \( BTA \in S_2(\mathcal{H}_1, \mathcal{K}_1) \).

Proof: 1 follows from\(^{(10.8.5.1)}\). 2 is because we can extend \( u \) to a basis of \( \mathcal{H} \).

3: \( ||-||_{HS} \) is clearly a semi-norm\(^{(10.6.1.8)}\), and it is a norm by item 2. To show the completeness, if \( A_j \) is an HS-Cauchy sequence, then it is a Cauchy sequence in the operator norm, thus converges to an operator \( A \). Then for any \( \varepsilon \), there is an \( N \) that for any \( j, k \geq N \), \( ||A_j - A_k||_{HS} \leq \varepsilon \). This implies

\[
\sum_{\alpha \in S} ||(A_k - A_j)e_\alpha||^2_\mathcal{K} \leq \varepsilon^2
\]
for any finite subset $S \subset I$. Then letting $k \to \infty$ and then letting $S$ be any subset, we get $\|A - A_j\|_{HS} \leq \varepsilon$. Thus $A$ is Hilbert-Schmidt and $A_j \to A$ in HS-norm.

4: it is clear that $\|BT\|_{HS} \leq ||B||||T||_{HS}$, and because of the transpose invariance of $HS$-norm and operator norm(10.8.2.9).

**Prop. (10.8.5.3) [Hilbert-Schmidt Operator is Compact]**. If $A \in S_2(\mathcal{H}, \mathcal{K})$ and $\{f_k\}$ is an orthonormal basis of $\mathcal{K}$, and we denote $\pi_n$ as the projection of $\mathcal{K}$ onto the span of $\{f_1, \ldots, f_n\}$, then

$$\|\pi_n A - A\|_{HS} \to 0.$$  

In particular, $A$ is compact, by(10.8.5.2) and(10.7.5.3).

**Proof:** By(10.8.5.2), it suffices to show that $\|A^* \pi_n - A^*\|_{HS} \to 0$. But this norm is just $\sum_{k>N} ||A^* f_k||^2_L$, which converges to 0.  \( \square \)

**Prop. (10.8.5.4) [Hilbert-Schmidt Inner Product]**. If $\mathcal{H}$ is a Hilbert space and $A, B \in S_2(\mathcal{H})$, then $B^*A \in S_1(\mathcal{H})$ by(10.8.5.2)(10.8.5.7), then we can define an **Hilbert-Schmidt inner product** on $S_2(\mathcal{H})$:

$$(A, B) = \text{tr}(B^*A)(10.8.5.9).$$

Then this makes $S_2(\mathcal{H})$ a Hilbert space.

**Proof:** This follows from(10.8.5.2).  \( \square \)

**Prop. (10.8.5.5) [Integral Operator is Hilbert-Schmidt]**. Let $\Omega$ be a $\sigma$-finite measure space and $K(x, y) \in L^2(\Omega \times \Omega)$, then the operator $L u(x) = \int_\Omega K(x, y) u(y) dy$ defined in(10.7.5.2) is a Hilbert-Schmidt operator on $L^2(\Omega)$. In fact, $\|L\|_2 = \|K\|_{L^2}.$

**Proof:** Let $\mathcal{E}$ be an Hilbert basis of $L^2(\Omega)$, then we have

$$\|L\|_2^2 = \sum_{f_1, f_2 \in \mathcal{E}} |(Lf_1, f_2)|^2 = \sum_{f_1, f_2 \in \mathcal{E}} |\int_X \int_X f_2(y) K(x, y) f_1(x) dx dy|^2 = \sum_{f_1, f_2 \in \mathcal{E}} (K, f_1 \otimes f_2)^2$$

But by(10.4.5.4) $\{f_i \otimes f_j\}$ form a Hilbert Basis for $L^2(\Omega \times \Omega)$, then the equation equals $\|K\|_2^2$.  \( \square \)

**Trace Classes**

**Def. (10.8.5.6) [Trace Classes]**. Let $\mathcal{H}$ be a Hilbert space, $\{e_i\}, \{f_i\}$ are two orthonormal basis, $A \in B(\mathcal{H})$. Let $|A| = (A^* A)^{1/2}$ which is positive, then

$$\sum_i (|A| e_i, e_i) = \sum_i (|A|^{1/2} e_i, |A|^{1/2} e_i) = \sum_i |||A|^{1/2} f_i|| = \sum_i (|A| f_i, f_i)$$

by(10.8.5.1), thus we can define $\|A\|_1 = \sum_i (|A| e_i, e_i)$, and say $A$ is a **trace class** if $\|A\|_1 < \infty$. The space of trace classes is denoted by $S_1(\mathcal{H})$.

A trace-class $A$ is clearly compact as $|A|$ is a limit of f.d. range operators.(Use diagonalization, then there are only countably many eigenvectors of $|A|$).

**Prop. (10.8.5.7)**. If $A \in B(\mathcal{H})$, then the following are equivalent:

- $A \in S_1(\mathcal{H})$.
- $|A|^{1/2} \in S_2(\mathcal{H})$.  

• $|A|$ is a product of two elements in $S_2(\mathcal{H})$.

• $A$ is a product of two elements in $S_2(\mathcal{H})$.

**Proof:**

1 → 2 → 3 is clear, for $3 \to 4$: if $|A| = TS$, then by polar decomposition $A = U|A| = (UT)S$, and $UT \in S_2(\mathcal{H})$ by (10.8.5.2), so $A$ is a product of two elements in $S_2(\mathcal{H})$.

4 → 3 is similar to 3 → 4.

$3 \to 1$: if $A = BC$ where $B,C \in S_2(\mathcal{H})$, then $B^* \in S_2(\mathcal{H})$ also by (10.8.5.2), so $A$ is a product of two elements in $S_2(\mathcal{H})$.

\[
||A||_1 = \sum_i (Ae_i, e_i) = \sum_i (Ce_i, B^*e_i) \leq \sum_i ||Ce_i|| ||B^*e_i|| \leq ||C||_2 ||B^*||_2 < \infty
\]

\[\square\]

**Lemma (10.8.5.8).** If $T$ is a positive trace-class and $S \in B(\mathcal{H})$, then if $x_i$ is an orthonormal basis of $\mathcal{H}$, then

\[
\sum_i (STx_i, x_i) \leq ||S|| ||T||_1
\]

is absolutely convergent, and is independent of the basis chosen.

**Proof:**

Let $e_i$ be the basis of eigenvectors of $T$ of eigenvalues $\lambda_i > 0$, then $\sum_i \lambda_i < \infty$ by (10.8.5.7), and

\[
(STx_i, x_i) = \sum_j (x_i, e_j)(STe_j, x_i) = \sum_j \lambda_j (x_i, e_j)(Se_j, x_i)
\]

And

\[
\sum_i \sum_j \lambda_j ||x_i, e_j|| (Se_j, x_i) \leq \sum_j \lambda_j ||e_j|| ||Se_j|| \leq ||S|| \sum \lambda_i < \infty.
\]

Moreover:

\[
\sum_i (STx_i, x_i) = \sum_j \sum_i (x_i, e_j)STe_j, x_i) = \sum_i \sum_j (STe_j, (e_j, x_i)x_i) = \sum_j (STe_j, e_j).
\]

\[\square\]

**Prop. (10.8.5.9) [Singular Trace].** If $T \in S_1(\mathcal{H})$ and $x_\alpha$ is an orthonormal basis of $\mathcal{H}$, then $\sum (Tx_\alpha, x_\alpha)$ absolutely converges, and is independent of the basis chosen, called the singular trace $\text{tr} T$ of $T$. The singular trace is a positive definite linear functional on $S_1(\mathcal{H})$.

**Proof:**

Use polar decomposition $T = U|T|$ (10.8.4.20) and notice $|T|$ is a positive trace class (10.8.5.7) and then use (10.8.5.8).

\[\square\]

**Prop. (10.8.5.10) [Trace of Integral Operators].** Let $A, B$ be $L^2$ integral operators on a $\sigma$-finite measure space $\Omega$ with kernel $K_1(x,y), K_2(x,y) \in L^2(\Omega \times \Omega)$, then $AB$ is also an integral operator with kernel

\[
\int K_1(x,z)K_2(z,y)dz,
\]

and

\[
\text{tr}(AB) = \int \int K_1(x,y)K_2(y,x)dxdy.
\]
**Proposition 10.8.5.11** [Properties of Trace Classes].

1. $S_1(\mathcal{H})$ is a two-sided $\ast$-ideal of $\mathcal{L}(\mathcal{H})$.
2. $|| \cdot ||_1$ is a norm on $S_1(\mathcal{H})$.
3. If $T \in S_1(\mathcal{H})$, then $\text{tr} T^\ast = \overline{\text{tr} T}$.
4. For any $T \in S_1(\mathcal{H})$ and $S \in L(\mathcal{H})$, $\text{tr}(ST) = \text{tr}(TS)$, and $|\text{tr}(ST)| \leq ||S|| ||T||_1$. In particular the singular trace is a bounded linear functional on $S_1(\mathcal{H})$.

**Proof:** Let $S,T \in S_1(\mathcal{H})$, $S = V|S|, T = W|T|$, $S + T = X|S + T|$ where $V,W,X$ are unitary, then $|S + T| = X^\ast (S + T)$ is positive compact, so it has an orthonormal eigenbasis $e_n$ by (10.8.4.16), so

$$\sum (|S + T| x_i, x_i) = \sum (X^\ast V|S|x_i, x_i) + \sum (X^\ast W|S|x_i, x_i) \leq ||S||_1 + ||T||_1$$

by (10.8.5.8). So $S + T$ is a trace class, and $||S + T||_1 \leq ||S||_1 + ||T||_1$.

Now if $U$ is unitary and $T \in S_1(\mathcal{H})$, then $(UT)\ast UT = T^\ast T$, so $UT$ is a trace class, and $(TU)^\ast TU = U^{-1}TU$ has $|TU| = U^{-1}|T|U$, so $TU$ is also a trace class. Moreover, $\text{tr}(TU) = \sum (TU x_i, x_i) = \sum (UTU x_i, U x_i) = \text{tr}(UT)$.

Then notice very $S \in L(\mathcal{H})$ is a linear combination of four unitary operators (10.8.4.9), so the proposition is true, and if $T$ is a trace class, then $T = V|T|$, and $T^\ast = |T|V^\ast$ is also a trace class.

4: $|\text{tr}(ST)| \leq ||SV|| ||T||_1 = ||S|| ||T||_1$ by (10.8.5.8). \qed

**Proposition 10.8.5.12** [Trace Class as a Banach Space]. Let $S_0(\mathcal{H})$ be the space of operators of f.d. range, then the map

$$\rho : S_1(\mathcal{H}) \to S_0(\mathcal{H})^\ast : \rho(A) : C \mapsto \text{tr}(CA)$$

is an isometric isomorphism. In particular, $S_1(\mathcal{H})$ is a Banach space, by (10.6.3.1).

**Proof:** Clearly $\rho$ is a linear map as singular trace is. For $T \in S_1(\mathcal{H})$, $||\rho(T)|| \leq ||T||_1$ by (10.8.5.11).

If $\Phi \in S_0(\mathcal{H})^\ast$, $g,h \in \mathcal{H}$, consider $g \otimes h^\ast \in S_0(\mathcal{H})$ that $g \otimes h^\ast(v) = (v,h)g$, then $B(g,h) = \Phi(g \otimes h^\ast)$ is a sesquilinear form on $\mathcal{H}$ that is bounded by $||\Phi||$. Thus by Lax-Milgram (10.8.2.7), there is a unique $T \in \mathcal{B}(\mathcal{H})$ that $B(g,h) = (g,Th)$.

Now let $A = T^\ast$ and let $A = U|A|$ be the polar decomposition, $\mathcal{E}$ an orthonormal basis of $\mathcal{H}$ and $S \subset \mathcal{E}$ a finite subset, define

$$C_S = (\sum_{e \in S} e \otimes e^\ast) U^\ast = \sum_{e \in S} e \otimes (Ue)^\ast.$$
Then $C_S$ is of f.d. and $||C_S|| \leq 1$. And:

$$
\sum_{e \in S} (|A|e, e) = \sum_{e \in S} (U^* Ae, e) = \sum_{e \in S} (e, TUe) = \sum_{e \in S} B(e, Ue) = \sum_{e \in S} \Phi(e \otimes (Ue)^*) = \Phi(C_S).
$$

So $||A||_1 \leq ||\Phi||$.

If $C$ is any operator of f.d. range that $C = \oplus g_k \otimes h_k^*$, then

$$
\Phi(C) = \sum k \Phi(g_k \otimes h_k^*) = \sum k B(g_k, h_k) = \sum k (Ag_k, h_k) = \sum \text{tr}(A(g_k \otimes h_k^*)) = \text{tr}(AC) = \rho(A)(C)
$$

so the image is $A$ is just $\Phi$. This shows that $\rho$ is surjective and moreover $||A||_1 = ||\rho(A)||$, so we are done. $\square$
10.9 Analysis on Locally Compact Groups

Main references are [Fol15], [Bum98].
All representations in this section are assumed to be over \( \mathbb{C} \).

1 Locally Compact Groups

Def.(10.9.1.1) [Left and Right Regular Actions]. On a topological group \( G \), the \textbf{left regular action} and \textbf{right regular action} are defined as follows: \( L_y f(x) = f(y^{-1}x) \), \( R_y f(x) = f(xy) \).

Def.(10.9.1.2) [Involution]. For \( f \in C_c(G) \) or \( f \in L^p(G) \) for some \( p \), let \( \tilde{f}(x) = f(x^{-1}) \).

Prop.(10.9.1.3) [Translation is Continuous]. If \( f \in C_c(G) \), then \( f \) is left and right uniformly continuous. Equivalently, \( G \rightarrow C_c(G) : y \mapsto R_y (f) \) and \( y \mapsto L_y (f) \) are continuous group homomorphisms from \( G \) to \( C_c(G) \).

Proof: Cf.[Folland Abstract Harmonic Analysis P38]. □

Prop.(10.9.1.4). Locally compact Hausdorff group is normal.

Proof: Notice that by choosing a precompact symmetric open neighbourhood \( U \) of identity, there exists a \( \sigma \)-compact clopen subgroup \( H \). So \( H \) can \( \sigma \)-locally refine every open cover, thus \( G \) can, too. So by (3.6.7.2) \( G \) is paracompact. As a topological group, \( G \) is regular, thus \( G \) is normal by (3.6.7.6). □

Prop.(10.9.1.5) [Dirac sequence]. For a locally compact Hausdorff group \( G \), a \textbf{Dirac sequence} is a sequence \( f_n \in C_c(G) \) that \( f_n \rightarrow \delta_1 \) in the weak topology of \( \text{Meas}_c(G) \).

Dirac sequences exist.

Proof: □

Prop.(10.9.1.6). Every locally compact group \( G \) has a subgroup \( G_0 \) that is clopen and \( \sigma \)-compact.

Proof: Let \( U \) be a symmetric precompact nbhd of \( 1 \) in \( G \), then let \( U_n = U^n \), then \( \overline{U_n} \subset U_{n+1} \), so let \( G_0 = \cup_n U^n = \cup \overline{U_n} \), then it is open because each \( U_n \) does, and compact because each \( \overline{U_n} \) does. □

Prop.(10.9.1.7). If \( G \) is locally compact Hausdorff, and \( H \) is subgroup that is locally compact in the induced topology, then \( H \) is closed in \( G \).

Proof: By hypothesis there exists an open nbhd \( U \) of \( e \in G \) that \( U \cap H \) has compact closure \( K \subset H \). But then \( K \) is also compact in \( G \) thus closed. So \( K \) is the closure of \( U \cap H \) in \( G \). Choose a symmetric open nbhd \( V \) of \( e \in G \) that \( V V \subset U \), and suppose \( x \in \overline{H} \), then \( x^{-1} \in \overline{H} \) and \( V x^{-1} \cap H \neq \emptyset \). Let \( y \in V x^{-1} \cap H \). For any nbhd \( U_i \) of \( e \in G \), choose \( x' \subset xU_i \cap H \), then \( yx' = yx(x^{-1}x') \in xyU_i \) and also \( yx \in H \), \( yx' \in V x^{-1} x V \subset U \). By arbitrariness of \( U_i \), this means \( yx \in \overline{U \cap H} = K \subset H \), thus \( x \in H \), and \( H \) is closed. □
Integration on Locally Compact Groups

Def.(10.9.1.8)[Positive Linear Functional]. A positive linear functional is a linear functional \( I \) on \( C_c(X) \) that \( I(f) \geq 0 \) whenever \( f \geq 0 \). How is this definition compatible with that of (10.8.3.10)?

Lemma(10.9.1.9) [Positive Linear Functional is Continuous]. For a LCH space \( X \), a positive linear functional (10.9.1.8) \( I \) on \( C_c(X) \) is automatically continuous, where \( C_c(X) \) is given compact convergence topology as in (10.7.2.1).

Proof: We need to prove that for any compact subset \( K \) of \( X \), there is a constant \( C_K \) that for any \( f \in C(G) \) with support in \( K \), we have \( |I(f)| \leq C_K ||f||_\infty \).

Given any \( K \), choose by Urysohn lemma a \( \varphi \in C_c(X, [0,1]) \) that \( \varphi = 1 \) on \( K \), so if \( \text{Supp} \ f \subset K \), then \( |f| \leq ||f||_\infty \varphi \), thus the positivity of \( I \) shows that \( |I(f)| \leq I(\varphi) ||f||_\infty \). □

Prop. (10.9.1.10)[Riesz-Markov-Kakutani Representation Theorem]. Let \( X \) be a locally compact Hausdorff space.

- If \( I \) is a positive linear functional (10.9.1.8) on \( C_c(X) \), there is a unique Radon measure \( \mu \) on \( X \) such that \( I(f) = \int f \, d\mu \). Moreover,

\[
\mu(U) = \sup \{ I(f) : f < U \} \text{ for } U \text{ open},
\]

\[
\mu(K) = \inf \{ I(f) : f > \chi_K \} \text{ for } K \text{ compact}.
\]

- If \( I \) is a continuous linear functional on \( C_0(X) \), there is a unique regular complex Borel measure \( \mu \) on \( X \) that \( I(f) = \int f \, d\mu \).

In particular if \( X \) is compact, \( M(X) \) the space of Radon measures on \( X \) is the dual space of \( C(X) \).

Proof: Cf.[Real Analysis Folland P212]. □

Prop. (10.9.1.11)[Haar Measure]. A left(right) Haar measure on a topological group \( G \) is a non-zero Radon measure (10.4.1.9) \( \mu \) on \( G \) that satisfies \( \mu(xE) = \mu(E)(\mu(Ex) = \mu(E)) \). A Radon measure \( \mu \) is a Haar measure iff it satisfies \( \int L_y f \, d\mu = \int f \, d\mu \) for any \( f \in C_c^+(G) \) and \( y \in G \) (10.9.1.3).

Every Locally compact group \( G \) possesses a unique left Haar measure \( \mu \).

Proof: If \( \mu \) is a Haar measure, then \( \int L_y f \, d\mu = \int f \, d\mu \) by approximation by simple functions (10.4.6.3). Conversely, if \( \int L_y f \, d\mu = \int f \, d\mu \) for any \( f \in C_c(G) \), then it holds for all \( f \in C_c(G) \), hence \( \mu(xE) = \mu(E) \) by Riesz-Markov-Kakutani representation theorem (10.9.1.10).

For \( f, \varphi \in C_c^+(G) \), define \( (f: \varphi) \) to be the infimum of all finite sums \( \sum_{i=1}^n c_i \) that \( f \leq \sum_{i=1}^n c_i L_{x_i} \varphi \) for some \( x_1, \ldots, x_n \in G \). This makes sense because \( f \) has finite support so can be covered by f.m. translation of any open set. This quantity satisfies the following properties:

- \( (f : \varphi) = (L_y f : \varphi) \) for any \( y \in G \).
- \( (f_1 + f_2 : \varphi) \leq (f_1 : \varphi) + (f_2 : \varphi) \).
- \( (cf : \varphi) = c(f : \varphi) \).
- \( (f_1 : \varphi) \leq (f_2 : \varphi) \) for \( f_1 \leq f_2 \).
- \( (f : \varphi) \geq ||f||_{\sup} ||\varphi||_{\sup} \).
- \( (f : \varphi) \leq (f : \psi)(\psi : \varphi) \) for any \( \psi \in C^+(G) \).
Now choose a \( f_0 \in C_c^+(G) \) and define \( I_\varphi(f) = \frac{\langle f, \varphi \rangle}{\langle f_0, \varphi \rangle} \) for \( f, \varphi \in C_c^+(G) \). Then \( I_\varphi \) is left-invariant, sub-additive, homogeneous of degree 1, and monotone. Moreover, it satisfies \( (f_0 : f)^{-1} \leq I_\varphi(f) \leq (f : f_0) \).

Let \( X_f \) be the interval \( [(f_0 : f)^{-1}, (f : f_0)] \), and let \( X = \prod_{f \in C_c^+(G)} X_f \), then for each nbhd \( V \) of \( 1 \in G \), let \( K(V) \) be the closure in \( X \) of \( \{I_\varphi|\text{Supp}(\varphi) \subset V\} \), then these sets satisfy finite intersection property. So by compactness, there is an \( I \) contained in every \( K(V) \). Which means for any nbhd \( V \) of \( 1 \in G \) and \( \varepsilon > 0 \) and \( f_1, \ldots, f_n \in C_c^+(G) \), there exists \( \varphi \in C_c^+(G) \) that \( |I(f_i) - I_\varphi(f_i)| < \varepsilon \). Then by some argument, \( I \) commutes with left translation, addition and multiplication by positive scalars. Now extend \( I \) to a positive linear functional on \( C_c(G) \), and then use Riesz-Markov-Kakutani representation theorem\(^{\text{(10.9.1.10)}}\) to finish.

**Lemma (10.9.1.12).** For any \( f_1, f_2 \in C_c^+(G) \) and \( \varepsilon > 0 \), there is a neighborhood \( V \) of \( 1 \in G \) that in the notation in the proof of\(^{\text{(10.9.1.11)}}\), \( I_\varphi(f_1) + I_\varphi(f_2) \leq I_\varphi(f_1 + f_2) + \varepsilon \) whenever \( \text{Supp}(\varphi) \subset V \).

**Proof:** Let \( g \in C_c^+(G) \) that \( g = 1 \) on \( \text{Supp}(f_1 + f_2) \) and \( \delta > 0 \), let \( h_i = f_i/(f_1 + f_2 + \delta g) \), then \( h_i \in C_c^+(G) \) and there is a nbhd \( V \) of \( 1 \in G \) s.t. \( |h_i(x) - h_i(y)| < \delta \) for \( i = 1, 2 \) and \( y^{-1}x \in V \). Take \( \varphi \in C_c^+(G) \) with \( \text{Supp}(\varphi) \subset V \). If \( h \leq \sum c_iL_{x_i}\varphi \), then
\[
  f_1(x) = h(x)h_i(x) = \sum c_j\varphi(x_j^{-1}x)h_i(x) \leq \sum c_j\varphi(x_j^{-1}x)[h_i(x_j) + \delta]
\]
becaus when ever \( \varphi(x_j^{-1}x) \neq 0 \), \( |h_i(x) - h_i(x_j)| < \delta \). As \( h_1 + h_2 < 1 \),
\[
  (f_1 : \varphi) + (f_2 : \varphi) \leq \sum c_j|h_1(x_j) + \delta| + \sum c_j|h_2(x_j) + \delta| \leq \sum c_j[1 + 2\delta]
\]
which implies
\[
  I_\varphi(f_1) + I_\varphi(f_2) \leq (1 + 2\delta)I_\varphi(h) \leq (1 + 2\delta)[I_\varphi(f_1 + f_2) + \delta I_\varphi(g)].
\]
Notice \( \delta \) is arbitrary, thus we can choose \( \delta \) small enough that the assertion is true.

**Prop. (10.9.1.13).** If \( G \) is a locally compact group and \( \mu \) is a Haar measure on \( G \), then for any open subset \( U \) of \( G \), \( \mu(U) > 0 \).

**Proof:** By inner regularity, \( \mu(K) > 0 \) for some compact subset \( K \). Suppose \( \mu(U) = 0 \) for an open subset \( U \), then f.m. translates of \( U \) covers \( K \), contradiction.

**Prop. (10.9.1.14).** Integration of a nontrivial character on a compact group \( G \) w.r.t. the Haar measure is 0.

**Proof:** \( \int f(x)d\mu(x) = \int f(y)d\mu(y) = f(y)\int f(x)d\mu(x) \). Now choose a \( y \) that \( f(y) \neq 1 \).

**Def. (10.9.1.15) [Modular Function].** For a left Haar measure \( \mu \) on a locally compact group \( G \), \( \mu_x(E) = \mu(Ex) \) is also a left Haar measure, so there is a \( \Delta(x) \) that \( \mu_x = \Delta(x)\mu \). Then the function \( \Delta \) is a group homomorphism from \( G \) to \( \mathbb{R}^+ \), which is called the **modular function** of \( G \).

\( G \) is called **unimodular** if \( \Delta = 1 \), i.e. a left Haar measure is also a right Haar measure. Obviously, a locally compact Abelian group is unimodular.

**Prop. (10.9.1.16).** \( \Delta \) is a continuous group homomorphism from \( G \) to \( \mathbb{R}^+ \), and
\[
  \int R_yf d\mu = \Delta(y^{-1})\int f d\mu.
\]
equivalently, \( d\mu(xy_0) = \Delta(y_0)d\mu(x) \).
**Proposition 10.9.1.17** [Involution Measure]. If \( \mu \) is a left Haar measure and \( \rho \) is defined by \( \rho(E) = \mu(E') \), then \( \rho \) is a right Haar measure, and \( d\rho(x) = d\mu(x^{-1}) = \Delta(x^{-1})d\mu(x) \).

**Proof:** Notice

\[
\int R_y(f)(x)\Delta(x^{-1})d\mu(x) = \Delta(y) \int f(xy)\Delta((xy)^{-1})d\mu(x) = \int f(x)\Delta(x^{-1})d\mu(x),
\]

so \( \Delta(x^{-1})d\mu(x) \) is a right Haar measure, hence \( cd\mu(x^{-1}) \) for some \( c \). If \( c \neq 1 \), we let \( U \) be a precompact symmetric nbhd of \( 1 \) such that \( |\Delta(x^{-1}) - 1| \leq \frac{1}{2}|c-1| \) on \( U \). Then \( |c-1|\mu(U) = |\int_U \Delta(x^{-1}) - 1|d\mu(x)| \leq \frac{1}{2}|c-1|\mu(U) \), contradiction. 

**Proposition 10.9.1.18**. For a compact group \( K \) of \( G \), \( \Delta \) is trivial on \( K \). So compact group is unimodular, and if \( G/[G,G] \) is compact, then it is also unimodular.

**Proof:** These all follow from (10.9.1.16) and the fact that a compact subgroup of \( \mathbb{R}^+ \) is \{1\}, and \( \mathbb{R} \) is Abelian.

**Proposition 10.9.1.19** [Lie Type Case]. Suppose \( G \) is an open subset of \( K^N \) where \( K \) is a local field, and the left translation is given by

\[
xy = A(x)y + b(x)
\]

then the Haar measure of \( G \) is given by \( |\det A(x)|^{-1}dx \), where \( dx \) is the Lebesgue measure on \( \mathbb{R}^N \).

Also when we want to calculate the right Haar measure, consider the right action.

**Proof:** Use change of variable formula, because \( A(xy) = A(x)A(y) \), and

\[
|\det A(ax)|^{-1}d(ax) = |\det A(ax)|^{-1}d(A(ax)b(x)) = |\det A(x)|^{-1}dx.
\]

**Corollary 10.9.1.20** [Examples of Lie Group Measures].

- \( dx/|x| \) is the Haar measure on \( \mathbb{R}^* \).
- \( dx dy / x^2 + y^2 \) is the Haar measure on \( \mathbb{C}^* \).
- \( x_1 x_2^{2} \ldots x_n^{n} \prod_{i<j} dx_{ij} \) (resp. \( x_1^{n} x_2^{n-1} \ldots x_n \prod_{i<j} dx_{ij} \)) are the left (resp. right) Haar measure on the group of upper-triangular matrixes in \( GL(n, \mathbb{R}) \).
- \( \prod_{i<j} dx_{ij} \) is the left and right Haar measure on the group of upper-triangular unipotent matrices in \( GL(n, \mathbb{R}) \).
- \( |\det T|^{-n}dT \) is the left and right Haar measure on the group \( GL(n, \mathbb{R}) \), where \( dT \) is the Lebesgue measure on \( M_n(\mathbb{R}) = \mathbb{R}^{n^2} \).
• The $ax + b$ group $G$ of all affine (invertible) translations of $\mathbb{R}$ has left measure $dadb/a^2$ and right Haar measure $dadb/a$.

**Proof:** Clear. □

**Prop. (10.9.1.21) [Modular Function of Lie Groups].** If $G$ is a Lie group and $\text{Ad}$ is the adjoint action of $G$ on $\mathfrak{g}$, then $\Delta(x) = |\det \text{Ad}(x^{-1})|$. 

**Proof:** Let $G$ be a Lie group of dimension $m$, then the Haar measure on a Lie group is given by the absolute value of a left-invariant $m$-form $\omega$. Now for any $X \in \mathfrak{g}$ corresponding to a left invariant vector space $L_X$, 

$$d(R_g)_p((L_X)_p) = (L_{\text{Ad}(g^{-1})X})_p g$$

by (11.6.3.5), so $R_g^*\omega = \det(\text{Ad}(g^{-1}))\omega$. So $\Delta(g)\omega = R_g^*|\omega| = |\det(\text{Ad}(g^{-1}))||\omega|$. □

**Cor. (10.9.1.22) [Unimodular Lie Groups].** Any Abelian/compact/semisimple/reductive/nilpotent Lie group is unimodular.

**Proof:** The nilpotent case follows directly from (10.9.1.21), as $\det \text{Ad}(x) = \exp(\text{tr} \text{ad}(x))$ and $\text{ad}(x)$ is nilpotent. The compact case is by (10.9.1.18). For the semisimple case, $G = [G, G]$ because $\mathfrak{g} = [\mathfrak{g}, \mathfrak{g}](2.5.2.4)$ and it is connected, so we are done by (10.9.1.18). For the reductive case: Cf. [Kna96]P467. □

### Convolutions

**Def. (10.9.1.23) [Convolution of Measures].** If $\mu, \nu$ are two complex (hence finite) Radon measures on $G$, the map 

$$I(\varphi) = \int \int \varphi(xy)d\mu(x)d\nu(y)$$

is clearly a linear functional on $C_c(G)$ that satisfies $|I(\varphi)| \leq ||\varphi||_{\text{sup}}||\mu|| ||\nu||$, so it defines a measure on $G$ by Riesz representation (10.9.1.10), called the **convolution** of $\mu$ and $\nu$, denoted by $\mu * \nu$, that 

$$||\mu * \nu|| \leq ||\mu|| ||\nu||.$$

**Prop. (10.9.1.24) [Measure Algebra].**

- The convolution of measure is associative.
- $\delta_x * \delta_y = \delta_{xy}$.
- The convolution of measure is commutative iff $G$ is commutative.
- The convolution makes $M(G)$ into a unital Banach algebra, called the **measure algebra** of $G$.

**Proof:**

1: If $\varphi \in C_c(G)$, then 

$$\int_G \varphi d[\mu * (\nu * \sigma)] = \int \int \varphi(xy)d\mu(x)d(\nu * \sigma)(y)$$

$$= \int \int \int \varphi(xyz)d\mu(x)d\nu(y)d\sigma(z)$$

$$= \int \varphi(yz)d(\mu * \nu)(y)d\sigma(z)$$

$$= \int \varphi d[(\mu * \nu) * \sigma]$$
Prop. (10.9.1.27). The convolution \( f \ast g \) can be calculated in multiple ways by left invariance and (10.9.1.17):

\[
\int f(y)g(y^{-1}x)dy = \int f(xy)g(y^{-1})dy = \int f(y^{-1})g(xy)\Delta(y^{-1})dy = \int f(xy^{-1})g(y)\Delta(y^{-1})dy.
\]

In particular, if \( G \) is unimodular, then it can be calculated anyway you want.

Prop. (10.9.1.28). For \( 1 \leq p < \infty \), the left and right translations of \( G \) on \( L^p(G) \) are all continuous.

**Prop. (10.9.1.29)** [*L^p-Estimate*]. If $1 \leq p < \infty$, $f \in L^1(G)$ and $g \in L^p(G)$, then
- $f * g \in L^p(G)$, and $\|f * g\|_p \leq \|f\|_1 \|g\|_p \leq \|f\|_p \|g\|_p$.
- If $G$ is unimodular or $f$ has compact support, then the same as above holds for $g * f$.

*Proof:* 1: By Minkowski’s inequality (10.4.5.5),
\[\|f * g\|_p = \left| \int f(y)L_y g dy \right|_p \leq \int |f(y)||L_y g|^p dy = \|f\|_1 \|g\|_p.
\]

2: This is similar, using (10.9.1.27). □

**Prop. (10.9.1.30)** [*Convolution*].
- Suppose $G$ is unimodular and $f \in L^p(G)$, $g \in L^q(G)$ with $1/p + 1/q = 1$, $1 < p < \infty$, then $f * g \in C_0(G)$, and $\|f * g\|_{sup} \leq \|f\|_p \|g\|_q$.
- Suppose $f \in L^1(G)$, $g \in L^\infty(G)$, then $f * g$ is left uniformly continuous, and $g * f$ is right uniformly continuous.


**Prop. (10.9.1.31)** [*Approximate Identity*]. Let $\mathcal{U}$ be a neighborhood base of $1 \in G$. A family of $L^\infty$ functions $\{\varphi_U\}$ are called an approximate identity if:
1. $\int_0^1 \Phi_U(x) dx = 1$.
2. $\sup \int_0^1 |\Phi_U(x)| dx < \infty$.
3. For any $\delta > 0$, $\int_{G \setminus U} |\Phi_U(x)| dx \to 0$ as $N \to +\infty$.

For any approximate identity, if $1 \leq p < \infty$ and $f \in L^p(G)$ for $1 \leq p < \infty$, or $p = \infty$ and $f$ is left uniformly continuous, then $\Phi_U * f \to f \in L^p(G)$.


**Homogenous Spaces**

**Def. (10.9.1.32)** [*Notations*]. If $G$ is a locally compact group with left Haar measure $dx$ and $H$ is a closed subgroup with left Haar measure $d\xi$, let $q : G \to G/H$ be the quotient map.

**Prop. (10.9.1.33)**. If $G$ is a $\sigma$-compact locally compact group and $S$ is a transitive $G$-space that is locally compact and Hausdorff, then if $s_0 \in S$ and $\text{Stab}(s_0) = H$, then $G/H \cong S$ as $G$-spaces.

*Proof:* Cf. [Folland P60]. □

**Lemma (10.9.1.34)**. If $E \subset G/H$ is compact, then there is a compact $K \subset G$ that $q(K) = E$.

*Proof:* Choose a precompact nbhd $V$ of $1$ in $G$, since $q$ is open, the set $q(xV)$ is an open cover of $E$, so there are f.m. $x_i$ that $E \subset \cup q(x_iV)$. Then let $K = q^{-1}(E) \cap (\cup x_iV)$, this will suffice. □

**Def. (10.9.1.35)** [*Fundamental Domain*]. A fundamental domain for a group $\Gamma$ acting discontinuously on a locally compact second countable Hausdorff space $X$ is an Borel subset $F \in X$ that:
- $\cup_{\gamma \in \Gamma} \gamma F = \mathcal{H}$.
- if $\gamma \neq 1 \in \Gamma$, then $\gamma F \cap F = \emptyset$. 


Then fundamental domains exist.

\textbf{Proof}: The quotient space $G \backslash \Gamma$ is locally compact second countable, thus there is a countable set of precompact open basis $\{B_i\}$ for $G \backslash \Gamma$, and a countable set of precompact open basis $\{C_i\}$ for $X$. For each $\pi \in G \backslash \Gamma$, choose $\pi \in B_i(\pi)$ and choose a preimage $x \in X$ and a nbhd $C_i(x)$ that $C_i(x) \cap \gamma(C_i(x)) = \emptyset$ for any $\gamma \neq 1$, then there is a nbhd $B_j(x)$ contained in the image of $C_i(x)$. Then we can take a precompact preimages of $B_j(\pi)$ in $C_i(x)$ (by (10.9.1.34)), labeled by $U_i$. Then $U_i$ maps isomorphically to their images in $G \backslash \Gamma$ and covers $G \backslash \Gamma$.

Now take $V_1 = W_1 = U_1$, and $W_{n+1} = U_{n+1} \setminus \bigcup_{\gamma \in \Gamma} \gamma(V_n)$, $V_{n+1} = V_n \cup W_{n+1}$. Then $\bigcup V_i$ is a fundamental domain. \hfill $\square$

\textbf{Prop. (10.9.1.36)[Projection of Functions]}. There is a map $P : C_c(G) \rightarrow C_c(G/H) : Pf(xH) = \int_H f(x\xi)d\mu(\xi)$. $Pf$ is continuous and this map is well-defined and surjective.

And $\text{Supp}(Pf) \subset q(\text{Supp }f)$, and if $\varphi \in C_c(G/H)$, then $P((\varphi \circ q)f) = \varphi Pf$.

\textbf{Proof}: $Pf$ is continuous because $f$ is left uniformly continuous (10.9.1.3). By (10.9.1.37), there is a $g \geq 0 \in C_c(G)$ that $Pg = 1$ on $\text{Supp }\varphi$. Let $f = (\varphi \circ f)g$, then $Pf = \varphi(Pg) = \varphi$. \hfill $\square$

\textbf{Lemma (10.9.1.37)}. If $F \in G/H$ is compact, then there is a $f \in C_c(G)$ that $f \geq 0$ and $Pf = 1$ on $F$.

\textbf{Proof}: Let $E$ be a precompact nbhd of $F$ in $G/H$, choose a compact $K \subset G$ that $q(K) = E$ by (10.9.1.34). Choose $g \in C_c(G) \geq 0$ that is positive on $K$ and $\varphi \in C_c(G/H)$ that is 1 on $F$ and vanish outside $E$, then set

$$f = \frac{\varphi \circ q}{Pg \circ q}$$

then $f \geq 0$ and $Pf = (\varphi/Pg)Pg = \varphi$. \hfill $\square$

\textbf{Prop. (10.9.1.38)[Quotient Measure Regular Case]}. If $G$ is a locally compact group and $H$ is a closed subgroup, then there is a $G$-invariant positive Radon measure $\mu$ on $G/H$ if $\Delta_G \mid H = \Delta_H$.

And if this is the case, then this measure is unique up to constant, and if suitably chose, satisfies:

$$\int_G f(x)dx = \int_{G/H} Pf d\mu = \int_{G/H} \int_H f(x\xi)d\xi d\mu(xH).$$

for any $f \in C_c(G)$.

\textbf{Proof}: Cf.[Folland Abstract Analysis P62]. \hfill $\square$

\textbf{Cor. (10.9.1.39)[Decomposition of Measure]}. If $G$ is a unimodular locally compact group and $P, K$ be closed subgroups s.t. $P \cap K$ is compact and $G = PK$. Let $dLP, dRk$ be the left and right Haar measure on $P, K$ respectively, then a Haar measure on $G$ is given by

$$\int_G f(g)dg = \int_K \int_P f(pk)dLpdRk.$$

\textbf{Proof}: Consider $H = P \times K$ and $M = P \cap K$ embedded diagonally in $H$, then there is a homeomorphism $H/M \cong G$ given by $(p, k) \mapsto pk^{-1}$. Then we can verify both side are $H$-invariant quotient measure on $G \cong H/M$, so by uniqueness in (10.9.1.38), the equation is true. \hfill $\square$

\textbf{Def. (10.9.1.40)[Rho-Functions]}. If $G$ is a locally compact subgroup and $H$ is a closed subgroup. Let $\Delta = \Delta_G/\Delta_H$. Let $S(G, \Delta)$ be the space of continuous functions on $G$ that satisfies
for any \( h \in H \), \( f(hg) = \Delta(h)f(g) \).

- \( f \) is compactly supported in \( H \setminus G \).

**Lemma (10.9.1.41)**. Let \( G \) be a locally compact group and \( H \) a closed subgroup, then there is a continuous function \( f_0 : G \to [0, \infty) \) that

- \( f_0^{-1}((0, \infty)) \cap Hx \neq \emptyset \) for any \( x \in G \).
- \( \text{Supp } f_0 \cap HK \) is compact for any compact group \( K \) of \( G \).

**Proof**: Cf.[Folland, P64]. \( \square \)

**Lemma (10.9.1.42)**. If \( f \in C_c(G) \) and \( Pf = 0 \), then \( \int f\rho = 0 \) for any rho-function \( \rho \). In fact, this is true if \( \rho \) is allowed to take value 0.

**Proof**: Cf.[Folland P65]. \( \square \)

**Lemma (10.9.1.43)**. There is an operator \( p : C_c(G) \to C(G) \) given by

\[
p(f)(g) = \int_H f(hg)\Delta_G^{-1}(h)d\mu_H(h).
\]

Then \( p \) is right \( G \)-invariant, and \( p(ff') = fp(f') \) for any \( f' \in C_c(G) \) and \( f \in C(G) \) that is \( H \)-invariant.

- The image of \( p \) is \( S(G, \Delta) \), and if \( s \geq 0 \in S(G, \Delta) \), then there is a non-negative \( f \geq 0 \in C_c(G) \) that \( p(f) = s \).

- If \( p(f) = 0 \), then \( \int_G f(x)d\nu_G(x) = 0 \), where \( d\nu_G \) is a right Haar measure on \( G \).

**Proof**: 1: It is clearly that \( p(f)(gh) = \Delta(h)p(f)(g) \), and let \( f_0 \) be defined as in(10.9.1.41), then \( s_0 = p(f_0) \) is positive-valued. Now for any \( s \in S(G, \Delta) \), \( p(ss_0^{-1}f_0) = ss_0^{-1}p(f_0) = s \), and \( sf_0 \in C_c(G) \) by hypothesis.

2: If \( p(f) = 0 \), then

\[
\int_G \int_H s_0^{-1}(g)f_0(g)f(hg)\Delta_G^{-1}(h)d\mu_H(h)d\nu_G(g) = \int_G \int_H \Delta(h)s_0^{-1}(g)f_0(h^{-1}g)f(g)d\mu_H(h)d\nu_G(g)
\]

\[
= \int_G \int_H f_0(hg)\Delta_G(h)^{-1}d\mu_H(h)]s_0^{-1}(g)f(g)d\nu_G(g)
\]

\[
= \int_G f(g)d\nu_G(g)
\]

\( \square \)

**Prop. (10.9.1.44) [Haar Measure on Rho-Functions]**. There exists a unique continuous positive functorial \( \nu_{H \setminus G} \) on \( S(G, \Delta) \) that for any \( f \in C_c(G) \),

\[
\int_G f(x)d\nu_G(x) = \int_{H \setminus G} p(f)(y)d\nu_{H \setminus G}(y) = \int_{H \setminus G} \int_H f(hg)\Delta_G^{-1}(h)d\mu_H(h)d\nu_{H \setminus G}.
\]

and it is invariant under the right action of \( G \). We denote \( \nu_{H \setminus G}(s) = \int_{H \setminus G} s(g)d\nu_{H \setminus G}(g) \) for \( s \in S(G, \Delta) \).

**Proof**: This follows from(10.9.1.43). \( \square \)

**Cor. (10.9.1.45)**. If \( G \) is a unimodular locally compact group and \( H, K \) be closed subgroups s.t. \( H \cap K \) is compact and \( G = PK \), then the the quotient measure \( \mu_{H \setminus G} \) is given by

\[
f \mapsto \int_K f(k)d\nu_K(k).
\]

where \( d\mu_K(k) \) is a right Haar measure on \( K \), by comparison with(10.9.1.39).
Maximal Compact Subgroup

Def.(10.9.1.46)[Maximal Compact Subgroup]. A maximal compact subgroup of a locally compact group $G$ is a maximal object in the set of all compact subgroup of $G$.

Prop.(10.9.1.47)[Cartan-Iwasawa-Malcev theorem]. Maximal compact subgroup exists for any locally compact group $G$.

Proof: □

Locally Profinite Groups

Def.(10.9.1.48)[Locally Profinite Group]. A locally profinite group is a locally profinite topological group. A profinite group is locally profinite, and any compact open subgroup of a locally profinite group is profinite.

Cor.(10.9.1.49). A closed subgroup of a locally profinite group is locally profinite, and a quotient group is locally profinite.

Proof: The proof is very similar to that of (2.1.14.4), as the result of (3.6.1.24) remains true, because any connected nbhd of $e$ is contained in any compact open subgroup. □

Prop.(10.9.1.50)[Compact Open Subgroups Form a Basis]. If $G$ is a locally profinite group, then the set of compact open subgroups form a basis of the nbhd of $1$.

Proof: For any nbhd $U$ of 1, choose a precompact nbhd $V$ of 1 contained in $U$, then there is another compact open subgroup contained in $V$, by (3.8.1.24). □

Prop.(10.9.1.51)[Quotient of Locally Profinite Group]. A quotient subspace of a locally profinite group is locally profinite.

Proof: Consider the $H$ action on $G$, then it is regular, because the graph is the preimage of $H$ in the map $G \times G \rightarrow G : (g_1,g_2) \mapsto g_1^{-1}g_2$. So by (3.8.1.10) $G/H$ is Hausdorff. But clearly $G \rightarrow G/H$ is open and $G/H$ is locally profinite as it has a basis of locally compact subsets. □

Lemma(10.9.1.52). Let $G$ be a locally profinite group and $H$ a closed subgroup, then for any open compact subspace $V \subset G/H$, there is an open compact subspace $U \subset G$ that $p(U) = V$.

Proof: The preimage $p^{-1}(V)$ is open, so there is a covering of $p^{-1}(V)$ by open compact subsets $U_i$. Then $p(U_i)$ are open and covers $V$, thus there are f.m. $U_i$ that $p(\cup U_i) = V$. □

Prop.(10.9.1.53)[Homogeneous Group]. Let $G$ be a locally profinite group that is $\sigma$-compact. If $G$ acts transitively on a locally profinite space $X$, let $x_0 \in X$ and $\text{Stab}(x_0) = H$, then $G/H \rightarrow X$ is a homeomorphism. Is this true for locally compact groups?

Proof: Let $N$ be a compact open subset of $N$, and $g_i$ be the left coset representatives for $N$, which is countable. Now $X = \cup_i \gamma(g_iN)x_0$. Because a locally profinite space is a Baire space, some $\gamma(g_iN)x_0$ contains a nbhd of $\gamma(g_iN)x$. Now left acts $(g,j)^{-1}$, we see $x_0$ is an interior point of $\gamma(N)x_0$. Now $N$ is arbitrary, thus (10.9.1.50) shows $g \mapsto \gamma(g)x$ is open, thus $G/H \rightarrow X$ is open. It is clearly continuous, thus $G/H \cong X$. □
2 Unitary Representations

Def. (10.9.2.1)[Intertwining Operators]. If $\pi_1, \pi_2$ are unitary representations of $G$, then the space $C(\pi_1, \pi_2)$ of intertwining operators of $\pi_1, \pi_2$ as:

$$C(\pi_1, \pi_2) = \{ T : \mathcal{H}_{\pi_1} \rightarrow \mathcal{H}_{\pi_2} : T\pi_1(x) = \pi_2(x)T, \ \forall x \in G \}.$$  

And denote $C(\pi_1, \pi_1)$ by $C(\pi_1)$.

Lemma (10.9.2.2). The adjoint operator $S \mapsto S^*$ induces a bijection between the spaces $C(\pi_1, \pi_2) \cong C(\pi_2, \pi_1)$.

Lemma (10.9.2.3). If $\mathcal{H}_\pi$ is a representation of $G$, $M$ is a closed subspace. Let $P$ be the orthogonal projection onto $M$, then $M$ is invariant under $\pi$ iff $P \in C(\pi)$.

Proof: If $P \in C(\pi)$ and $v \in M$, then $\pi(x)v = \pi(x)Pv = P\pi(x)v \in M$, so $M$ is $\pi$-invariant. Conversely if $M$ is $\pi$-invariant, then so does $M^\perp$, so $\pi(x)Pv = P\pi(x)v$, and also for $v \in M^\perp$, so $\pi(x)P = P\pi(x)$, for any $x$. □

Prop. (10.9.2.4)[Schur’s Lemma].

- A unitary representation $\pi$ of $G$ is irreducible iff $C(\pi)$ consists only of scalar multiples of identity.
- If $\pi_1, \pi_2$ are non-equivalent irreducible unitary representations of $G$, then $C(\pi_1, \pi_2) = 0$.

Proof: 1: if $\pi$ is reducible, then it contains a non-trivial projection by lemma (10.9.2.3). Conversely, if $T \neq cI \in C(\pi)$, then we consider $A = \frac{1}{2}(T + T^*)$, $B = \frac{1}{2}(T - T^*)$, then at least one of them are not $cI$. But they are normal, thus by symbolic calculus (10.8.4.3) any $\chi_E(A)$ for some $E \subset \mathbb{R}$ Borel is non-trivial (because the spectrum of $A$ is not a single point) and commutes with $\pi$, so $\mathcal{H}_\pi$ is reducible by (10.9.2.3) again.

2: By (10.9.2.2), for $T \in C(\pi_1, \pi_2)$, $T^* \in C(\pi_2, \pi_1)$, $TT^* = cI, T^*T = cI$. so $T = 0$ or $c^{-1/2}T$ is unitary, and it is an isomorphism between $\pi_1, \pi_2$. □

Cor. (10.9.2.5). If $G$ is Abelian, then any irreducible representation of $G$ is 1-dimensional.

Proof: If $\pi$ is a representation of $G$, then any $\pi(x)$ commutes with $\pi$, thus $\pi(x) = c_x I$ for some $c_x$, so every subspace of $\mathcal{H}_\pi$ is irreducible, thus $\dim \mathcal{H} = 1$. □

Prop. (10.9.2.6)[Unitary Representation and $L^1(G)$-Representation]. Any unitary representation $(\pi, \mathcal{H})$ of $G$ determines a representation of $L^1(G)$ by

$$f \mapsto \int f(x)\pi(x)dx$$

This is a non-degenerate $*$-representation of $L^1(G)$.

And conversely, any non-degenerate $*$-representation of $L^1(G)$ arises from a unitary representation of $G$.

Proof: If $\pi$ is a unitary representation and $f \in L^1$, let $\pi(f)$ be defined as

$$\pi(f)u = \int f(x)\pi(x)udx,$$
where the integral is in the weak sense (10.7.3.25), and it satisfies \( ||\pi(f)|| \leq ||f||_1 \).
For the \(*\)-algebra structure (10.9.1.26), it suffices to prove that
\[
\pi(f * g) = \pi(f)\pi(g), \quad \pi(f^*) = \pi(f)^* ,
\]
which are true for formal reason:
\[
\begin{align*}
\pi(f * g) &= \int \int f(y)g(y^{-1}x)\pi(x)dydx = \int \int f(y)g(xy)dx dy = \pi(f)\pi(g), \\
\pi(f^*) &= \int \Delta(x^{-1})\overline{f(x)}\pi(x)dx = \int \overline{f(x)}\pi(x^{-1})dx = \int (f(x)\pi(x))^* dx = \pi(f)^*.
\end{align*}
\]
and verified by supplying \( u, v \). For the non-degeneracy, for any \( u \neq 0 \in \mathcal{H} \), choose a precompact nbhd \( V \) of identity that \( ||\pi(x)u - u|| < ||u|| \) for \( x \in V \), and let \( f = |V|^{-1}\chi_V \), then it can be verified that \( ||\pi(f)u|| \neq 0 \).
For the converse, Cf. [Folland P79-81]?
\( \square \)

**Prop. (10.9.2.7).** We want to consider the difference of the image of \( L^1(G) \) and \( G \) under these two representations: Let \( \pi \) be a unitary representation of \( G \), then
- The bicommutant (10.8.3.13) of \( \pi(G) \) and \( \pi(L^1(G)) \) are identical.
- \( T \in \mathcal{L}(\mathcal{H}) \) intertwines \( \pi \) iff it commutes with every \( \pi(f) \in \pi(L^1(G)) \).
- A closed subspace \( M \) of \( \mathcal{H} \) is invariant under \( \pi \) iff \( \pi(f)M \subset M \) for any \( f \in L^1(G) \).

**Proof:**
1: Cf. [Folland, P82].
2 follows from 1 noticing the fact that \( T \) commutes with an algebra iff it commutes with its von-Neumann algebra.
3 follows from 2 and (10.9.2.3).
\( \square \)

**Prop. (10.9.2.8) [Completion of Unitary Representation].** If \( \mathcal{H}_0 \) is a Hermitian inner product space that \( G \) is a topological group acting continuously on \( \mathcal{H}_0 \) that preserves the inner product, then if \( \mathcal{H} \) is the Hilbert completion of \( \mathcal{H}_0 \), then the action of \( G \) extends to a continuous unitary action on \( \mathcal{H} \).

**Proof:**
The extension is clear as \( ||\pi(g)f|| = ||f|| \). For the continuity, if \( v \in \mathcal{H}, g \in G, \varepsilon > 0 \), let \( v_0 \in \mathcal{H}_0 \) that \( |v - v_0| < \varepsilon/6 \), then there is a nbhd \( W \) of \( g \) that if \( g_1 \in W \), then \( |\pi(g_1)v_0 - \pi(g)v_0| < \varepsilon/3 \). Then if \( |v_1 - v| < \varepsilon/6 \) and \( g_1 \in W \), then
\[
|\pi(g_1)v_1 - \pi(g)v| = |\pi(g_1)v_1 - \pi(g_1)v_0 + \pi(g_1)v_0 - \pi(g)v_0 + \pi(g)v_0 - \pi(g)v| \\
\leq |\pi(g_1)v_1 - \pi(g_1)v_0| + |\pi(g_1)v_0 - \pi(g)v_0| + |\pi(g)v_0 - \pi(g)v| \\
= |v_1 - v_0| + |\pi(g_1)v_0 - \pi(g)v_0| + |\pi(g)v_0 - \pi(g)v| \\
\leq \varepsilon
\]
which shows the action is continuous.
\( \square \)

**Cor. (10.9.2.9).** Given a locally compact group \( G \) and a discrete subgroup \( \Gamma \), the right regular action of \( G \) extends to a continuous unitary representation of \( G \) on \( L^2(\Gamma \backslash G, \omega) \).

**Proof:**
Because we can approximate \( f \in L^2(\Gamma \backslash G) \) by compactly supported continuous functions (10.4.6.6), then the \( G \) action is uniformly continuous.
Lemma (10.9.2.10) [Auxiliary Compact Supported Function Approximation]. Let \( G \) be a locally compact Lie group and \( K \) a compact subgroup. If \((\pi, \mathcal{H})\) is a unitary representation of \( G \) on a Hilbert space, and let \( f \neq 0 \in \mathcal{H} \), then for any \( \varepsilon > 0 \), there is a \( \varphi \in C_c^\infty(G) \) s.t. \( \pi(\varphi) \) is self-adjoint and \(|\varphi(\rho)f - f| < \varepsilon\).

Moreover, if \( f \in \mathcal{H}^c \) which is the decomposition part for \( K \), we can assume \( \varphi(kg) = \varphi(gk) = \xi(k)^{-1}\varphi(g) \). In particular if \( \mathcal{H}^c \) is f.d., we find a \( \varphi \) that \( \pi(\varphi)f = f \).

Proof: By continuity, there is a nbhd \( H \) of 1 that \(|\pi(g)f - f| < \varepsilon\), then we can choose a \( \varphi \) positive real valued with support in \( U \) with integral 1, then \(|\pi(\varphi)f - f| < \varepsilon\) by (10.7.3.22). We can also choose \( \varphi(g) = \varphi(g^{-1}) \), then \( \pi(\varphi) \) is self-adjoint.

For the second case, notice first there is a nbhd \( V \) of 1 that \( kV^{-1}k^{-1} \in U \) for any \( k \in K(3.8.1.6) \), so let \( \varphi_1 \) be a positive real valued function supported in \( V \), and let

\[
\varphi_0(g) = \int_K \varphi_1(kgk^{-1})dk
\]

then \( \varphi_0 \) is supported in \( U \) and \( \varphi(kgk^{-1}) = \varphi_0(g) \) for any \( k \in K \). Assume now that \( \pi(k_0) = e^{ik\theta}f \), then we can use (10.9.1.39) for \( P = G \) to see that

\[
\pi(\varphi_0)f = \int_G \varphi_0(h)\pi(h)fgh = \int_G \int_K \varphi_0(hk)\pi(h)kfkdhdh = \int_G \int_K \xi(k)\varphi_0(hk)k\pi(h)fkdhdh = \pi(\varphi)f
\]

where

\[
\varphi(g) = \int_K \xi(k)\varphi_0(gk)dk = \int_K \xi(k)\varphi_0(gk)dk
\]

so \( \varphi(k) = \varphi(gk) = \xi^{-1}(k)\varphi(g) \) as required. \( \square \)

Functions of Positive Type

Def. (10.9.2.11) [Positive Type Function]. A function of \textbf{positive type} on a closed compact group \( G \) is a function \( \varphi \in L^\infty(G) \) that defines a positive linear functional on the \( B^*\)-algebra \( L^1(G) \). In other word,

\[
\int f(x)\overline{f(y)}\varphi(y^{-1}x)dxdy \geq 0, \quad \forall f \in L^1(G).
\]

We denote by \( P(G) \) the set of continuous functions of positive type on \( G \).

Prop. (10.9.2.12). If \( \varphi \) is of positive type, then so does \( \overline{\varphi} \). (Easy calculation).

Prop. (10.9.2.13). If \( \pi \) is a unitary representation of \( G \) and \( u \in \mathcal{H}_\pi \), then \( \varphi(x) = (\pi(x)u, u) \in P \).

Proof: \( \varphi \) is continuous by definition, so if \( f \in L^1 \), then

\[
\int \int f(x)\overline{f(y)}\varphi(y^{-1}x)d\mu(x)d\mu(y) = \int \int (f(x)\pi(x)u, f(y)\pi(y)u)dxdy = ||\pi(f)u||^2 \leq 0
\]

Prop. (10.9.2.14). If \( f \in L^2(G) \), then \( f \ast \overline{f} \in P(G)(10.9.1.2) \).

Proof: Cf.[Folland, P84]. \( \square \)

Prop. (10.9.2.15) [Cyclic Representations and Functions of Positive Type]. Any function of positive type arises from an irreducible representation and a cyclic vector \( \varepsilon \) as in (10.9.2.13)
Proof: Cf.[Folland P84-85]. □

Cor. (10.9.2.16). If $\varphi$ is a function of positive type, then $\varphi$ can be chosen to be continuous.

Cor. (10.9.2.17). If $\varphi \in P$, then $|||\varphi|||_{\infty} = \varphi(1)$, and $\varphi(x^{-1}) = \overline{\varphi(x)}$.

Proof: $
\varphi(x) = (\pi(x)u, u) \text{ for some representation } \pi \text{ and } u \in \mathcal{H}, \text{ so } |\varphi(x)| \leq ||u||^2 = \varphi(1) \text{ and } \varphi(x^{-1}) = (\pi(x^{-1})u, u) = (u, \pi(x)u) = \overline{\varphi(x)}.
\Box$

Def. (10.9.2.18). We set:

- $P_0(G) = \{ \varphi |||\varphi|||_{\infty} \leq 1 \} = \{ \varphi(1) = 1 \}$.
- $P_1(G) = \{ \varphi |||\varphi|||_{\infty} = 1 \} = \{ 0 \leq \varphi(1) \leq 1 \}$.

By Banach-Alaoglu, $P_0(G)$ and $P_1(G)$ are a weak*-compact set.

Prop. (10.9.2.19) [Extreme Points of $P_1$]. A $\varphi \in P_1$ is an extreme point iff the representation it corresponds is irreducible. And $E(P_0) = E(P_1) \cup \{ 0 \}$.

Proof: Cf.[Folland P86]. □

Prop. (10.9.2.20) [Two Topologies Coincide]. On $P_1$, the compact-open topology coincides with that of the weak*-topology.

Proof: Cf.[Folland Abstract Harmonic Analysis P80]. □

Prop. (10.9.2.21). The linear span $B(G)$ of $C_c(G) \cap P(G)$ includes all functions of the form $f * g$ where $f, g \in C_c(G)$. And it is dense in $C_c(G)$ and $L^p(G)$ for $p < \infty$.

Denote $B^p(G) = B(G) \cap L^p(G)$.

Proof: By (10.9.2.14), $P \cap C_c(G)$ includes all functions of the form $f \ast \tilde{f}$ with $f \in C_c(G)$, thus its linear span includes all $f \ast g$ for $f, g, \in C_c(G)$ by polarization. Thus it is dense in $C_c(G)$ and $L^p(G)$ because we can use approximate identity (10.9.1.31). □

Prop. (10.9.2.22) [Gelfand-Raikov]. If $G$ is a locally compact group, then the irreducible representations of $G$ separate points of $G$.

Proof: Cf.[Folland Abstract Analysis P91]. □

3 Locally Compact Abelian Group

Dual Group

Def. (10.9.3.1) [Dual Space]. If $G$ is locally compact, denote $\hat{G}$ the set of all irreducible unitary representations of $G$, called the dual space of $G$.

Def. (10.9.3.2) [Dual Group]. If $G$ is locally compact Abelian, the irreducible unitary representations of $G$ are all 1-dimensional by (10.9.2.5), so it forms a group, called the dual group of $G$, denoted by $\hat{G}$.

An element of $\hat{G}$ is called a character of $G$, denoted by $\xi$. And a continuous homomorphism from $G$ to $\mathbb{C}$ is called a quasi-character.

The topologies on $\hat{G}$ that makes it into a LCA group is given in (10.9.3.6).

Remark (10.9.3.3). $\hat{\mathbb{R}} \cong \mathbb{R}$, and the quasi-characters of $\mathbb{R}$ are all of the form $x \mapsto e^{sx}$ for $s \in \mathbb{C}$.
Prop. (10.9.3.4) [Dual Group as Spectrum of $L^1(G)$]. The dual group $\hat{G}$ can be regarded as the spectrum of $L^1(G)$, i.e. multiplicative homomorphism of $L^1(G)$:

$$\xi \mapsto \left( \xi(f) = \int (x, \xi)f(x)dx \right).$$

Proof: First, $\xi$ is multiplicative because

$$\xi(f \ast g) = \int \int f(y)g(y^{-1}x)(x, \xi)dydx = \int \int f(y)g(x)(xy, \xi)dydx = \xi(f)\xi(g).$$

Conversely, any continuous functional on $L^1$ is like $\varphi(f) = \int f(x)\varphi(x)dx$ for some $\varphi \in L^\infty$, and it is multiplicative, so

$$\varphi(f)\int \varphi(x)g(x) = \varphi(f)\varphi(g) = \varphi(f \ast g) = \int \int \varphi(y)f(y^{-1}x)g(x)dydx = \int \varphi(L_x(f))g(x)dx$$

So $\varphi(x) = \frac{\varphi(L_x(f))}{\varphi(f)}$, a.e., for any $f$. So $\varphi(x)$ can be chosen to be continuous, as $x \rightarrow L_x(f)$ is continuous (10.9.1.3). And clearly $\varphi$ is multiplicative. □

Cor. (10.9.3.5). $\hat{G} \subset P_1(G)$, because $\int (f \ast f)\varphi d\mu = |\Phi(f)|^2 \geq 0$.

Cor. (10.9.3.6) [Dual Group as a LCA Group]. Now we can give $\hat{G}$ the compact-open topology, then the group operation is clearly continuous, and the topology coincides with that inherited by the weak*-topology of the $L^\infty$ by (10.9.2.20), so $\hat{G} \cup \{0\}$ is a compact Hausdorff space because $\hat{G} \subset P_1(G)$ and it is the subset of $L^\infty$ that $\{h(xy) = h(x)h(y)\}$ which is weak*-closed hence weak*-compact. In particular, $\hat{G}$ is a locally compact topological group.

Prop. (10.9.3.7) [Duality between Discrete Groups and Compact Groups]. If $G$ is discrete, then $\hat{G}$ is compact, if $G$ is compact, then $\hat{G}$ is discrete.

Proof: if $G$ is discrete, then there is a unit $\delta$ in $L^1(G)$, which is 1 on $e$ and 0 otherwise. So the spectrum of $L^1(G)$ is compact by (10.8.1.21).

If $G$ is compact, then $1 \in L^1$, so $U = \{f \in L^\infty ||f| > \frac{1}{2}\}$ is weak*-open, but $U \cap \hat{G} = \{1\}$ by (10.9.1.14), so $\hat{G}$ is discrete. □

Fourier Transform

Prop. (10.9.3.8) [Fourier Transform]. The Fourier transform on $G$ is defined as in (10.9.3.4) to be the map

$$L^1(G) \rightarrow C(\hat{G}): f \mapsto \mathcal{F}f(\xi) = \hat{f}(\xi) = \int f(x)(x, \xi).$$

It is a norm-decreasing *-homomorphism form $L^1(G)$ to $C_0(\hat{G})$, and its range is a dense subspace of $C_0(\hat{G})$.

Equivalently, the Fourier transform is just the Gelfand transform of $L^1(G)$ (10.8.1.21) composed with an inverse map.
Prop. (10.9.3.9). There is another map from $M(\hat{G})$ to bounded continuous functions on $G$:

$$
\mu \mapsto (\varphi_{\mu} : x \mapsto \int (x, \xi) d\mu(\xi)).
$$

This is a norm decreasing injection from $M(\hat{G})$ to $L^\infty(G)$, and if $\mu$ is positive, then $\varphi_{\mu}$ is a function of positive type.

Proof: It suffices to prove injectivity, but if $\varphi_{\mu} = 0$, then $0 = \int \int f(x)(x, \xi) d\mu(\xi) dx = \int \hat{f}(\xi)^{-1} d\mu(\xi)$ for all $f \in L^1(G)$, so this shows $\mu = 0$ because of (10.9.3.8) and Riesz representation.

For the positive type, notice that

$$
\int \int f(x)\overline{f(y)} v_{\mu}(y^{-1}x) dx dy = \int \int f(x)\overline{f(y)}(y, \xi)(x, \xi) d\mu(\xi) dx dy = \int |\hat{f}(\xi)|^2 d\mu(\xi) \geq 0
$$

\[ \square \]

Prop. (10.9.3.10) [Bochner’s Theorem]. If $\varphi \in P(G)$, there is a unique positive $\mu \in M(\hat{G})$ s.t. $\varphi = \varphi_{\mu}$.

Proof: We have the map defined in (10.9.3.9) injects $M(\hat{G})$ into $P(G)$ (norm-decreasing), so it suffices to prove the existence. For this, we may assume $\varphi \in P₀(G)$. Let $M₀$ be the set of positive measure $\mu \in M(\hat{G})$ that $\mu(\hat{G}) \leq 1$, then $M₀$ is weak*-compact in $M(\hat{G})$. Now

$$
\int f(x)\varphi_{\mu}(x) dx = \int \int f(x) d\mu(\xi) dx = \int \hat{f}(\xi^{-1}) \mu(x)
$$

so the mapping $\mu \mapsto P₀$ must be continuous w.r.t their weak*-topologies, so the image is a compact convex subset of $P₀$. But the image contains all characters and 0 (by taking the point mess), which are the extreme points of $P₀$, by (10.9.2.19), so it contains all the $P₀$, by Krein-Milman (10.7.3.15).

\[ \square \]

Cor. (10.9.3.11). $\{\varphi_{\mu}\} = B(G)(10.9.2.21)$, by (10.9.3.10) and (10.9.3.9). Thus the inverse $B(G) \to M(\mathcal{G})$ is denoted by $f \mapsto d\mu_f$.

Cor. (10.9.3.12) [Herglotz]. A numerical sequence $\{a_n\}$ is positive iff there is a positive measure $\mu \in M(T)$ s.t. $a_n = \mu(n)$.

Prop. (10.9.3.13). The set of regular Borel probability measures on a compact $X$ is weak*-compact in $C(X)^*$. (Use Alaoglu).

Prop. (10.9.3.14) [Fourier Inversion Formula]. (special case of (10.9.3.24)) If $f \in B^1(G)(10.9.2.21)$, then $\hat{f} \in L^1(\hat{G})$, and if the Haar measure $d\xi$ of $\hat{G}$ is suitably normalized w.r.t. the Haar measure of $G$, then $d\mu_f(\xi) = \hat{f}(\xi) d\xi (10.9.3.11)$, i.e. $f(x) = \int f(x, \xi) \hat{f}(\xi) d\xi$. This measure $d\xi$ is called the dual measure of $dx$.

Proof: Cf. [Folland Abstract Harmonic Analysis P105].

Cor. (10.9.3.15). If $f \in L^1(G) \cap P$, then $\hat{f} \geq 0$, as $d\mu_f(\xi) = \hat{f}(\xi) d\xi$ and $\mu_f$ is positive, by Bochner’s theorem (10.9.3.10).
Prop. (10.9.3.16) [Dual Measure of Discrete Group]. If $\mu$ is the counting measure on a discrete group, then its dual measure satisfies $|\hat{\mu}| = 1$, and if $G$ is compact and $|\mu| = 1$, then the dual measure is the counting measure on $\hat{G}$.

Proof: First (10.9.3.7) should be noticed. If $G$ is compact and $|\mu| = 1$, then $\hat{\mu} = \chi(1)$, so $g(x) = \sum(x, \xi)\hat{g}(\xi)$, which shows the dual measure is counting measure by definition (10.9.3.14). □

Prop. (10.9.3.17) [Plancherel Theorem]. The Fourier transform on $L^1(G) \cap L^2(G)$ extends uniquely to an isomorphism from $L^2(G)$ to $L^2(\hat{G})$ that satisfies Fourier inversion formula.

Proof: Cf. [Folland P108]. □

Cor. (10.9.3.18). If $G$ is compact and $\mu(G) = 1$, then $\hat{G}$ is an orthonormal basis of $L^2(G)$.

Proof: Firstly $\hat{G}$ is an orthonormal set by (10.9.1.14). And if $f \in L^2(G)$ is orthogonal to all $\xi \in \hat{G}$, then $\int_G f\xi = \hat{f}(\xi) = 0$, thus $\hat{f} = 0$, and then $f = 0$ by Plancherel (10.9.3.17). □

Cor. (10.9.3.19) [Hausdorff-Young Inequality]. Let $1 \leq p \leq 2$ and $p^{-1} + q^{-1} = 1$. If $f \in L^p(G)$, then $\hat{f} \in L^q(\hat{G})$, and $||\hat{f}||_q \leq ||f||_p$.

Proof: Cf. [Folland, P109]. □

Schrödinger Representations

Def. (10.9.3.20) [A(G)]. Let $G$ be an locally compact Abelian group, denote $\mathbb{T} = \{c \in \mathbb{C}||c| = 1\}$, $A(G) = G^* \times G \times \mathbb{T}$ with the group law

$$ (v_1^*, v_1, t_1)(v_2^*, v_2, t_2) = (v_1^* + v_2^*, v_1 + v_2, t_1 t_2 \langle v_1, v_2^* \rangle). $$

Also we denote for $w, w' \in G^* \times G$, $[w, w'] = \langle v_1, v_2^* \rangle$.

Let $B(G) = \text{Aut}(A(G))$, $B_0(G) \subset B(G)$ be the group of elements fixing elements in the center $Z(A(G))$.

Note the commutator

$$ (v_1^*, v_1, 1)(v_2^*, v_2, 1)(v_1^*, v_1, 1)^{-1}(v_2^*, v_2, 1)^{-1} = (0, 0, \langle v_1, v_2^* \rangle \langle v_2, v_1^* \rangle^{-1}), $$

thus $\langle v_1, v_2^* \rangle \langle v_2, v_1^* \rangle^{-1}$ defines a multiplicative skew-symmetric, bilinear and perfect pairing $[,]$ of $G^* \times G$ with itself.

Prop. (10.9.3.21) [Segal-Shale-Weil]. There is an unitary representation of $A(G)$ on $L^2(G)$ given by

$$ (\rho(v^*, v, t)\Phi)(u) = t\langle u, v^* \rangle \Phi(u + v), $$

called the Schrödinger representation. In fact, it is the induced representation $\text{Ind}_{G \times \mathbb{T}}^{A(G)} \chi$, where $\chi(g, t) = t$. This representation is irreducible, and for any $\sigma \in B_0(G)$, there exists uniquely up to scalar a unitary operator $\omega(\sigma)$ on $L^2(G)$ s.t.

$$ \rho(\sigma(h)) = \omega(\sigma) \circ \rho(h) \circ \omega(\sigma)^{-1}. $$

Remark (10.9.3.22). This should be a direct consequence of the Stone-Von Neumann theorem. Cf. [History of Stone Von-Newmann Theorem] or [Easy proof of the Stone-Von Neumann Theorem]?
Proof: This is clearly a unitary representation. \( \rho \) induces an action of \( G^* \times G \) on \( L^2(G) \) via \( t = 1 \), thus an action of \( C_c(G^* \times G) \) on \( L^2(G) \):

\[
(\rho(\varphi)\Phi)(u) = \int_{G^* \times G} \varphi(w)(\rho(w,1)\Phi)(u)dw = \int_G K_{\varphi}(u,v)\Phi(v)dv
\]

where \( K_{\varphi}(u, u + v) = \int_{G^*} \varphi(v^*, v)(\langle u, v^* \rangle)dv^* \) is the Fourier transform of \( \varphi \) w.r.t. \( G^* \). As Fourier transform is \( L^2 \)-isometry, \( \varphi \mapsto K_{\varphi} \) extends to an isometry \( \lambda : L^2(G^* \times G) \cong L^2(G \times G) \), whose inverse is given by

\[
\varphi(v^*, v) = \int_G K_{\varphi}(u, u + v)(-u, v^*)du,
\]

and also the action \( \rho \) extends to all \( \varphi \in L^2(G^* \times G) \).

It can be verified that \( \rho(\varphi_1) \circ \rho(\varphi_2) = \rho(\varphi_1 \ast \varphi_2) \), where

\[
(\varphi_1 \ast \varphi_2)(w) = \int_{G^* \times G} \varphi_1(w_1)\varphi_2(w - w_1)[w_1, w - w_1]dw_1.
\]

Then by comparison with the equation above, \( K_{\varphi_1 \ast \varphi_2} = K_{\varphi_1} \ast K_{\varphi_2} \), where \( \ast \) is defined in (10.4.5.6).

\[ \sigma \in B_0(G) \] is of the form \( \sigma(w, t) = (s(w), f(w)t) \), where \( w \in G^* \times G, f : G^* \times G \rightarrow T \) is a map satisfying

\[
f(w_1 + w_2) = f(w_1)f(w_2)[s(w_1), s(w_2)][w_1, w_2]^{-1}.
\]

Notice \( s \) preserves Haar measure on \( G^* \times G \): it is preserved the pairing \( \langle \cdot, \cdot \rangle \) as it is a commutator and \( \sigma \) fixes \( Z(A(G)) \). Thus \( s \) preserves Haar measure of \( G^* \times G \), by (10.9.3.34).

Now we define a unitary transformation \( \Sigma \) of \( L^2(G^* \times G) \) by \( (\Sigma \varphi)(w) = f(w)^{-1}\varphi(s(w)) \), then it can be checked? by using the equations above that

\[
\Sigma(\varphi_1 \ast \varphi_2) = \Sigma(\varphi_1) \ast \Sigma(\varphi_2).
\]

Thus by the isomorphism \( \lambda : L^2(G^* \times G) \cong L^2(G \times G) \), \( \Sigma \) induces a unitary transformation on \( L^2(G \times G) \), also denoted by \( \Sigma \) and it preserves \( \ast \). Then by (10.4.5.7), there is a unitary map \( \omega : L^2(G) \rightarrow L^2(G) \) that

\[
\Sigma(P \otimes Q) = \omega^{-1}(P) \otimes \omega^{-1}Q.
\]

Next, notice for any \( (w, t) \in A(G) \),

\[
\lambda^{-1}(P \otimes Q)(w) = \int_G P(u)\overline{Q(u + v)}\langle u, v^* \rangle dw = (P, \rho(w, t)Q)_{L^2},
\]

thus

\[
(P, \rho(\sigma(w, t)))_{L^2} = (P, \rho(s(w), f(t))Q)_{L^2} = \overline{\lambda(f(w))(P \otimes \overline{Q})}(s(w))
\]

\[
= \overline{\lambda}(\Sigma^{-1}(P \otimes \overline{Q}))(w) = \overline{\lambda}^{-1}(\omega^{-1}(P) \otimes \omega^{-1}(Q))(w)
\]

\[
= \langle \omega^{-1}(P), \rho(w, t)\omega^{-1}(Q) \rangle_{L^2}
\]

\[
= ((P), \omega\rho(w, t)\omega^{-1}(Q))_{L^2}
\]

Because \( P, Q \) are arbitrary, this means \( \rho(\sigma(w, t)) = \omega(\sigma) \circ \rho(w, t) \circ \omega(\sigma)^{-1} \).

It remains to show that \( \rho \) is irreducible: For any endomorphism of \( L^2(G) \) commuting with \( \rho \), it commutes with \( \rho(\varphi) \) for any \( \varphi \in L^2(G^* \times G) \). Take \( \varphi = \lambda^{-1}(P \otimes \overline{Q}) \), where \( P, Q \in L^2(G) \), then

\[
\rho(\varphi)\Phi = (\Phi, Q)_{L^2}P, \text{ so } (T\Phi, Q)_{L^2}P = (\Phi, Q)_{L^2}TP. \text{ Then } T \text{ is a scalar.} \]
Pontryagin Duality

**Prop. (10.9.3.23) [Pontryagin Duality]**. For a locally compact Abelian group $G$, $G \rightarrow (\hat{G})^\wedge$ is an isomorphism of topological groups.

**Proof**: Cf.[Folland Abstract Harmonic Analysis P110].

**Cor. (10.9.3.24) [Fourier Inversion Theorem]**. If $f \in L^1(G)$ and $\hat{f} \in L^1(\hat{G})$ and the measure are dual to each other(10.9.3.14), then $f(x) = \hat{f}(x^{-1})$, i.e. $f(x) = f(x, \xi)\hat{f}(\xi)d\xi$ a.e..

**Proof**: As

$$\hat{f}(\xi) = \int (x, \xi)f(x)dx = \int (x^{-1}, \xi)f(x)dx = \int (x, \xi)f(x^{-1})dx,$$

so by definition $\hat{f} \in B^1(\hat{G})$, and $d\mu\hat{f}(x) = f(x^{-1})dx$. Then by(10.9.3.14), $f(x^{-1}) = (f^\wedge)^\wedge(x)$. □

**Cor. (10.9.3.25) [Fourier Uniqueness Theorem]**. If $u, v \in M(G)$ satisfy $\hat{u} = \hat{v}$, then $u = v$. In particular, if $f, g \in L^1(G)$ and $\hat{f} = \hat{g}$, then $f = g$.

**Proof**: By(10.9.3.9)(norm decreasing), $\mu$ is uniquely determined by $\varphi_\mu(\xi) = \hat{\mu}(\xi^{-1})$ by Fourier inversion. □

**Lemma (10.9.3.26)**. If $\varphi, \psi \in C_0(\hat{G})$, then $\varphi * \psi = \hat{h}$ where $h \in B^1(G)$. In particular, $\mathcal{F}(B^1(G))$ is dense in $L^p(\hat{G})$ for $p < \infty$.

**Proof**: Cf.[Folland, P109].

**Prop. (10.9.3.27) [Duality of Subgroups]**. $(H^\perp)^\perp = H$ for closed subgroup $H$ of a locally compact Abelian group $G$.

**Proof**: Suffices to prove $(H^\perp)^\perp \subset H$. If $x_0 \notin H$, then Gelfand-Raikov shows that there is a character $\eta$ on $G/H$ that $\eta(q(x_0)) \neq 1$, so $x_0 \notin (H^\perp)^\perp$. □

**Prop. (10.9.3.28) [Duality of Subgroups]**. $(H^\perp)^\perp = H$ for closed subgroup $H$ of a locally compact Abelian group $G$.

**Proof**: Suffices to prove $(H^\perp)^\perp \subset H$. If $x_0 \notin H$, then Gelfand-Raikov shows that there is a character $\eta$ on $G/H$ that $\eta(q(x_0)) \neq 1$, so $x_0 \notin (H^\perp)^\perp$. □

**Prop. (10.9.3.29) If $H$ is a closed subgroup of $G$, then there are natural isomorphisms of LCA groups: $\Phi : (G/H) \cong H^\perp$, $\Psi : \hat{G}/H^\perp \cong \hat{H}$.

**Proof**: $\Phi$ is clearly algebraic isomorphism. If $|\eta(q(K)) - 1| < \varepsilon$, then $|\eta(K) - 1| < \varepsilon$, so $\Phi$ is continuous in the compact-open topology. Similarly, to show $\Phi$ is open, it suffices to show a compact subset of $G/H$ has a compact inverse image in $G$, but this is just(10.9.1.34).

Now for $\Psi$, notice $\hat{G}/H^\perp \cong (H^\perp)^\perp \cong H$ by(10.9.3.28), so by Pontryagin duality theorem, $\hat{G}/H^\perp \cong \hat{H}$. □

**Cor. (10.9.3.30) [Hahn-Banach for LCA Groups]**. By the surjectivity of $\Psi$, any character of $\hat{H}$ extends to a character of $G$.

**Prop. (10.9.3.31) [Poisson Summation Formula]**. Suppose $H$ is a closed subgroup of $G$, if $f \in L^1(G)$, define $F(xH) = \int_H f(xy)dy$ on $G/H$, then $F \in L^1(G/H)$ by(10.9.1.38), then:
Prop.(10.9.3.35) [Self Duality of Topological Fields].

- \( \hat{F} = \hat{f}\big|_{H^\perp} \), where \( G/H \) is identified with \( H^\perp \) by (10.9.3.29).
- If \( \hat{f}\big|_{H^\perp} \in L^1(H^\perp) \), then with the dual measure of \( G/H \) on \( H^\perp \) (10.9.3.14), we have
  \[
  \int_H f(x)ydy = \int_{H^\perp} \hat{f}(\xi)\langle x,\xi\rangle d\xi.
  \]
  In particular, take \( x = e \), then
  \[
  \int_H f(y)dy = \int_{H^\perp} \hat{f}(\xi)d\xi.
  \]

Proof: Notice for \( \xi \in H^\perp \),
\[
\hat{F}(\xi) = \int_{G/H} F(xH)(x,\xi)d(xH) = \int_{G/H} \int_H f(xy)(xy,\xi)dyd(xH) = \int_G f(x)(x,\xi)dx = \hat{f}(\xi)
\]
by (10.9.1.38). And 2 is just (10.9.3.24) applied to \( F(xH) \) on \( G/H \).

Cor. (10.9.3.32). In the situation of (10.9.3.31), if \( H \) is discrete in \( G \) and \( G/H \) is compact, then both \( H, H^\perp \) are discrete, then by considering the dual measure using (10.9.3.16), the Poisson summation reads:
\[
\sum_{H} f(x) = \frac{1}{\mu(G/H)} \sum_{H^\perp} \hat{f}(\xi)\langle x,\xi\rangle.
\]

Perfect Pairing

Def. (10.9.3.33) [Self-Adjoint Haar Measures]. If \( G \) is a locally compact Abelian group, and there is an isomorphism \( G \cong \hat{G} \), or a perfect bilinear pairing \( G \times G \to \mathbb{C}^* \), then by Fourier inversion (10.9.3.14), a Haar measure \( d\mu \) on \( G \) corresponds to a Haar measure \( d\alpha \) on \( \hat{G} \), but via the isomorphism, \( d\alpha \) corresponds to a measure \( \tilde{d}\alpha \) on \( G \). Now anyway, there is a unique \( d\mu \) that \( d\mu = \tilde{d}\alpha \), and this is called the self-dual Haar measure on \( G \).

Via this pairing, we define the Fourier transform as an isomorphism
\[
L^2(G) \cong L^2(G) : \Phi(f)(x) = \int_G f(y)(x,y) d\mu(y).
\]
Then \( d\mu \) is a self-dual measure is equivalent to \( \Phi(\Phi(f))(x) = f(-x) \), or equivalently \( f(y) = \int_G \hat{f}(y)(x,y) d\mu(y) \).

Prop. (10.9.3.34). If \( G \) is a locally compact Abelian group, and there is a perfect bilinear pairing \( G \times G \to \mathbb{C}^* \) and \( \sigma : G \to G \) is a group automorphism of \( G \) that preserves this pairing, then \( \sigma \) preserves the Haar measure on \( G \).

Proof: It is clear that \( \sigma^*d\mu = |\sigma|d\mu \) for some real constant \(|\sigma| > 1 \). Consider the Fourier transform w.r.t. this pairing: \( F\varphi(x) = \int_G \varphi(y)(x,y)dy \), then \( F(\varphi \circ \sigma) = |\sigma|^{-1} F(x) \). But \( F \) is an isomorphism \( L^2(G) \cong L^2(G) \), so \(|\sigma|^{-1} = |\sigma| \), thus \(|\sigma| = 1 \). \( \square \)

Prop. (10.9.3.35) [Self Duality of Topological Fields]. Let \( K \) be a locally compact topological field. If \( X \) is a non-trivial character on the additive group \( K^+ \), then for any \( \eta \in K^+ \), \( \xi \mapsto X(\eta\xi) \) is also a character, and
\[
F_X : \eta \mapsto (\xi \mapsto X(\eta\xi))
\]
is an isomorphism of topological groups of \( K^+ \) and \( \hat{K^+} \).

Then by (10.9.3.33), we find a self-dual measure Haar measure \( dx \) on \( K^+ \) w.r.t. \( X \).

In fact, such a character \( X \) does exist, by Gelfand-Raikov (10.9.2.22).
10.9. ANALYSIS ON LOCALLY COMPACT GROUPS

Proof: First this is clearly a homomorphism of groups, and it is injective, because if $X(\eta \xi) = 1$ for all $\xi$, then $\eta K^+ \neq K^+$ (because $X$ is nontrivial), so $\eta = 0$.

Now the image of $F$ is dense, because if $X(\eta \xi) = 1$ for all $\eta$, then $\xi = 0$, so $\text{Im}(\eta K) = 1$. Now $(H^+)^\perp = H$ for $H$ closed (10.9.3.28) and use Pontryagin duality (10.9.3.23), so $\text{Im} f$ is dense in $\hat{G}$.

Now $F$ is open and continuous, because: for any $B \in G$ compact, there is a nbhd $V$ of 0 that $|X(V) - 1| < \varepsilon$, so there is a nbhd $V'$ that $V'B \subset V$, so if $\eta \in V$, $|X(\eta B) - 1| < \varepsilon$, so $F$ is continuous ($\hat{K}^+$ has the compact-open topology). And if we choose $\xi_0$ that $X(\xi_0) \neq 1$, then choose $B = B(0, \frac{\xi_0}{\varepsilon})$ compact, if $|X(\eta B) - 1| < |X(\xi_0) - 1|$, then $\xi_0 \notin \eta B$, which means that $|\eta| < \varepsilon$. This means $F(B(0, \varepsilon))$ contains $V(B, |X(\xi_0) - 1|)$, so $F$ is open.

So the image of $F$ is a locally compact subgroup of $\hat{G}$, so by (10.9.1.7) it is closed, hence equals $G$ as it is dense, so $F$ is surjective, and is an isomorphism.

4 Compact Group

Cf. [群表示论 notes] and [Fol15] Chap5.

In this subsection, we consider representations of a compact group over $\mathbb{C}$.

Unitary Representations

Prop. (10.9.4.1) [F.d. Representation is Unitary]. If $V$ is a real/complex f.d. representation $\pi$ of a compact group $G$, then there is an inner product on $V$ that the action of $G$ is orthogonal/unitary.

Proof: Choose an arbitrary inner product $(\cdot, \cdot)_0$ on $V$, then consider

$$(u, v) = \int_G (\pi(x)u, \pi(x)v)_0 dx.$$ 

where $dx$ is a Haar measure on $G$. Then

$$(\pi(y)u, \pi(y)v) = \int_G (\pi(xy)u, \pi(xy)v)_0 dx = \Delta(y) \int_G (\pi(x)u, \pi(x)v) dx = \int_G (\pi(x)u, \pi(x)v)_0 dx$$

because $G$ is compact hence unimodular (10.9.1.18). Thus this is an inner product on $V$ that is invariant under $G$. 

Cor. (10.9.4.2) [F.D. Representation of Compact Groups Totally Decomposable]. Any f.d. representation of a compact group is totally decomposable.

Proof: This is because we can assume this representation is unitary by (10.9.4.1), and then for any subrepresentation we can take the orthogonal complement.

Lemma (10.9.4.3). Suppose $(\pi, \mathcal{H})$ is a continuous unitary representation of the compact group $G$, let $u \neq 0 \in \mathcal{H}$ be a unit vector, if the operator $T$ on $\mathcal{H}$ is defined by

$$Tv = \int_G (v, \pi(x)u)\pi(x)udx,$$

then $T$ is a positive, non-zero compact operator in $C(\pi)$. 

\begin{proof}
\((Tv, v) = \int_G (v, \pi(u)) (\pi(x) u, v) dx = \int_G |(\pi(x) u, v)|^2 dx \geq 0,
\)
so it is positive. Moreover, if \(v = u\), then \(x \mapsto |(\pi(x) u, v)|\) is a positive on a nbhd of 1, so \(T \neq 0\).

Finally, because \(G\) is compact, \(x \mapsto \pi(x) u\) is uniformly continuous, so for any \(\varepsilon > 0\), there is a disjoint partition \(E_i\) of \(G\) and \(x_i \in E_i\) that if \(x^\prime \in E_i\), then \(||\pi(x) - \pi(x') u|| \leq \varepsilon/2\). Then

\[||(v, \pi(x) u) \pi(x') u - (v, \pi(x_i) u) \pi(x_i) u|| \leq ||(v, [\pi(x) - \pi(x_i)] u) \pi(x) u|| + ||(v, \pi(x_i) u) [\pi(x) - \pi(x_i)] u|| < \varepsilon ||v||.\]

So consider

\[T_\varepsilon (v) = \sum |E_j| (v, \pi(x_j) u) \pi(x_j) u = \sum \int_{E_i} (v, \pi(x_j) u) \pi(x) u dx\]

then \(||T - T_\varepsilon|| < \varepsilon\), and \(T_\varepsilon\) has f.d image, thus \(T\) is compact, by (10.7.5.3).

Also \(T \in C(\pi)\) because

\[
\pi(y)Tv = \int_G (v, \pi(x) u) \pi(yx) dx = \int_G (v, \pi(y^{-1} x) u) \pi(x) dx = \int_G (\pi(y)v, \pi(x) u) \pi(x) dx = T\pi(y)v.
\]

\end{proof}

Prop. (10.9.4.4) [Unitary Representations of Compact Groups]. If \(G\) is compact group, then every unitary representation \((\rho, V)\) of \(G\) is an orthogonal sum of irreducible unitary subrepresentations. Moreover, the isotopic part \(V^\pi\) for any irreducible representation \(\pi\) of \(G\) is uniquely determined. And very irreducible representation of \(G\) is of f.d. (thus unitary by (10.9.4.1)).

\begin{proof}
By taking orthogonal complements and Zorn’s lemma, it suffices to show any unitary representation \(\pi\) has an irreducible subrepresentation. Choose \(T\) as in (10.9.4.3), then \(T\) is compact nonzero self-adjoint, so by Riesz-Fredholm (10.7.5.9) it has a finite-dimensional eigenspace, which is \(\pi\)-invariant, and it clearly has an irreducible subrepresentation by taking orthogonal complements.

For the orthogonality, Let \(V^\pi\) be the linear span of invariant subspaces isomorphic to \(\pi\), for \(L_1, L_2\) of type \(\pi_1 \neq \pi_2\), then consider the orthogonal projection \(P\) onto \(L_2\), then \(P|_{L_1} \in C(\pi_1, \pi_2)\), which vanishes by Schur (10.9.2.4), so they are orthogonal.

The final assertion follows from (10.9.4.19). \qed \end{proof}

Cor. (10.9.4.5). The cardinality of irreducible constituents of \(V\) that is isomorphic to \(\pi\) is independent of the decomposition, and it is equal to \(\dim \text{Hom}_G(\pi, \rho)\), and is denoted by \(\text{mult}(\pi, \rho)\).

\begin{proof}
Cf. [Folland, P137]. \qed \end{proof}

Cor. (10.9.4.6). Let \(G\) be a compact subgroup and \(H\) a closed subgroup, then \(G\) acts unitarily on \(L^2(G/H)\), and it decomposes as

\[L^2(G/H) \cong \bigoplus_{\pi \in \hat{G}} \text{Hom}_H(\pi, \rho)\]

where \(\text{Hom}_H(\pi) = \text{dim} \pi^H\) the dimension of \(H\)-fixed vectors in \(V\).

\begin{proof}
By (10.9.4.4), it suffices to determine the multiplicity of \(\pi\) in \(L^1(G/H)\), which is just dimension of \(\text{Hom}_G(\pi, L^2(G/H))\), which can be viewed as \(G\)-invariant \(L^2\) functions on \(G/H\) with values on \(\pi^*\). For any such function \(f\), \(f(1)\) is \(H\)-invariant, and for any \(H\)-invariant vector \(v\), \(g \mapsto gv\) is continuous, thus is \(L^2\). So the dimension of this space is just \(\text{dim} \pi^H\). \qed \end{proof}
Matrix Coefficients and Peter-Weyl Theorem

**Def. (10.9.4.7) [K-Finite Vectors].** Let $K$ be compact group. For an irreducible representation $\rho$ of $K$, denote $V^\rho = \rho \otimes \text{Hom}_K(\rho, V)$ the $\rho$-isotypic component in $V$. And let $V^{K-\text{fin}} = \bigoplus_{\rho} V^\rho$ the space of $K$-finite vectors in $V$.(10.9.4.4).

**Def. (10.9.4.8) [Matrix Coefficients].** Firstly $C(G)$ is a representation of $G \times G$ by $((g_1, g_2)f)(g) = f(g_1^{-1}g_2)$. For a f.d. representation $(\pi, V)$ of a topological group $G$, we can view $\text{End}(V)$ as a representation of $G \times G$ via

$$(g_1, g_2)S = \pi(g_1)S\pi(g_2^{-1})$$

There is a matrix coefficient map:

$$MC_V : \text{End}(V) \rightarrow C(G), \quad MC_V(S)(g) = MC_{S,V}(g) = \text{tr}(S\pi(g^{-1})|V)$$

is a map of $K \times K$-representations. And denote $\mathcal{E}_\pi$ the image of of $MC_V$, and let $L^2_{\text{alg}}(G) = \bigoplus_{\pi \in \hat{G}} \mathcal{E}_\pi$.

**Prop. (10.9.4.9) [Schur Orthogonality Conditions].** Let $(\pi_1, V_1), (\pi_2, V_2)$ be f.d. continuous irreducible representations of $K$, then

$$\int_K MC_{S_1,V_1}(k)MC_{S_2,V_2}(k) = 0$$

unless $V_2 \cong V_1^*$, in which case

$$\int_K MC_{S_1,V}(k)MC_{S_2,V^*}(k) = \frac{1}{\dim V} \text{tr}(S_1 \circ S_2^*)|V).$$

In particular, $\mathcal{E}_\pi$ is orthogonal to $\mathcal{E}_{\pi'}$ for $[\pi] \neq [\pi']$, and if $\{e_i\}$ is any orthonormal basis of $V$, $\sqrt{d_\pi} \pi_{ij}$ is an orthonormal basis of $\mathcal{E}_\pi$, and $\mathcal{E}_\pi$ is isomorphic to $\text{End}(V)$ as $K \times K$-representations.

**Proof:** Cf.[Gaitsgory P3].

**Cor. (10.9.4.10).** $MC_{S,V}(k^{-1}) = MC_{S^*,V^*}(k)$.

**Prop. (10.9.4.11).** $\mathcal{E}_\pi$ is invariant under left and right translations of $G$, and it is a two-sided ideal in $L^1(G)$.

**Proof:** It can be shown that $f \star \varphi_{u,v} = \varphi_{u,\pi(\hat{T})v}$, and $\varphi_{u,v} \star f = \varphi_{\pi(\hat{f})u,v}$, where $\hat{f}(x) = f(x^{-1})$.

**Prop. (10.9.4.12).** If $\rho$ is an irreducible f.d representation of $K$ and $V$ is a continuous representation of $K$, then for any $S \in \text{End}(\rho^*)$, the image of

$$MC_{S,\rho^*\mu_{\text{Haar}}} \in M(K)$$

acting on $V$(10.7.3.24) belongs to $V^\rho$.

**Proof:** Cf.[Gaitsgory P7].

**Cor. (10.9.4.13).** For an irreducible representation $\rho$ of $K$, the element $\xi_{\rho^*\mu_{\text{Haar}}} \in \text{Meas}(K)$ acts in any continuous representation $V$ as a projection with image equal to $V^\rho$.

**Proof:** Directly from the proposition and(10.9.4.26).
Prop. (10.9.4.14). $\mathcal{E}$ is an algebra, Cf.[Folland, P141]. It is dense in $C(K)$, and dense in $L^p(K)$ for $p < \infty$.

Proof: 

Prop. (10.9.4.15)[Peter-Weyl]. For a compact group $K$,

- $\otimes_{\pi \in G} \mathcal{E}_\pi = L^2(K)$, where $\mathcal{E}_\pi \cong \text{End}(V_\pi)$.

- $L^2_{\text{alg}}(K) = \otimes_{\pi \in G} \mathcal{E}_\pi$ identifies with the $K$-finite vectors in $L^2(K)$ w.r.t. the left translation.

Proof: 1: By (10.9.4.4), the multiplicity of $\pi$ in $L^2(K)$ is just $\dim \pi$, and this is just the multiplicity of $\pi$ in $E_\pi$ by (10.9.4.9), so this is an isomorphism.

2: Clearly every vector in $\otimes_{\pi \in G} \mathcal{E}_\pi$ is $K$-finite. Conversely, if some vector $v$ is $K$-finite, then it generates a finite vector space $V$ under the left translation action of $G$. Now the linear function $f \mapsto f(1)$ restricts to a linear function $l$ on $V$, and then $l(L^*_g v) = v(g)$, so $v$ is a matrix coefficient of $V$, so $v \in L^2_{\text{alg}}(K)$.

\[\square\]

Cor. (10.9.4.16)[Representations of Product Groups]. Any irreducible representation of the product group $G \times H$ for $G, H$ is of the form $\rho \boxtimes \psi$ where $\rho$ and $\psi$ are irreducible representations of $G, H$ resp.

Proof: By orthogonality of characters (10.9.4.22), there representations are irreducible and different. They are all the representations because they already form a basis in $L^2(G \times H)$.

\[\square\]

Prop. (10.9.4.17). For any continuous representation $K$, the subset $V^{K-fin}$ is dense in $V$.

Proof: For any $v \in V$, choose a Dirac sequence $f_n$, then $\pi(f_n)v \to v$. Then by Peter-Weyl (10.9.4.15), we can choose $K$-finite functions $g_n$ that $\|g_n - f_n\|_{L^2} < \frac{1}{n}$. Then $g_n$ also converges to $\delta_1$ in the weak topology. Thus $\pi(g_n)v \to v$ and (10.9.4.12) shows $\pi(g_n)v \in V^{K-fin}$.

\[\square\]

Cor. (10.9.4.18). Matrix coefficients of f.d. representations are dense in $C(K)$. (Immediate from the proposition and Peter-Weyl theorem (10.9.4.15)).

Cor. (10.9.4.19). Every irreducible continuous representation of a compact group is of f.d.

Proof: This is because $V^{K-fin}$ is a sub-representation of $V$ and it is dense in $V$, thus $V = V^{K-fin}$ is of f.d. because it is irreducible.

\[\square\]

Fourier Analysis on Compact Groups

Def. (10.9.4.20)[Characters]. Let $V$ is a f.d. continuous representation of $K$, let $\chi_V = MC_V(\text{Id}_V) = \text{tr}(g|V)$, called the character of $V$, and if $V$ is irreducible, define $\xi_V = \text{dim} V \cdot \chi_V$.

This definition of character is compatible the abstract definition viewed as a representation of the group algebra $C[G]$.

Prop. (10.9.4.21). If we take an invariant inner product on $V$, and $e_i$ an orthonormal basis, then

$$\chi_V(g) = \sum_i (ge_i, e_i),$$

and

$$\chi_V^\ast(g) = \chi_V(g^{-1}) = \overline{\chi_V(g)}, \quad \chi_V \oplus W = \chi_V + \chi_W, \quad \chi_V \otimes W = \chi_V \cdot \chi_W$$
Cor. (10.9.4.22) [Orthogonality of Characters]. Let $V, W$ be irreducible, then

$$
\int_K \chi_V(k)\chi_W(k^{-1}) = \int_K \chi_V(k)\overline{\chi_W(k)} = \int_K \chi_V(k)\overline{\chi_W(k)}
$$

so by (10.9.4.9) this equals 1 if $V \cong W$ and 0 otherwise.

Prop. (10.9.4.23). Let $\chi$ be a character of a representation of compact group $K$ of dimension $n$, then

- $\chi(1) = n$.
- $\chi(s^{-1}) = \chi(s)^*$. 
- $\chi(tst^{-1}) = \chi(s)$.

Proof: Notice the eigenvalues of $\rho(g)$ all have absolute value 1, because this representation is unitarizable (10.9.4.1) thus $\rho^*(g) = \rho(g)^*$. □

Prop. (10.9.4.24) [Fourier Transform on Compact Groups]. Let $K$ be a compact group and $f \in L^2(K)$, then by Peter-Weyl (10.9.4.15) and (10.9.4.9),

$$
f = \sum_{\pi \in \hat{G}} \sum_{i,j=1}^{d_\pi} c_{ij}^\pi \pi_{ij}, \quad c_{ij}^\pi = d_\pi \int_G f(x)\overline{\pi_{ij}(x)}dx.
$$

So

$$
f(x) = \sum_{\pi \in \hat{G}} \sum_{i,j=1}^{d_\pi} d_\pi \int_G f(y)\overline{\pi_{ij}(y)}\pi_{ij}(x)dx = \sum_{\pi \in \hat{G}} d_\pi f(y)\text{tr}(\pi(y^{-1}x)) = \sum_{\pi \in \hat{G}} d_\pi (f \ast \chi_\pi)(y).
$$

Thus

$$
f = \sum_{\pi \in \hat{G}} d_\pi f \ast \chi_\pi
$$

and $d_\pi f \ast \chi_\pi$ are the projection of $f$ onto $E_\pi$ (10.9.4.9).

Cor. (10.9.4.25). $\xi_V \ast \xi_W = 0$ unless $W \cong V$ and $\xi_V \ast \xi_V = \xi_V$ (10.9.4.20).

Cor. (10.9.4.26). For continuous irreducible representations $V, W$ of $K$, $\pi(\xi_V) \in \text{End} W$ equals $\text{Id}_W$ if $W \cong V$ and zero otherwise.

Def. (10.9.4.27) [Class Functions]. A measurable function on $G$ is called a **class function** iff $f(y^{-1}xy) = f(x)$ a.e. $(x, y) \in G \times G$. Denote $ZL^p(G)$ the space of class functions in $L^p(G)$ and $ZC(G)$ the space of continuous functions on $G$.

Prop. (10.9.4.28). For a compact group $K$ and $1 \leq p < \infty$, the spaces $L^p(K)$ and $C(K)$ are Banach algebras under convolution (10.9.1.26), and $ZL^p(K)$ and $ZC(K)$ are their centers.

Proof: By (10.9.1.29), $\|f \ast g\|_p \leq \|f\|_1\|g\|_p \leq \|f\|_p\|g\|_p$, for $1 \leq p \leq \infty$, thus $L^p(G)$ and $C(K)$ are Banach algebras.

For $f \in L^p(K)$, $f \ast g = g \ast f$ iff

$$
\int_K f(xy)g(y^{-1})dy = \int_K g(y)f(y^{-1}x)dy = \int_K f(yx)g(y^{-1})dy, \quad \text{a.e.} x
$$

for any $g \in L^p(K)$, which is equivalent to $f(xy) = f(yx)$ a.e. $x, y$. Similarly for $f \in C(K)$. □
Lemma (10.9.4.29). If \( f \in ZL^1(K) \) and \( \pi \in \hat{K} \), then \( d_\pi f \ast \chi_\pi = \int_K (f \chi_\pi) \chi_\pi \).

**Proof:** For \( x \in G \),
\[
\pi(f)\pi(x) = \int_K f(y)\pi(xy)\,dy = \int_K f(xy^{-1})\pi(y)\,dy = \int_K f(x^{-1}y)\pi(y)\,dy = \int_K f(y)\pi(xy)\,dy = \pi(x)\pi(f)
\]
so \( \pi(f) \) is a scalar by Schur’s lemma (10.9.2.4). Notice \( f'(g) = f(g^{-1}) \in ZL^1(K) \) also, so
\[
d_\pi[f \ast \chi_\pi](x) = d_\pi \int_K f(y^{-1})(\tr \pi)(yx)\,dy = d_\pi \tr(\int_K f(y^{-1})\pi(yx)\,dy) = \tr(\pi(f'))\tr(\pi(x))
\]
and \( \tr(\pi(f')) = \int_K f(y^{-1})\tr(\chi(y))\,dy = \int_K f\chi_\pi \). □

Prop. (10.9.4.30) [Characters Orthonormal Basis]. \( \{\chi_\pi | \pi \in \hat{K}\} \) is an orthogonal basis for \( ZL^2(K) \).

**Proof:** \( \chi_\pi \in ZC(K) \subset ZL^2(K) \) by (10.9.4.23), and they are orthonormal by (10.9.4.22). They are a basis by (10.9.4.29).

Prop. (10.9.4.31). The linear spans of \( \{\chi_\pi | \pi \in \hat{K}\} \) is dense in \( ZC(K) \) and \( ZL^p(K) \) for \( 1 \leq p < \infty \).

**Proof:** Cf. [Fol15] P148.

Prop. (10.9.4.32) [Real Type]. Let \( G \) be a topological group and \( V \) is a complex representation, then the following are equivalent:

- \( V = U \otimes_R \mathbb{C} \) is a complexification of a real representation \( U \) of \( G \).
- \( V \) admits a \( G \)-invariant anti-linear endormorphism \( S \) that \( S^2 = 1 \).
- There is a \( G \)-invariant symmetric form \( B \) on \( V \) inducing an isomorphism \( V \cong V^* \).

**Proof:**
1 \( \iff \) 2 is clear.

2 \( \rightarrow \) 3: By averaging there is a \( G \)-invariant Hermitian form \( h \) on \( V \), then we can define \( B(u,v) = h(u,Sv) \). As \( h(u,v) = h(Sv,Su) \) is also a \( G \)-invariant Hermitian form, \( h(Sv,Su) = \pm h(u,v) \), so \( B(v,u) = B(u,v) \).

3 \( \rightarrow \) 1: \( h \) induces a \( G \)-isomorphism \( \varphi_h : V \cong V^* \). Then \( \sigma = \varphi_h \circ \varphi_B \) is a \( G \)-isomorphism \( V \rightarrow V \). Then \( \sigma \circ \sigma : V \rightarrow V \) is a \( G \)-isomorphism, thus by Schur’s lemma \( \sigma \circ \sigma = \lambda \) for some \( \lambda \in \mathbb{C} \). More explicitly, \( B(v,u) = H(v,\sigma(u)) \) for any \( u,v \in V \). Because \( B \) is symmetric or symplectic, \( B(u,v) = \pm B(v,u) \), thus \( H(v,\sigma(u)) = \pm H(u,\sigma(v)) \), and
\[
\lambda H(v,u) = H(v,\sigma^2(u)) = \pm H(\sigma(u),\sigma(v)) = \pm H(\sigma(v),\sigma(u)) = H(u,\sigma^2(v)) = \lambda H(v,u).
\]

Thus \( \lambda \) is real. And then we can normalize \( \sigma \) so that \( \sigma = \pm 1 \). If \( \sigma^2 = 1 \), then consider \( V_0 = \ker(\sigma - 1) \), then \( iV_0 = \ker(\sigma + 1) \), and \( V_0 \oplus iV_0 = V \). If \( \sigma^2 = -1 \), then consider the action of \( \mathbb{H} \) on \( V \) given by \( (\alpha + \beta j)(v) = \alpha v + \beta \sigma(v) \). It is an action because \( \sigma \) is anti-linear and \( \sigma^2 = -1 \). □

Prop. (10.9.4.33) [Quaternion Type]. Let \( G \) be a topological group and \( V \) is a complex representation, then the following are equivalent:

- \( V = W_\mathbb{C} \) is a restriction of a quaternionic representation \( W \) of \( G \).
- \( V \) admits a \( G \)-invariant anti-linear endormorphism \( S \) that \( S^2 = -1 \).
- There is a \( G \)-invariant alternating form \( B \) on \( V \) inducing an isomorphism \( V \cong V^* \).
10.9. ANALYSIS ON LOCALLY COMPACT GROUPS

\textbf{Proof: } 1 \iff 2 \text{ is clear. The proof of } 2 \rightarrow 3 \rightarrow 1 \text{ is the same as the proof of (10.9.4.32).} \hfill \Box

\textbf{Proposition (10.9.4.34).} An irreducible complex representation \( V \) of \( G \), then \( V \) is of real/complex/quaternionic type iff \( \text{End}_{\mathbb{R}[G]}(V) \cong M_2(\mathbb{R})/C/H \)

\textbf{Proof: } By (10.9.4.32), if \( V \) is of real type, then \( V \cong U \otimes_{\mathbb{R}} \mathbb{C} \cong V \oplus V \), then \( \text{End}_{\mathbb{R}[G]}(V) \cong M_2(\mathbb{R}) \).

By (10.9.4.33), if \( V \) is of quaternionic type, then it is a restriction of a quaternionic representation, so \( H \subset \text{End}_{\mathbb{R}[G]}(V) \). And for any \( \mathbb{R} \)-linear endomorphism \( f \) of \( V \), \( f = \frac{f + if_0}{2} + \frac{f - if_0}{2} \) is a sum of \( \mathbb{C} \)-linear and anti-linear endomorphisms of \( V \). For an anti-linear endomorphism \( g \), \( gj \) is \( \mathbb{C} \)-linear, thus \( f \in H \).

If \( V \) is of complex type, then there are no invariant anti-linear endomorphisms, thus \( f = \frac{f + if_0}{2} + \frac{f - if_0}{2} \) is \( \mathbb{C} \)-linear, so \( \text{End}_{\mathbb{R}[G]}(V) \cong \mathbb{C} \).

\textbf{Proposition (10.9.4.35) [Types of Representations].} Let \( V \) be a finite-dimensional irreducible \( \mathbb{C} \)-representation of a compact group \( G \). Let \( dg \) be the Haar measure on \( G \) with \( \int_G dg = 1 \), then:

\[ \int_G \chi(g^2)dg = \begin{cases} 1 & \text{iff } V \text{ is of real type} \\ 0 & \text{iff } V \text{ is of complex type} \\ -1 & \text{iff } V \text{ is of quaternionic type} \end{cases} \]

\textbf{Proof: } Notice that \( \chi(g^2) = \chi_{\text{Sym}^2(V)}(g) - \chi_{\wedge^2(V)}(g) \), so \( \int_G \chi(g^2)dg = \dim \text{Sym}^2(V)^G - \dim \wedge^2(V)^G \). Then it is clear by (15.1.1.5). \hfill \Box

5 Induced Representation

\textbf{Lemma (10.9.5.1).} If \( H \) is a closed subgroup of a locally compact subgroup \( G \), \( q : G \rightarrow G/H \), for any unitary representation \( (\sigma, \mathcal{H}) \) of \( H \), let \( \mathcal{F}_0 \) be the space of continuous functions \( f : G \rightarrow \mathcal{H} \) that \( q(\text{Supp}(f)) \) is compact, and

\[ f(x\xi) = \sqrt{\frac{\Delta_H(\xi)}{\Delta_G(\xi)}} \sigma(\xi^{-1})f(x). \]

Then if \( \alpha : G \rightarrow \mathcal{H} \) is continuous with compact support, then

\[ f_\alpha(x) = \int_H \sqrt{\frac{\Delta_G(\eta)}{\Delta_H(\eta)}} \sigma(\eta)\alpha(x\eta)d\eta \in \mathcal{F}_0 \]

and is left uniformly continuous w.r.t \( G \). Moreover, every element in \( \mathcal{F}_0 \) arises in this way.

\textbf{Proof: } Clearly \( q(\text{Supp } f_\alpha) \subset q(\text{Supp } \alpha) \), and

\[ f_\alpha(x\xi) = \int_H \sqrt{\frac{\Delta_G(\eta)}{\Delta_H(\eta)}} \sigma(\eta)\alpha(x\xi)d\eta = \int_H \sqrt{\frac{\Delta_G(\xi^{-1})}{\Delta_H(\xi^{-1})}} \sigma(\xi^{-1})\alpha(x\eta)d\eta = \sqrt{\frac{\Delta_H(\xi)}{\Delta_G(\xi)}} \sigma(\xi^{-1})f_\alpha(x). \]

For left uniformly continuity, Cf. [Folland, P164].

For the surjectivity, if \( f \in \mathcal{F}_0 \), by (10.9.1.37), there exists \( \psi \in C_c(G) \) that \( \int_H \psi(x\eta)d\eta = 1 \) for \( x \in \text{Supp } f \). So we can let \( \alpha = \psi \cdot f \), then

\[ f_\alpha(x) = \int_H \sqrt{\frac{\Delta_G(\eta)}{\Delta_H(\eta)}} \psi(x\eta)\sigma(\eta)f(x\eta)d\eta = \int_H \psi(x\eta)f(x)d\eta = f(x) \]
Remark (10.9.5.2) [Left and Right Compatibility]. If we consider the right action, then it suffices to consider all the functions $g(x) = f(x^{-1})$. Then $g$ satisfies

$$g(\xi x) = \sqrt{\frac{\Delta_G(\xi)}{\Delta_H(\xi)}} \sigma(\xi) g(x).$$

Def. (10.9.5.3) [Induced Representations]. Let $(\sigma, V)$ be a unitary representation of $H$, for any $f, f' \in \text{ind}^G_H \rho$, consider the function $g \mapsto (f(g), f'(g))$, then it is a function on $S(G, H)(10.9.1.40)$, thus

$$(f, f') \mapsto \int_{H \setminus G} (f, f') d\nu_{H \setminus G}(g)$$

is a right $G$-invariant Hermitian inner product on $\text{ind}^G_H \rho$, thus $\text{ind}^G_H \rho$ is unitarizable, called the induced representation.

Prop. (10.9.5.4) [Induction and Restriction]. If $(\sigma, \mathcal{H})$ is a unitary representation of $H$ and $(\pi, \mathcal{H}')$ is a unitary representation of $G$, then $\text{ind}^G_H(\sigma \otimes \text{res}(\pi)) \cong \text{ind}^G_H(\sigma) \otimes \pi$.

Prop. (10.9.5.5) [Frobenius Reciprocity]. If $G$ is compact group and $H$ is a closed subgroup, $\pi$ is an irreducible unitary representation of $G$, $\rho$ is an irreducible unitary representation of $H$, then

$$C(\pi, \text{ind}^G_H(\rho)) = C(\pi|_H, \rho), \quad \text{mult}(\pi, \text{ind}^G_H(\rho)) = \text{mult}(\rho, \pi|_H).$$

Proof: It suffices to prove the first one, the second follows from (10.9.2.2) and (10.9.4.5).

$G/H$ admits a $G$-invariant measure as $\Delta_G = \Delta_H = 1$. For the rest, it is similar to that of (15.1.4.44), Cf. [Folland, P172].
10.10 Harmonic Analysis

Main reference are [Rudin, Functional Analysis]. Notice much should be rewritten in greater
generality of Abstract Harmonic Analysis 10.9.

1 Distributions

Def. (10.10.1.1) [Test Functions]. The space $D(\Omega)$ of test functions has the induced topology
coincides with that of $D(K)$, and any bounded subsets are in some $D(K)$, thus it is complete and
has Heine-Borel because $D(K)$ does.

The space of continuous linear functionals of $D(\Omega)$ is called the space of distributions $D'(\Omega)$.
It is equivalence to the restriction to every $D(K)$ is continuous, Cf.[Rudin P155]. The order of a
distribution $\Lambda$ is the minimal $N$ that $|\Lambda \varphi| \leq C_K ||\varphi||_N$ for every $\varphi \in D(K)$, it might be $\infty$.

Def. (10.10.1.2). The differentiation of a distribution $\Lambda$ is defined as $D^\alpha \Lambda(\varphi) = (-1)^{|\alpha|} \Lambda(D^\alpha \varphi)$.
The multiplication by a smooth function $f$ is defined by $f \Lambda(\varphi) = \Lambda(f \varphi)$.

Support of a Distribution

Def. (10.10.1.3). The support $\text{Supp}(\Lambda)$ of a distribution is the complement of the open sets $U$ that
$\Lambda(f) = 0$ for any $f$ with support in $U$.

If $\text{Supp}(\Lambda)$ is compact, then $\Lambda$ has finite order and $|\Lambda \varphi| \leq C ||\varphi||_N$ for some $N$, and $\Lambda$ extends
uniquely to a continuous linear functional on $C^\infty(\Omega)$.

Proof: This is because its support is compact so we can choose a smooth $\psi$ that = 1 on $\text{Supp} \varphi$
and has support in $W \subset \Omega$. Then by (10.10.1.1), there is a $C$ that $|\Lambda(\psi \varphi)| < C ||\psi \varphi||_N$, and Leibniz
rule will give us the result. □

Prop. (10.10.1.4). If the support of a $\Lambda$ is a pt $p$ (thus has finite order $m$), then it is a linear
combination of $D^\alpha \delta_p, |\alpha| \leq m$. (use approximate identity and show the kernel of $\Lambda$ is contained in
the kernel of $D^\alpha \delta_p$).

Proof: Cf.[Rudin P165]. □

Prop. (10.10.1.5). For any distribution $\Lambda$, there exist continuous functions $g_\alpha$ in $C^\infty(\Omega)$ that each
compact $K$ intersects support of f.m $g_\alpha$ and $\Lambda = \sum D^\alpha g_\alpha$. When $\Lambda$ has finite order, we can use
only f.m $g_\alpha$.

Proof: use partition of unity. Then for a compact $K$, find a compact-open $W$, then find a bump
function between $K \subset W$, thus reduce to the case of $D(W)$. For the rest, Cf.[Rudin P169]. □

Convolution on $\mathbb{R}^n$

Denote $D = D(\mathbb{R}^n), D' = D'(\mathbb{R}^n)$.

Def. (10.10.1.6). The translation of a distribution $u$ is defined as $(\tau_x u)(\varphi) = u(\tau_{-x} \varphi)$, where
$\tau_x \varphi(y) = \varphi(y - x)$.

The convolution of a test function with a distribution $u$ is defined as $(u * \varphi)(x) = u(\tau_x \varphi)$, where $\tilde{\varphi}(y) = \varphi(-y)$.
Prop. (10.10.1.7) [Special Case of (10.10.1.10)]. For $u \in D', \varphi \in D, \psi \in D$,
\begin{itemize}
  \item $\tau_x (u * \varphi) = (\tau_x u) * \varphi = u * (\tau_x \varphi)$.
  \item $u * \varphi \in C^\infty$ and $D^\alpha (u * \varphi) = (D^\alpha u) * \varphi = u * (D^\alpha \varphi)$.
  \item $u * (\varphi * \psi) = (u * \varphi) * \psi$.
\end{itemize}
If $u$ has compact support, then (10.10.1.3) shows that $u$ can extend to $C^\infty$, thus convolution is defined for $\varphi \in C^\infty$ and the first two formulae still hold, and when $\psi \in D$,
\[ u * \psi \in D, \quad u * (\varphi * \psi) = (u * \varphi) * \psi = (u * \psi) * \varphi \]

Proof: Cf. [Rudin P171], [Rudin P174]. \hfill \Box

Cor. (10.10.1.8). $L : \varphi \mapsto u * \varphi$ is a continuous linear map into $C^\infty$ that commutes with $\tau_x$. And any these map comes from a $u*$: let $u = (L \varphi)(0)$.

Proof: It is continuous because of of closed graph theorem (10.6.2.8), $\lim (u * \varphi_i)(x) = \lim u(\tau_x \varphi_i) = u(\tau_x \varphi)$. \hfill \Box

Cor. (10.10.1.9). When $u, v \in D'$ and one of them has compact support, then similar to (10.10.1.8), $L \varphi = u * (v * \varphi)$ is a continuous linear map that commutes with $\tau_x$, so there is a unique convolution distribution $u * v$ that $(u * v) * \varphi = u * (v * \varphi)$. This convolution is compatible with the previous one when $v \in D$.

Prop. (10.10.1.10) [Convolution of Distributions]. For $u, v, w \in D'$,
\begin{itemize}
  \item if one of $u, v$ has compact support, then $u * v = v * u$, and $\text{Supp}(u * v) \subset \text{Supp}(u) + \text{Supp}(v)$.
  \item if two of three of $u, v, w$ has compact support, then $(u * v) * w = u * (v * w)$.
  \item $D^\alpha u = (D^\alpha \delta) * u$.
  \item if one of $u, v$ has compact support, then $D^\alpha (u * v) = (D^\alpha u) * v = u * (D^\alpha v)$.
\end{itemize}

Proof: Cf. [Rudin P177]. \hfill \Box

Def. (10.10.1.11). A approximate identity here is a $h \in D$ that $h_k(x) = k^n h(kx)$. Then we will have $\lim \varphi * h_j = \varphi$ for $\varphi \in D$, $\lim u * h_j = u$ in $D'$.

2 Fourier Analysis on $\mathbb{R}^n$

Def. (10.10.2.1) [Notations]. We denote the normalized notation $\mathbb{R}^n$ as $dm = (2\pi)^{-n/2} dx$ and
\[ D_\alpha = \frac{1}{i^{|\alpha|}} D^\alpha = \frac{1}{i^{|\alpha|}} \frac{\partial}{\partial x^\alpha}, \]
which will simplify many notations compared to $D^\alpha$. The Fourier transform here of a function $f \in L^1(\mathbb{R}^n)$ is the function $\hat{f}$ that $\hat{f}(t) = \int_{\mathbb{R}^n} f e^{-ix \cdot t} dm_n = (f * e_t)(0)$.

See (10.10.2.12) for general Fourier transform.

Prop. (10.10.2.2). For $f \in L^1(\mathbb{R})$,
\[ \hat{\tau_x f} = e^{-ix} \hat{f}, \quad \hat{e_x f} = \tau_x \hat{f}, \quad \hat{f * g} = \hat{f} \hat{g}, \quad \hat{f(x/\lambda)}(t) = \lambda^n \hat{f}(\lambda t). \]
(Note $||f * g||_1 \leq ||f||_1 ||g||_1$).
Lemma (10.10.2.3). Let \( f = e^{-1/2|x|^2} \), then \( f \in S \), \( \hat{f} = f \) and \( f(0) = \int \hat{f} \).

Proof: Reduce to the 1 dimensional case, in which case, \( f' + xy = 0 \), and \( \hat{f} \) also satisfies this. \( \square \)

Lemma (10.10.2.4). For \( f, g \in L^1 \), Fubini theorem shows \( \int \hat{f}g = \int f\hat{g} \).

Prop. (10.10.2.5) [Classical Fourier Transform].

- \( S \) is a Fréchet space in the topology defined by these norms.
- multiplication by \( g \in S \) and derivations are continuous linear map from \( S \) to \( S \) (direct calculation).
- \( \hat{P(D)f(t)} = P(t)\hat{f(t)} \) and \( \hat{Pf} = P(-D)\hat{f} \).
- The Fourier transform is a continuous linear one-to-one automorphism of \( S \), and \( \Psi^2g = g \).

Proof:

1: 
2: 
3: use (10.10.1.10) for the first one, and for the second one, should use definition of derivative and dominated convergence.

4: \( \Psi f \in S \) by 3, and it is continuous by closed graph theorem. By (10.10.2.4) and (10.10.2.2), \( \int \hat{f}(t)g(t/\lambda) = \int f(t/\lambda)\hat{g}(y) \). If \( \hat{f}, \hat{g} \in L^1 \), dominant convergence shows \( g(0)\int \hat{f} = \int f(0)\hat{g} \). So we only need one \( f \) that \( f(0) = \int \hat{f} \). \( f \) is continuous and \( \Psi^2g \) will suffice (10.10.2.3). Hence \( g(0) = \int \hat{g} \) for every such \( g \), and the conclusion follows by translation (10.10.2.2), and (10.9.3.14) also follows. \( \square \)

Cor. (10.10.2.6). If \( f \in L^1(\mathbb{R}^n) \), then \( \hat{f} \in C_0(\mathbb{R}^n) \), and \( ||\hat{f}||_\infty \leq ||f||_1 \), because \( S \) is dense in \( L^1(\mathbb{R}^n) \).

Prop. (10.10.2.7) [Inversion Theorem]. If \( f \in L^1(\mathbb{R}^n) \) and \( \hat{f} \in L^1(\mathbb{R}^n) \), then \( \hat{f} = \Psi^2f \) a.e.

Proof: In (10.10.2.4), let \( g \in S \) and substitute \( g = \Psi g \) and use Fubini, we get \( \hat{f} - \Psi^2f \) is orthogonal to every \( S \), then every continuous function with compact support by (10.4.6.10). Thus they equal a.e. \( \square \)

Cor. (10.10.2.8). If \( f, g \in S \), then \( \hat{fg} = \hat{f} \ast \hat{g} \) (apply Fourier one time and use (10.10.2.2)), and thus \( f \ast g \in S \).

Prop. (10.10.2.9) [Fourier-Plancherel]. If \( f, g \in S \), then

\[
\int fg = \int \overline{g(x)}\hat{f}(t)e^{ixt} = \int \hat{f}(t)\int \overline{g(x)}e^{ixt} = \int \hat{f}g
\]

by inversion formula. And \( S \) is dense in \( L^2 \), thus it extends to a linear isometry of \( L^2(\mathbb{R}^n) \rightarrow L^2(\mathbb{R}^n) \). This coincides with the Fourier transform on \( L^1 \cap L^2 \).

Prop. (10.10.2.10). \( D \) injects into \( S \) and is dense.(Notice they both are complete, but the subspace topology are different)(Use scaling, Cf. [Rudin Functional Analysis P189]). So we call a distribution tempered iff it comes from a continuous functional of \( S \).

From (10.10.1.3), we know any distribution with compact support is tempered. By Holder, every \( f \in L^p(\mathbb{R}^n) \), \( p \geq 1 \) is tempered distribution, and every polynomial or functions of polynomial growth are tempered distribution. \( D \subset S \subset L^2 = (L^2)^\vee \subset S' \subset D' \).

\( S, S' \) is complete (10.6.4.3).
Prop. (10.10.2.11). A \( f \in \mathcal{S}' \) iff \( f = \sum_{|\alpha| \leq m} D\alpha(u\alpha(1 + |x|^2)^{m/2}) \) for some \( m \), where \( u\alpha \in L^2(\mathbb{R}^n) \).

Proof: In fact,

\[
||\varphi||'_m = \left( \sum_{|\alpha| \leq m} \int (1 + |x|^2)^m |D\alpha \varphi|^2 \, dx \right)^{1/2}
\]

is an equivalent set of norms of \( \mathcal{S}' \), Cf.[泛函分析张恭庆 P182]. And each of them defines a Hilbert space. So by Riesz we get the result.

Prop. (10.10.2.12) [Generalized Fourier Transform]. For a tempered distribution \( u \in \mathcal{S}' \), we define the Fourier transformation as the tempered distribution \( \hat{u}(\varphi) = u(\hat{\varphi}) \). It is easily verified that it is compatible with previously defined Fourier transform when seen as tempered distributions by?? In particular, this is defined for compactly supported distribution, \( L^p(\mathbb{R}^n), p \geq 1 \) and smooth functions of polynomial growth (10.10.2.10).

Prop. (10.10.2.13). \( \hat{P(D)u} = Pu \) and \( \hat{Pu} = P(-D)\hat{u} \). And The Fourier transformation is a continuous linear isometry of \( \mathcal{S}' \) in the weak* topology.

Cor. (10.10.2.14). \( \hat{1} = \delta \), thus \( \hat{P} = P(-D)\delta \) and \( \hat{P(D)\delta} = P \). Now (10.10.1.4) tells us a distribution is the Fourier transform of a polynomial iff it has support in the origin.

Prop. (10.10.2.15) [Convolution of Tempered Distributions]. Let \( u \in \mathcal{S}' \) and \( \varphi, \psi \in \mathcal{S} \), then

- \( u * \varphi \in C^\infty \) of polynomial growth and \( D^\alpha(u * \varphi) = (D^\alpha u) * \varphi = u * (D^\alpha \varphi) \).
- \( u * (\varphi * \psi) = (u * \varphi) * \psi \).
- \( \hat{u * \varphi} = \hat{\varphi} \hat{u}, \hat{u} * \hat{\varphi} = \hat{\varphi} \hat{u} \).
- If \( P \) is a polynomial and \( g \in \mathcal{S} \), then \( D^\alpha u, Pu \) and \( gu \) are all tempered.


Prop. (10.10.2.16) [Mellin Inversion Formula]. Given a function \( f : \mathbb{R}^+ \to \mathbb{C} \) satisfying suitable conditions, its Mellin transformation is defined to be

\[
M(f)(s) = \int_0^\infty f(t)t^s \frac{dt}{t}.
\]

whenever this integral is absolutely convergent.

Notice if \( \int_0^1 f(t)t^s \frac{dt}{t} \) is convergent for some \( s \), then it converges for any bigger \( s \), and if \( \int_1^\infty f(t)t^s \frac{dt}{t} \) converges for some \( s \), then it converges for any smaller \( s \). So the domain of \( M(f) \) if nonempty, is a vertical strip \( \sigma_1 < \text{Re}(\sigma) < \sigma_2 \) for \( \sigma_1, \sigma_2 \in [-\infty, \infty] \).

Then \( f \) can be recovered from \( M(f) \): for any \( \sigma_1 < \sigma < \sigma_2 \),

\[
f(x) = \frac{1}{2\pi i} \int_{\sigma-i\infty}^{\sigma+i\infty} x^{-s}M(f)(s)ds.
\]

Proof: Using the isomorphism of groups \( t = e^z : \mathbb{R}^+ \to \mathbb{R} \), this is just the usual Fourier transformation on \( \mathbb{R} \).
Paley-Wiener Theory

**Prop. (10.10.2.17).** For \( \varphi \in D(\mathbb{R}^n) \) that has support in \( rB \), the You-Know-How defined \( \hat{\varphi}(z) \) is an entire function of several variable and satisfies:

\[
|\varphi'(z)| \leq \gamma_N (1 + |z|)^{-N} e^{r|\text{Im} z|}.
\]

For \( N \geq 0 \). Conversely, any such function correspond to a \( \varphi \in D(\mathbb{R}^n) \) that has support in \( rB \).

**Proof:** Cf.[Rudin P198]. \( \square \)

**Prop. (10.10.2.18) [Fourier-Laplace transformation].** For \( u \in D'(\mathbb{R}^n) \) that has support in \( rB \), of order \( N \), the \( \hat{u}(z) = u(e_{-z}) \) is an entire function of several variable and satisfies:

\[
|f(z)| \leq \gamma (1 + |z|)^N e^{r|\text{Im} z|}.
\]

Conversely, any such function correspond to a \( u \in D'(\mathbb{R}^n) \) that has support in \( rB \).

**Proof:** Cf.[Rudin P199]. \( \square \)

3 Sobolev Space

**Def. (10.10.3.1).** For \( 1 \leq p < \infty \), the Sobolev space \( W^{m,p}(\Omega) \) is the space of functions \( u \) that \( D^\alpha u \in L^p(\Omega) \) for every \( |\alpha| \leq m \), with the norm \( \|u\| = \sum_{|\alpha| \leq m} \int_\Omega |D^\alpha u(x)|^p dx \). The Sobolev space \( W_0^{m,p}(\Omega) \) is the completion of the subspace \( C_0^\infty(\Omega) \).

**Prop. (10.10.3.2) [Meyers-Serrin].** The Sobolev space \( W^{m,p}(\Omega) \) is the completion of \( u \in C^\infty(\Omega) \) that \( D^\alpha u \in L^p(\Omega) \) for every \( |\alpha| \leq m \).

**Proof:** Choose a countable partition of unity \( \psi_k \), then as in the proof of(10.4.6.11), we can choose \( \delta_k \) small enough and \( \|\psi u - (\psi u)_{\delta_k}\| < \varepsilon/2^k \) and \( \varphi = \sum (\psi u)_{\delta_k} \) is definable. \( \square \)

**Prop. (10.10.3.3).** We denote \( H^m(\Omega) = W^{m,2}(\Omega) \) and \( H_0^m(\Omega) = W_0^{m,2}(\Omega) \) and \( H^{-m}(\Omega) = (H_0^m(\Omega))^* \) when \( m \) is an integer. Notice derivative is not applicable for \( H^{-m}(\Omega) \) unless \( \Omega = \mathbb{R}^n \).

When \( \Omega = \mathbb{R}^n \), \( D(\mathbb{R}^n) \) is dense in \( W^{m,p}(\Omega) \), thus \( W_0^{m,p} = W^{m,p} \). Define the Sobolev space

\[
H^s = \{ u |(1 + |y|^2)^{s/2} |\hat{u}| \in L^2 \}
\]

\( H^s \) is a Hilbert space and \( H^s \subset S' \) for every \( s \) (use Holder to show \( \hat{u} \in S' \)). \( H^m \) coincides with previously defined \( H^m \) when \( m \) is a positive integer thus also negative-integer. A linear operator on \( H = \bigcup H^s \) is said to have order \( t \) if it maps every \( H^s \) continuously into \( H^{s-t} \).

**Proof:** By Plancherel,

\[
\|\varphi\|_m = (\sum_{|\alpha| \leq m} \|D_\alpha u\|_{L^2}^{2})^{1/2} \quad \text{and} \quad (\int (1 + |y|^2)^m |\hat{u}|^2)^{1/2}
\]

are equivalence norms on \( H^m \). \( \square \)

**Lemma (10.10.3.4) [Poincare Inequality].** For \( \Omega \) bounded, on \( C_0^\infty(\Omega) \) the \( W^{m,p} \) norm is controlled by \( L^p \) norms of its \( m \)th order derivatives.
Proof: We may assume \( \Omega \subset \prod_{i=1}^{n} [0, a] \), then for any \( u \in W^{m,p} \), \( u(x) = \int_0^x D^1 u(t, x_2, \ldots, x_n) dt \), so by Holder inequality,

\[
|u(x)| \leq a^{1/q} \left( \int_0^a |D^1 u|^p dx_1 \right)^{1/p}.
\]

so

\[
\int_{\Omega} |u(x)|^p dx \leq a^q \int_{\Omega} |D^1 u|^p dx_1.
\]

Doing the same for all other derivatives, we can see the norm is controlled by the highest \((m\text{-th})\) order norms.

\( \square \)

Prop. (10.10.3.5). When \( t < s \), \( H^s \subset H^t \). And \( H^s \) are isometric to \( H^t \) by \( \hat{v} = (1 + |y|^2)^{t/2} \hat{u} \) and is of order \( t \). \( D^\alpha \) is of order \( |\alpha| \). If \( f \in S \), then \( u \rightarrow fu \) is an operator of order \( 0 \).

Proof: Cf. [Rudin P217].

\( \square \)

Prop. (10.10.3.6) [Sobolev Embedding Theorem]. On a manifold of dimension \( n \) which is compact with Lipschitz boundary or complete of positive injective radius and bounded sectional curvature,

- if \( k > l \) be integers and

\[
\frac{1}{p} - \frac{k}{n} = \frac{1}{q} - \frac{l}{n}
\]

then \( W^{k,p}(\text{int}(M)) \subset W^{l,q}(M) \) continuously.

- if

\[
\frac{1}{p} - \frac{k}{n} = -\frac{r + \alpha}{n}
\]

then \( W^{k,p}(\text{int}(M)) \subset C^{r,\alpha}(M) \) continuously.

Proof: Cf. [Evans P290].

\( \square \)

Cor. (10.10.3.7) [Gagliardo-Nirenberg-Sobolev]. On a manifold of dimension \( n \) which is compact with Lipschitz boundary or a complete of positive injective radius and bounded sectional curvature, if \( \frac{1}{p'} = \frac{1}{p} - \frac{1}{n} \) (Sobolev conjugate), then \( W^{1,p}(\text{int}(M)) \subset L^{p'}(M) \) continuously.

Cor. (10.10.3.8). On a manifold of dimension \( n \) which is compact with Lipschitz boundary or a complete of positive injective radius and bounded sectional curvature, if \( m > n/2 \), then \( W^{m,2}(\text{int}(M)) \subset C(\Omega)(M) \) continuously. And the functions in \( W^{m,2}_0 \) are continuous and vanish at the boundary, by \( C_0 \) approximation.

Proof: The \( \mathbb{R}^n \) case can be directly proved: because we have the equivalent norm (10.10.3.3), \( \tilde{u} \in L^2 \) thus \( u \in L^2 \), and

\[
\int |\tilde{u}| \leq \left( \int (1 + |x|^2)^m |\tilde{u}|^2 \right)^{1/2} \cdot \left( \int 1/(1 + |x|^2)^m \right)^{1/2}.
\]

We have \( \tilde{u} \in L^1 \), thus inversion formula applies that \( u \) is continuous and \( ||u||_\infty \leq ||\tilde{u}||_1 \leq C ||u||_{H^m} \).

\( \square \)

Cor. (10.10.3.9). \( \cap s H^s = C^\infty(M) \).
Prop. (10.10.3.10)[Rellich-Kondrechov]. On a compact manifold with $C^1$ boundary of dimension $n$, if $k > l$ and
\[
\frac{1}{p} - \frac{k}{n} < \frac{1}{q} - \frac{l}{n}
\]
then $W^{k,p} \subset W^{l,q}$ completely continuously.

Proof: Cf.[Distributions and Operators P199], [Evans P290]. □

Cor. (10.10.3.11). On a bounded extension domain of $\mathbb{R}^n$, $W^{1,p} \subset L^p$ completely continuously.

Proof: We prove the $p = 2$ case. For a sequence $u_m$ in $W^{1,2}$, we have $\|u_m - u_p\|_2 = \|U_m - U_p\|_2$. By (10.7.4.9), there is a subsequence that $\hat{U}_m$ pointwise converge. Notice they are uniformly bounded, Now apply two region argument, for $|x| < r$, use Lebesgue dominant convergence, and for $|x| > r$, use $\int (1 + |x|^2)|\hat{U}_m - \hat{U}_p|^2$ is bounded to conclude $\|u_m - u_p\|_2 \to 0$. □

Prop. (10.10.3.12). $u \in D'(\Omega)$ is a locally $H^s$ $\iff$ $\psi u \in H^s$ for every $\psi \in D(\Omega)$ $\iff$ $D_\alpha u$ is locally $L^2$ for every $|\alpha| \leq s$.

Thus every smooth function is locally $H^s$ for every $s$.

Proof: 1 $\to$ 2 use partition of unity, 2 $\to$ 1 easy, and 2,3 are all equivalent to $D_\alpha(\psi u) \in L^2$ for every $\psi \in D(\Omega)$. by Leibniz+Plancherel or (10.10.3.5). □

Prop. (10.10.3.13). If $r > p + n/2$, then if a function $f$ on $\Omega$ has all the distribution derivative $D^k f$ locally $L^2, = g_{i\alpha}$, for $0 \leq k \leq r$, then $f \in C^p(\Omega)$ a.e.

Cor. (10.10.3.14). If $u \in D'(\Omega)$ is locally $H^s$, then $u \in C^{s-n/2}(\Omega)$. Thus $\cap$ locally $H^s = C^\infty(\Omega)$.

Holder Space

Def. (10.10.3.15). Holder space $C^{k,\alpha}(\Omega)$ is the subspace of $C^k(\Omega)$ with the norm
\[
\|f\|_{C^{k,\alpha}} = \|f\|_{C^k} + \max_{|\beta| = k} \sup_{x \neq y \in \Omega} \frac{|D^\beta f(x) - D^\beta f(y)|}{|x - y|^\alpha}.
\]

4 Fourier Analysis on $\mathbb{T}^n$

Prop. (10.10.4.1). If $f$ is a periodic function on $\mathbb{R}$ with period $2\pi$ and piecewise-differentiable, then the Fourier series of $f$ converges to $\frac{1}{2}(f(x+) + f(x-))$ everywhere.

Proof: [武胜健 2, P264]. □

Prop. (10.10.4.2). If $f$ is a periodic differentiable function on $\mathbb{R}$ with period $2\pi$ and $f'$ is integrable at $[-\pi, \pi]$, then the Fourier series of $f$ converges to $f$ uniformly.

Proof: [武胜健 2, P281]. □

Prop. (10.10.4.3). If $f \in L^1(\mathbb{T})$ is absolutely continuous, then $(\hat{f})(n) = 2\pi in \cdot \hat{f}(n)$.

Prop. (10.10.4.4). $f \in L^1(\mathbb{T})$ is determined by its Fourier coefficients.
10.11 Differential Operators

1 ODE-Fundamentals

Prop. (10.11.1.1).

\[ x^{(2)} = f(x) \]

It can be solved.

Proof:

\[ x'(x^{(2)}) = f(x)x' \]
\[ \frac{1}{2}(x')^{2} = \int f(t)dt \]

Prop. (10.11.1.2) [Wronsky].

2 ODE-Theorems

Prop. (10.11.2.1) [Existence and Uniqueness of ODE of Lipschitz Type]. If \( F(t, x) \) defined on \([-h, h] \times [\eta - \delta, \eta + \delta]\) is a function that is locally Lipschitz: that is, \( \exists \delta, L, \text{ s.t. } |t| \leq h, |x_i - \eta| \leq \delta, \) then

\[ |F(t, x_1) - F(t, x_2)| \leq L|x_1 - x_2|. \]

Then the initial value problem:

\[ (T x)(t) = \eta + \int_{0}^{t} F(\tau, x(\tau))d\tau \]

has a unique solution on the interval \([-h, h]\) if \( h < \min\{\delta/M, 1/L\} \), where \( M \) is the maximum of \( F \) on \([-h, h] \times [\eta - \delta, \eta + \delta]\). Because \( T \) is a contraction.

Prop. (10.11.2.2) [Existence of ODE of continuous Type (Caratheodory)]. If \( F(t, x) \) defined on \([-h, h] \times [\eta - \delta, \eta + \delta]\) is a continuous function, then

\[ (T x)(t) = \eta + \int_{0}^{t} F(\tau, x(\tau))d\tau \]

has a unique solution on the interval \([-h, h]\) if \( h < \delta/M \), where \( M \) is the maximum of \( F \) on \([-h, h] \times [\eta - \delta, \eta + \delta]\). (Use Schauder fixed point theorem and Arzela-Ascali).

Prop. (10.11.2.3) [Existence Theorem for Complex Differential Equations]. Let \( f(z, w) \) be a holomorphic vector function in a domain \( D \subset \mathbb{C}^{n+1} \), then the initial value problem

\[ w' = f(z, w), \quad w(z_0) = w_0 \]

has exactly on holomorphic solution locally (Thus on a simply connected domain).

Cor. (10.11.2.4). So a holomorphic high-order ODE for a complex variable can be solves. And luckily it can be solved even \( \overline{z} \) appears (just regard it as a constant). \( \Delta \)

Proof: Cf. [Ordinary Differential Equations, P110].
Prop. (10.11.2.5). For the equation:

\[ \frac{dy}{dx} = Ay, \]

One solution basis is:

\[
\begin{cases} 
  e^{\lambda_1 x} P^{(1)}_1(x), \ldots, e^{\lambda_1 x} P^{(1)}_{n_1}(x); \\
  \ldots \ldots \\
  e^{\lambda_s x} P^{(d)}_1(x), \ldots, e^{\lambda_s x} P^{(1)}_{n_s}(x); 
\end{cases}
\]

Where

\[ P^{(i)}_j(x) = r^{(i)}_j + x r^{(i)}_{j+1} + \cdots, \]

where \( r^{(i)}_{j0} \) is a basis of solution of \((A - \lambda_i I)^n x = 0\), and \( r^{(i)}_{k+1} = (A - \lambda_i I) r^{(i)}_k \).

Proof: Cf. [常微分方程丁同仁定理 6.6]. □

Cor. (10.11.2.6). For the equation:

\[ y^{(n)} + a_1 y^{(n-1)} + \cdots + a_{n-1} y' + a_n y = 0, \]

If the characteristic equation has \( s \) different roots \( \lambda_1, \ldots, \lambda_s \) and corresponding multiplicities \( n_1, \ldots, n_s \), then:

\[
\begin{cases} 
  e^{\lambda_1 x}, x e^{\lambda_1 x}, \ldots, x^{n_1-1} e^{\lambda_1 x}; \\
  \ldots \ldots \\
  e^{\lambda_s x}, x e^{\lambda_s x}, \ldots, x^{n_s-1} e^{\lambda_s x}; 
\end{cases}
\]

is a solution basis.

Proof: Cf. [常微分方程丁同仁 P198]. □

Prop. (10.11.2.7) [Lyapunov]. Consider the Lyapunov stability of an autonomous system of the form:

\[ \frac{dx}{dt} = Ax + o(|x|), \]

Then:

1. If \( A \) has an eigenvalue whose real part is positive, then the trivial solution is not weak stable.
2. If all eigenvalues of \( A \) have negative real part, then the trivial solution is strong stable.

Stum-Liouville

Prop. (10.11.2.8) [Stum-Liouville]. The eigenvalue BVP problem of L-S equation:

\[ Lu = (pu')' + qu = \lambda u, \quad a_1 u(a) + a_2 u'(a) = 0, \quad b_1 u(b) + b_2 u'(b) = 0, \quad \sigma(x) > 0. \]

can be solved by the method of Green’s function. For the function:

\[ G(x, s) = \begin{cases} 
  C u_1(x) u_2(s), & x < s \\
  C u_2(x) u_1(s), & x > s 
\end{cases} \]
for some $C$, where $u_1$ is a solution of the L-S equation with boundary value at $a$, and $u_2$ with boundary value at $b$ that are linear independent (This happens when the homogenous equation has no solution). It satisfies: $LG(x, s) = \delta(x - s)$ and satisfies the boundary conditions.

Because $L$ is self-adjoint, we have:

$$Gf(x) = \int f(s)G(x, s)ds, \quad LG = \text{id}, \quad GL = \text{id}$$

thus the eigenvalues of $L$ is the reciprocal of the eigenvalues of $G$, and $G$ is a compact self-adjoint operator on $L^2(\sigma, \mathbb{R})$, so by spectral theorem, the eigenvectors are countable and form an orthonormal basis.

And when the homogenous problem do have a solution $\phi$, then we have: $Lu = f$ has a solution iff $(f, \phi) = 0$. one way is simple and the other way is because we solve the initial problem of ODE and find that it automatically satisfies the boundary condition. Cf.[Stum Liouville Theory].

**Prop. (10.11.2.9).** More generally, if there the boundary is mixed of $u(a), U'(a), u(b), u'(b)$, the solution of

$$Lu = (pu')' + qu = 0, \quad B_1(u) = \alpha, \quad B_2(u) = \beta.$$ 

has a unique solution for any $\alpha, \beta$ iff the homogenous equation has only non-trivial solution. (Because the solution space is of 2 dimensional.

**Prop. (10.11.2.10)[Stum Separation Theorem].**

**Prop. (10.11.2.11)[Stum Comparison Theorem].** If $y'' + K_i(x)y = 0$ are equations. If $y_i(0) = 0$ and $|y_1'(0)| = |y_2'(0)|$, then if $K_1(x) \geq K_2(x)$, then $y_1(x) \geq y_2(x)$ until $y_2(x)$ is zero. (directly from (11.2.4.10)).

### 3 Linear PDE

**Def.(10.11.3.1).** For a linear PDE with constant coefficients $P(D)u = v$, the **fundamental solution** is a distribution $E \in D'(\mathbb{R}^n)$ that $P(D)E = \delta$. This is important because if $v$ is a distribution with compact support, $P(D)(E*v) = (P(D)E)*v = \delta*v = v(10.10.1.10)$, so $u = E*v$ is a distribution solution.

**Prop.(10.11.3.2).** When $v \in D'(\mathbb{R}^n)$ has compact support, $P(D)u = v$ has a solution $u$ with compact support iff $Pg = \hat{v}$ has a solution $g$ entire. In this case, $g = \hat{u}$ for some distribution $u$, and $u$ has support in the convex hull of the support of $v$.

**Proof:** Use(10.10.2.18), and some bound relation between $g$ and $Pg$. Cf.[Rudin Functional Analysis P212].

**Prop.(10.11.3.3).** The fundamental solution always exist when for PDE of constant coefficients.

**Proof:** For a $\varphi \in D(\mathbb{R}^n)$, there is at most one $\psi$ that $\psi = P(D)\varphi$ because $\hat{\psi} = P\hat{\varphi}$ and they are entire function. Thus the task is to verify the functional $u : P(D)\varphi \mapsto \varphi(0)$ is continuous and extend to a distribution $u \in D'(\mathbb{R}^n)$. Cf.[Rudin Functional Analysis P215].

### 4 Differential Operators on Manifolds

**Prop. (10.11.4.1)[Index Theorem P109].** has a nice definition of symbol of a differential operator on a manifold as a map form $\text{Sym}^m T^*M \otimes C \to \text{Hom}(E, F)$.
5 Pseudo-Differential Operator

Def.(10.11.5.1). Denote the Japanese bracket \(|x| = (1 + |x|^2)^{1/2} \sim 1 + |x|\).

Motivated by the formula \((\tilde{P}f) = P(D)f\) for \(f \in \mathcal{S}\) and polynomial \(P\) of \(\xi\) with coefficients smooth functions of \(x\)? we define the symbol class \(S^{\mu, \beta}\) as the space of smooth functions \(a : \mathbb{R}^{2n} \to \mathbb{C}\) that
\[
|D_{x, \alpha}D_{\xi, \beta}a(x, \xi)| \leq C_{\alpha, \beta}|x|^{|\mu| - |\beta|}
\]
and denote \(S^m = S^{0,m}\).

We denote the symbol class \(A^v\) as the space of smooth functions \(a : \mathbb{R}^{2n} \to C\) that \(|D_\alpha a| \leq C_a|x + \xi|^v\) for any \(\alpha\). So \(S^{\mu - |\alpha|, m} \subset A^{\mu + |\alpha|}\).

And we define the pseudo-differential operator of symbol \(a\):
\[
(a(x, D)u)(x) = \int_\xi e^{ix\xi}a(x, \xi)\hat{u}
\]
Moreover, we can define the amplitude function \(p(x, y, \xi)\) and define
\[
Pu(x) = \int e^{i(x - y)\xi}p(x, y, \xi)u(y)dy.
\]

Def.(10.11.5.2). We define the space \(S^d\) of polyhomogenous symbols of degree \(d\) as the set of all symbols in \(S^d_{0,1}\) that there exists a set of \(p_{d-l}\) homogenous in \(\xi\) of degree \(d-l\) that \(p = \sum p_{d-l}\) modulo an operator in \(S^{-\infty}\). Note that when \(p_{d-l}\) is homogenous of degree \(d-l\), then it is automatically in \(S^d_{0,1}\).

Def.(10.11.5.3). A pseudo operator \(a\) is called elliptic if \(\sigma(a) \in S^m\) and \(\sigma(a) \geq |\xi|^{-m}\) for \(\xi\) big enough.

Prop.(10.11.5.4)[Peetre’s Inequality]. For all \(v \in \mathbb{R}\), there is a constant \(C\) that
\[
[X + Y]^v \leq C[X]^v[Y]^v.
\]

Proof: For \(v > 0\), just as normal. For \(v < 0\), use \(X = (X + Y) + (-Y)\) applied to \(-v\). \(\square\)

Prop.(10.11.5.5). The mapping \(a(x, \xi) \times u(x) \mapsto a(x, D)u\) is continuous from \(A^v \times \mathcal{S} \to \mathcal{S}\), thus also continuous from \(S^{\mu, m} \times \mathcal{S} \to \mathcal{S}\). Cf.[Pseudo Differential Operator P28].

Lemma(10.11.5.6)[Schur Test]. For a function \(K\) on \(\mathbb{R}^{2n}\) and \(u \in L^p(\mathbb{R}^n)\), let \(||K||_1 = \sup_x \int |K(x, y)|dy\) and \(||K(x, y)||_2 = \sup_y \int |K(x, y)|dx\). Let \(Au(x) = \int K(x, y)u(y)dy\), then
\[
||Au||_p \leq ||K||_1^{1/p}||K||_2^{1/p}||u||_{L^p}.
\]

by Holder.

Prop.(10.11.5.7)[Calderón-Vaillancourt]. There is a constant \(C, N_{CV}\) that for \(u \in \mathcal{A}^0\) and \(\varphi \in \mathcal{S}\)
\[
||Op(u)\varphi||_{L^2} \leq C\max_{|\alpha| + |\beta| \leq N_{CV}}||\partial^\alpha_x \partial^\beta_\xi u||_{L^\infty}||\varphi||_{L^2}.
\]

This in particular applies to \(u \in S^0\).

Proof: Cf.[Calderon-Vaillancourt]. \(\square\)

Cor.(10.11.5.8). \(S^m\) maps \(H^s\) to \(H^{s-m}\). Because by symbolic calculus(10.11.5.10), we have
\[
Op([\xi]^{s-m})Op(u)Op([\xi]^{-s}) = Op(b) \in S^0,
\]
thus \(Op(u) = Op([\xi]^{m-s})Op(b)Op([\xi]^s)\) maps \(H^s\) into \(H^{s-m}\).
Symbolic Calculus

Def. (10.11.5.9) [Semiclassical Operator]. For $a \in S^{\mu,m}$ and $h \in (0,1]$, we denote $a_h(x,\xi) = a(x,h\xi)$, it is also in $S^{\mu,m}$.

Prop. (10.11.5.10) [Composition]. If $a \in S^{\mu_1,m_1}$ and $b \in S^{\mu_2,m_2}$, there is a pseudo-differential operator $(a\#b)(h) \in S^{\mu_1+\mu_2,m_1+m_2}$ for every $h \in (0,1]$ that

$$Op(a_h)Op(b_h) = Op((a\#b)(h))$$

and for all $J > 0$, $(a\#b)(h)$ can be written as

$$a\#b(h) = \sum_{j<J} h^j \left( \sum_{|\alpha| = j} \frac{1}{\alpha!} aD_\xi^\alpha D_x^\alpha b \right) + h^J r^\#_J(a,b,h)$$

where $r^\#_J(a,b,h) \in S^{\mu_1+\mu_2,m_1+m_2-J}$ and it is bilinear of $a,b$ and equicontinuous independently of $h$.

Proof: Cf. [Pseudo Differential Operator P36]. \qed

Prop. (10.11.5.11) [Adjoint]. If $a \in S^{\mu,m}$ and $u,v \in \mathcal{S}$, there is a pseudo-differential operator $a^*(h)$ for every $h \in (0,1]$ that

$$(u,Op(a_h)v) = (Op(a^*(h))u,v)$$

in the $L^2$ norm and for all $J > 0$, $a^*(h)$ can be written as

$$a^*(h) = \sum_{j<J} h^j \left( \sum_{|\alpha| = j} \frac{1}{\alpha!} aD_\xi^\alpha D_x^\alpha a \right) + h^J r^*_J(a,h)$$

where $r^*_J(a,h) \in S^{\mu,m-J}$ and it is anti-linear of $a$ and equicontinuous independently of $h$.

Proof: Cf. [Pseudo Differential Operator P30]. \qed

Def. (10.11.5.12). For $u \in \mathcal{S}'$, we define the action of $a(x,\xi)$ on $u$ by

$$(Op(a_h)u)(\varphi) = u(\overline{Op(a^*(h))\varphi}).$$

This is compatible with the definition on $\mathcal{S}$.

6 General PDE

Direct Solution

Prop. (10.11.6.1) [Characteristic Line]. Consider a 1-dimensional parabolic equation:

$$p_t + c(p,x,t)p_x = r(p,x,t)$$

Let $P(t) = p(X(t),t)$, this equation is equivalent to

$$P_t = r(X(t),t,P(t)), \quad X_t = c(X(t),t).$$

an ODE equation.
Prop. (10.11.6.2). A set of equations:

\[ \frac{\partial}{\partial x^i} \mu = A_i \mu \]

where \( \mu \) is an \( n \)-vector. It has a solution iff

\[ [A_i, A_j] = \frac{\partial}{\partial x^i} A_i - \frac{\partial}{\partial x^j} A_j. \]

Proof:

\[ \square \]

Cor. (10.11.6.3). This seems to be able to derive Frobenius integrability theorem, but I cannot figure it out.

7 Analysis on Manifolds

Prop. (10.11.7.1) [Peetre’s Theorem]. For a linear operator from \( C^\infty(M) \) to \( C^\infty(M) \) such that \( \text{Supp}(Lu) \subseteq \text{Supp}(u) \) where \( M \) is a compact manifold, then on every compact subset of a coordinate chart \( L \) looks like a differential operator of finite order.

Proof: The first thing is to prove on a chart \( \Omega \), \( L \) is continuous on \( C^\infty_0(\Omega) \). In fact, it suffice to show it is continuous from \( C^\infty_0(\Omega) \) to \( C^0_{0}(\Omega) \) because we can apply to \( D_\alpha L \). For this, Cf.[Pseudo Differential Operator P86].

Then we have \( |Lu| \leq C \max_{\alpha \leq m} \sup_K |D_\alpha \varphi| \) for every \( \varphi \in C_0(K) \). And the functional \( \varphi \rightarrow (L\varphi)(x) \) is a distribution supported on \( x \), thus by (10.10.1.4), it is of the form

\[ Lu(x) = \sum_{|\alpha| \leq m} a_\alpha(x) D_\alpha \varphi(x). \]

We need to show \( a_\alpha \) is smooth, which we choose a bump function \( \chi \) to show \( a_0 \) is smooth and then choose \( x_i \chi \) applied to \( L\varphi - a_0 \varphi \) to show \( a_i \) is smooth, etc. \[ \square \]

Prop. (10.11.7.2). The property of \( \psi\text{do} \) of order \( d \) is preserved under diffeomorphism, Cf.[Distributions and Operators P195], giving us the possibility to define \( \psi\text{do} \) differential operator on manifolds, and the principal symbol variate in this way that it forms a function from the cotangent bundle to the \( M_n(\mathbb{C}) \). And the Sobolev space is defined by the property that all of its restrictions on a atlas are Sobolev, using the partition of unity.

Prop. (10.11.7.3). All the norms of different are commensurable up to constant factor w.r.t. each other, so it doesn’t quite matter with different norms.

Prop. (10.11.7.4). The parametrix exists for an elliptic operator on manifolds. Cf.[Distributions and Operators P207].

8 Elliptic Operators

Prop. (10.11.8.1). Elliptic operator is a Fredholm operator. And the kernel and cokernel are smooth functions, so it is also a Fredholm operator on \( C^\infty(\Omega) \).

Proof: It suffice to find a left and right inverse modulo compact operators, and in fact we find it modulo \( S^{-\infty} \). Since \( S^{-\infty} \) are all compact operators, i.e. it has a parametrix. Cf.[Distributions and Operators, P184]. \[ \square \]
Prop. (10.11.8.2) [Garding Inequality]. For an elliptic operator of order \( d \) on \( \Gamma(E) \),
\[
||f||_{H^s} \leq C(||f||_{H^{s-d}} + ||Pf||_{H^{s-d}})
\]

Proof: \( \square \)

Cor. (10.11.8.3) [Elliptic Regularity Theorem]. The inverse image of a smooth function under an elliptic operator is a smooth function, because the intersection of \( H^s(E) \) is \( C^\infty(E) \).

Cor. (10.11.8.4) [Elliptic Regularity Theorem]. For \( L = \sum_{|\alpha| \leq N} f_\alpha D_\alpha \), where \( f_\alpha \in C^\infty(\Omega) \) and the equation \( Lu = v \) for distributions \( u \) and \( v \in D'(\Omega) \), when \( v \) is locally \( H^s \), \( u \) is locally \( H^{s+N} \). Thus if \( v \in C^\infty(\Omega) \), then \( u \in C^\infty(\Omega) \) by (10.10.3.12)(10.10.3.14).

Proof: We prove the case when \( L \) has leading coefficients constant. For every \( \varphi \in D(\Omega) \) that is 1 on some open ball \( B \), \( \varphi u \) has compact support thus in some \( H^t < \) and then we use a sublemma that says if \( \psi \) is 1 on the support of \( \varphi \), then if \( \psi u \) is in \( H^t \), where \( t \leq s + N - 1 \), then \( \varphi u \in H^{t+1} \). In this way, we can shrink the nbhd to reach \( H^{s+N} \). The proof of the lemma is in [Rudin Functional Analysis P220]. \( \square \)

Prop. (10.11.8.5) [Analytic Ellipticity theorem]. Suppose \( L \) is an analytic elliptic differential operator on a domain \( M \subset \mathbb{R}^n \), then every solution to \( L \varphi = 0 \) is analytic.

Proof: \( \square \)

Prop. (10.11.8.6). The formal adjoint of an elliptic operator is an elliptic operator.

Proof: \( \square \)

Cor. (10.11.8.7). The index of an elliptic operator, regarded as an operator form \( L_s \to L_{s-d} \) doesn’t depend on \( s \), because all the kernel of \( P \) and \( P^* \) are smooth.

Prop. (10.11.8.8). For an elliptic operator, \( H \) has a inverse, the Green function which is a compact operator, so it has countable eigenfunctions consisting of smooth functions on \( L^2 \) with eigenvalues converging to \( \infty \). Moreover, the eigenvalues satisfy \( |\lambda_n| \geq Cn^\delta \) for some \( \delta, C \).

Proof: We prove for \( P \) self-adjoint. Use (10.11.8.1), ker \( P \) is all smooth, so there is a map \( P(H^{-2d}) \to P(H^{-d}) \) which is bijective thus an isomorphism by Banach. So the inverse of this isomorphism composed with the Sobolev embedding \( H^{-d} \to L^2 \) is a compact operator \( G \). We notice that this map has the same eigenfunctions as \( P \), thus the result from that of compact operators.

For the second assertion, if suffice to prove \( \dim N(\lambda) \leq C\lambda^M \). Using Garding inequality and Sobolev embedding, we have for \( f \in N(\lambda), ||f||_{C^0} \leq C(1 + \lambda^l)||f||_{L^2} \) for large \( l \). So if we choose an orthonormal basis \( f_i \), then \( |a_i f_i(x)| \leq C(1 + \lambda^l)|\sqrt{\sum |a_i|^2} | \). Let \( a_i = f_i(x) \) and integrate over \( M \), we get the desired result. \( \square \)

Cor. (10.11.8.9). For a self-adjoint elliptic operator \( P \) which is not a constant, \( L^2(E) \) has a basis consisting of eigenfunctions of \( P \).

Cor. (10.11.8.10) [Stum-Liouville]. This can be used to solve for example eigenvalue problem for Liouville’s equation:
\[
(pu')' + qu = \lambda \sigma u.
\]
where \( p \) and \( \sigma \) are positive. Cf. (10.11.8.2).
Cor. (10.11.8.11). The Hermite functions $C_n e^{x^2/2} d^n e^{-x^2}$, as the eigenvector of $\hat{H} = x^2 - \frac{d^2}{dx^2}$, forms a complete basis for $L^2(\mathbb{R})$. Because it is $e^{-x^2}$ times the solution of the operator $(e^{-x^2} F')' - e^{-x^2} F$.

Prop. (10.11.8.12). For a formally self-adjoint elliptic operator $P$ of degree $d$ on $E$, $\Gamma(E) = \text{Im} P \oplus P(\Gamma(E))$.

Proof: We know that $L^2(E) = P(H^dE) \oplus \ker P$, and $\ker P$ are all smooth by (10.11.8.3), so $\Gamma(E) = \ker P \oplus P(H^dE) \cap \Gamma(E)$. Now use Garding’s inequality (10.11.8.2), the intersection is just $P(\Gamma(E))$, thus the result. □

Prop. (10.11.8.13) [Asymptotic Heat Equation]. In this case we have the series

$$h_t(A^*A) = \sum_{\lambda} e^{-\lambda t} \dim \Gamma_\lambda(E)$$

converges and $h_t$ has an asymptotic expansion

$$h_t = \sum_{k \geq -n} t^{k/2m} U_k(A^*A)$$

where $n = \dim M$ and $U_k = \int_M \mu_k$ for a differential form on $M$. Cf. [Heat Equation and the Index Theorem P297].

By the proposition above, the eigenspaces of eigenvalue non-zero neutralize, so $\text{Ind } A = h_t(A^*A) - h_t(\AA^*)$, so

$$\text{Ind } A = U_0(A^*A) - U_0(\AA^*) = \int_M \mu_0(A^*A) - \mu_0(\AA^*).$$

The proof consists of the following propositions,

Prop. (10.11.8.14). Using the fact that an elliptic operator has a countable basis, for an elliptic operator $P$, when $t > 0$, we let $K(t, x, y) = \sum_{n} e^{-t\lambda_n} \Phi_n(x) \overline{\Phi}_n(y)$, then

$$e^{-tP} f(x) = \int K(t, x, y) f(y) dy.$$

$K(t, x, y)$ is smooth, and the trace of $e^{-tA^*A}$ is exactly $h_t(A^*A)$ as in the last proposition. And the trace is just $\int_M K(t, x, x)$, as can be easily seen.

Proof: Use Garding inequality and (10.11.8.8), we can show $\|K\|_{C^k}$ is bounded. □
10.12 D-modules
10.13 Dynamic System

Main References are [B-S02].

1 Topological Dynamic System

Def. (10.13.1.1) [Topological Dynamic System]. A topological dynamic system is a topological space \( X \) and either a continuous map \( f : X \to X \) or a continuous (semi)flow \( f^t \) on \( X \).

Def. (10.13.1.2) [Notations]. Let \( f : X \to X \) be a topological dynamic system, then

- For \( x \in X \), its \( \omega \)-limit points are defined to be
  \[
  \omega(x) = \cap_{n \in \mathbb{N}} \overline{\cup_{i \geq n} f^i(x)}
  \]

- If \( f \) is invertible, for \( x \in X \), its \( \alpha \)-limit points are defined to be
  \[
  \alpha(x) = \cap_{n \in \mathbb{N}} \overline{\cup_{i \leq n} f^i(x)}
  \]

- The set \( \mathcal{R}(f) \) of (positively) recurrent points are the points \( x \) that \( x \in \omega(x) \).

- The set \( NW(f) \) of non-wandering points are the points \( x \) that for any nbhd \( U \) of \( x \), there is an \( n > 0 \) that \( f^n(U) \cap U = \emptyset \).

- Denote
  \[
  \mathcal{O}(x) = \cup_{n \in \mathbb{Z}} f^n(x), \quad \mathcal{O}^+(x) = \cup_{n \geq 0} f^n(x).
  \]

- Let \( X \) be compact, then a closed non-empty forward \( f \)-invariant \( Y \subset X \) is called a minimal set for \( f \) if there is no smaller such set.

- A point \( x \in X \) is called almost periodic if for any nbhd \( U \) of \( x \), \( \{i | f^i(x) \in U\} \) is relatively dense in \( \mathbb{N} \), i.e. appear in every \( k \) consecutive integers for some \( k \).

Prop. (10.13.1.3).

- \( NW(f) \) is closed, \( f \)-invariant, and contains \( \alpha(x), \omega(x) \) for all \( x \).

- Every recurrent point is non-wandering, thus \( \mathcal{R}(f) \subset NW(f) \).

- Let \( X \) be compact Hausdorff, then \( \overline{\mathcal{O}^+(x)} \) is minimal for \( f \) iff \( x \) is almost periodic.

Proof: item1 is easy, 2 follows from1 as \( x \in \omega(x) \).

For 3: suppose \( x \) is almost periodic and \( y \in \overline{\mathcal{O}^+(x)} \), we need to show that \( x \in \overline{\mathcal{O}^+(y)} \). For any nbhd \( x \in U \), there is a small nbhd \( x \in U' \subset U \) and a nbhd \( \Delta \subset V \subset X \times X \), that if \( x_1 \in U' \) and \( (x_1, x_2) \in V \), then \( x_2 \in U \). Since \( x \) is periodic, there is a \( K \) that for any \( j \geq 0 \), there is a \( f^{j+k}(x) \in U' \) for some \( 0 \leq k \leq K \). Let \( V' = \cap_{i=0}^K f^{-1}(V) \), then \( V' \) is open and contains the diagonal. Thus there is a nbhd \( W \) of \( y \) that \( W \times W \subset V' \). Now choose \( f^n(x) \in W \) by almost periodicity, and \( f^{n+k}(x) \in U' \) for some \( 0 \leq k \leq K \), then we have \( (f^{n+k}(x), f_k(x)) \in V \) by the definition of \( V' \) and \( W \), and hence \( f^k(x) \in U \). This shows \( x \in \overline{\mathcal{O}^+(y)} \).

Conversely, if \( x \) is not almost periodic, then there is a nbhd \( U \) of \( x \), that there is a sequence \( \{a_i\} \in \mathbb{N} \), that \( f^{a_i+j}(x) \notin U \) for \( j \leq i \). By convergence theorem and passing to a subsequence, we assume \( y \) is a the limit of \( f^{a_i}(x) \), and \( f^j(y) \notin U \) for any \( j > 0 \), thus \( x \notin \overline{\mathcal{O}^+(y)} \), showing \( \overline{\mathcal{O}^+(x)} \) is not minimal. □
Prop. (10.13.1.4) [Minimal Set Exists on Compact Dynamic System]. If \( f \) is a topological dynamic system on a compact space, then there exists a minimal set. In particular, there exists an almost periodic point, in priori positively recurrent point, by (10.13.1.3).

Proof: Use Zorn’s lemma and the finite intersection property. □

Def. (10.13.1.5) [Topologically Transitive]. A topological dynamic system \( f : X \to X \) is called topologically transitive if there is a point \( x \) that \( \overline{O(x)} = X \).

Prop. (10.13.1.6). Let \( f \) be a continuous map of a locally compact Hausdorff second countable space \( X \). Suppose that for any two non-empty open set \( U, V \), there is \( n > 0 \) that \( f^n(U) \cap V \neq \emptyset \), then \( f \) is topologically transitive.

Proof: For any open subset \( V \), the hypothesis says \( \bigcup_{n>0} f^{-n}(V) \) is dense in \( X \). Let \( V_i \) be a countable basis for the topology of \( X \), and \( Y = \bigcap_i \bigcup_{n>0} f^{-n}(V_i) \), then it is non-empty, by Baire category theorem (3.6.9.2). Now the orbit of any \( y \in Y \) enters every \( V_i \), thus its orbit is dense in \( X \). □

Prop. (10.13.1.7). Let \( f : X \to X \) be a homeomorphism of a compact metric space, and suppose \( X \) has no isolated points, then if there is a dense orbit \( O(x) \), there will be a dense orbit \( O^+(x) \).

Proof: The hypothesis that \( X \) has no isolated points shows that \( O(x) \) meets every open subset \( U \) infinitely many times, thus we can choose \( f^{n_k}(x) \in B(x, 1/k) \) that \( |n_k| \to \infty \). Thus \( f^{n_k+l}(x) \to f^l(x) \) for any \( l \).

If there are infinitely many \( n_k > 0 \), then we have \( O(x) \subset O^+(x) \), hence \( O^+(x) \) is dense. If there are infinitely many \( n_k < 0 \), then \( O^-(x) \) is dense. Then for any open subset \( U, V \), we can find \( i < j < 0 \) that \( f^i(x) \in U, f^j(x) \in V \), thus \( f^{j-i}(U) \cap V \neq \emptyset \). Hence we use (10.13.1.6) to conclude \( f \) is topologically transitive. □

Def. (10.13.1.8) [Topological Mixing]. A topological dynamic system \( f : X \to X \) is called topologically mixing if for any two non-empty open subsets \( U, V \), there is \( N > 0 \) that \( f^n(U) \cap V \neq \emptyset \) for any \( n \geq N \).

Def. (10.13.1.9). A homeomorphism \( f : X \to X \) is called expansive if there is a \( \delta > 0 \) that for any two distinct points \( x, y \), there is some \( n \in \mathbb{Z} \) that \( d(f^n(x), f^n(y)) \geq \delta \). Similarly, we can define positively expansive for a non-invertible continuous map \( f : X \to X \). This constant \( \delta \) is called a expansiveness constant of \( f \).

Prop. (10.13.1.10) [Compact Metric Space not positively expansive]. If \( f \) be a continuous map of an infinite compact metric space \( X \), then it is not positively expansive.

Proof: First assume \( f \) is invertible. Fix \( \varepsilon > 0 \), consider all \( m \) that there are points \( x \neq y \) that

\[
d(f^n(x), f^n(y)) < \varepsilon, \quad 0 < n \leq m, \quad d(x, y) \geq \varepsilon.
\]

If these \( m \) are infinite, then we can use convergence point theorem to find a point \( x, y \) that \( d(f^n(x), f^n(y)) < \varepsilon \) for any \( n > 0 \), thus \( f \) is not expansive.

If these \( m \) are finite, let \( M \) be a maximal, then by absolute convergence, there is a \( \delta \) that if \( d(x, y) \leq \delta \), then \( d(f^n(x), f^n(y)) < \varepsilon \) for any \( 0 \leq n \leq m \). Then by definition of \( M \),

\[
d(f^{-1}(x), f^{-1}(y)) < \varepsilon, \text{ and similarly } d(f^{-n}(x), f^{-n}(y)) < \varepsilon \text{ for any } n < 0.
\]
Now choose a finite $\delta/2$-net $\{x_i\}$ of $M$, then for each $j \in \mathbb{Z}$, there are two $f^j(x_\alpha), f^j(x_\beta)$ in the same $B(\delta/2, x_j)$, thus $d(f^n(x_\alpha), f^n(x_\beta)) < \varepsilon$ for $n \leq j$. Now there are only f.m. pairs of elements in $M$, there are some pair $(x_\alpha, x_\beta)$ appeared infinitely many times for different $j > 0$, thus we have $d(f^n(x_\alpha), f^n(x_\beta)) < \varepsilon$ for any $n \in \mathbb{Z}$.

For the non-invertible case, the proof is the same, noticing that $f^{-1}$ is chosen wisely when it can be defined. □

Cor. (10.13.1.11). Let $f$ be an expansive homeomorphism of an infinite compact metric space $X$, then there are distinct points $x_0, y_0$ that $\lim_{n \to \infty} d(f^n(x_0), f^n(y_0)) = 0$.

Proof: Let $\delta$ be an expansive constant of $f$, then by (10.13.1.10), there are $x_0 \neq y_0 \in X$ that $d(f^n(x_0), f^n(y_0)) \leq \delta$ for all $n > 0$. Suppose $d(f^n(x), f^n(y)) \to 0$, then by compactness in $X \times X$, there is a subsequence $\{n_k\} \in \mathbb{N}$ that $f^{n_k}(x) \to x', f^{n_k}(y) \to y'$ with $x' \neq y'$. Then this will show that $d(f^{m_k}(x), f^{m_k}(y)) < \delta$ for any $m \in \mathbb{Z}$, contradicting expansiveness of $f$. □

Def. (10.13.1.12). Let $f : X \to X$ be a homeomorphism of compact Hausdorff space, then

- two points $x, y$ are called **proximal** if the closure of orbits $\overline{O}(x,y)$ under $f \times f$ intersect the diagonal $\Delta \subset X \times X$. It is called **distal** otherwise. $f$ is called **distal** if every two distinct points $x, y$ are distal.

- $f$ is called **equicontinuous** if the family $\{f^n\}_{n \in \mathbb{Z}}$ is equicontinuous.

Prop. (10.13.1.13). A equicontinuous homeomorphism $f$ of a compact metric space are distal.

Proof: Suppose $f$ is not distal, then there is a proximal pair $(x, y)$, thus there is a sequence $\{n_k\} \subset \mathbb{Z}$ that $d(f^{m_k}(x), f^{m_k}(y)) \to 0$. Let $d(x, y) = \varepsilon$, thus for any $\delta > 0$, there is some $d(f^{m_k}(x), f^{m_k}(y)) < \varepsilon$, thus contradicting the equicontinuity of $f^{-n}$. □

Def. (10.13.1.14) [Almost Periodic Set]. For a subset $A \subset X$ and a homeomorphism $f : X \to X$, denote by $f_A$ the action of $f$ on $X^A$. Then $A$ is called **almost periodic** if every $z \in \text{Mor}(A, A)$ is almost periodic for $f_A$. Equivalently, for any finite set of points $\{x_i\} \in A$, and nbhds $x_i \in U_i$, the set $\{k \in \mathbb{Z} | f^k(x_i) \in U_i\}$ is relatively dense in $\mathbb{Z}$. This is compatible with the previous definition of almost periodic point (10.13.1.2).

Def. (10.13.1.15). A homeomorphism of a compact Hausdorff space is called **pointwise almost periodic** if every point $x$ is almost periodic. By (10.13.1.3), we can see that this is equivalent to $X$ is a union of minimal sets.

Lemma (10.13.1.16). Every almost periodic set $A$ is contained in a maximal almost periodic set in $X$.

Proof: It is because of the second definition of almost periodic set (10.13.1.14) that the sum of an ordered family of almost periodic sets is also almost periodic. □

Prop. (10.13.1.17). Let $f$ be a homeomorphism of a compact Hausdorff space $X$, then every point $x \in X$ is proximal to an almost periodic point.

Proof: If $x$ is almost periodic, then we are done. If not, consider a maximal almost periodic set $A \subset X$, then $x \notin A$. Then for $z \in X^A$ with range $A$, consider $(x, z) \in X \times X^A$, and find an almost periodic point $(x_0, z_0)$ of $f \times f_A$ in $\overline{O}(x, z)$, by (10.13.1.4). Because $z$ is almost periodic, $z \in \overline{O}(z_0)$, by (10.13.1.3). Thus we see $(x', z) \in \overline{O}(x_0, z_0)$ for some $x'$, by the compactness of $X$. Then $(x', z)$ is also almost periodic, and we can forget about $x_0, z_0$.

Therefore, $\{x'\} \cup \text{Im}(z) = \{x'\} \cup A$ is almost periodic for $f$, and since $A$ is maximal, $x' \in A = \text{Im}(z)$. This shows $(x', x') \in \overline{O}(x, x')$, showing $x$ is proximal to $x'$. □
**Cor.(10.13.1.18) [Distal Homeomorphism is Pointwise Almost Periodic]**. If \( f \) is a distal homeomorphism of a compact Hausdorff space, then \( f \) is pointwise almost periodic.

**Prop.(10.13.1.19).**

- A homeomorphism of a compact Hausdorff space is distal iff the product system \( (X \times X, f \times f) \) is pointwise almost periodic.
- A factor system of a pointwise almost periodic homeomorphism is pointwise almost periodic.
- A factor system of a distal homeomorphism is distal.

**Proof:**

1: If \( f \) is distal, then so is \( f \times f \), hence it is pointwise almost periodic, by (10.13.1.18). Conversely, if \( f \times f \) is pointwise almost periodic, then if \( x, y \) is proximal, then \( (z, z) \in \overline{O(x, y)} \), but since \( \overline{O(x, y)} \) is minimal, by (10.13.1.3), \( (x, y) \subset \overline{O(z, z)} \subset \Delta \), hence \( x = y \).

2: This is easy.

3: if \( f \) is a factor of \( g \), then \( f \times f \) is a factor of \( g \times g \), but the latter is pointwise locally periodic, thus the first is also locally periodic, by 2, and then \( f \) is distal, by 1.

---

**Topological Entropy**

**Def.(10.13.1.20) [Definitions].** Let \( (X, d) \) be a compact metric space, and \( f \) a continuous map \( X \to X \), we define

- for \( x, y \in X \), \( d_n(x, y) = \max_{0 \leq k \leq n-1} d(f^k(x), f^k(y)) \).
- a subset \( A \subset X \) is called \( (n,\varepsilon)\)-spanning if it is a \( \varepsilon \)-net in \( X, d_n \). Similarly, we can define \( (n,\varepsilon)\)-separated and \( \text{cov}(n,\varepsilon, f) \) the minimal number of covering of \( X \) of \( d_n \)-diameter\( < \varepsilon \).

**Lemma(10.13.1.21).** \( \text{cov}(n, 2\varepsilon, f) \leq \text{span}(n,\varepsilon, f) \leq \text{sep}(n,\varepsilon, f) \leq \text{cov}(n,\varepsilon, f) \).

**Proof:** Easy.

**Prop.(10.13.1.22) [Topological Entropy].** The number

\[
\lim_{n \to \infty} \frac{1}{n} \log(\text{cov}(n,\varepsilon, f)) = h_\varepsilon(f)
\]

is well-defined and finite. It is increasing as \( \varepsilon \) decreces, so \( h(f) = \lim_{\varepsilon \to 0^+} h_\varepsilon(f) \) exists, which lies in \([0,\infty]\). It is called the **topological entropy** of \( f \).

Notice the entropy can be calculated by either cov, span or sep, by (10.13.1.21).

**Proof:** For this, we need to notice if \( U \) has \( d_n \)-diameter\( < \varepsilon \) and \( V \) has \( d_m \)-diameter\( < \varepsilon \), then \( U \cap f^{-m}(V) \) has \( d_{m+n} \)-diameter\( < \varepsilon \). Hence

\[
\text{cov}(m + n,\varepsilon, f) \leq \text{cov}(m,\varepsilon, f) \cdot \text{cov}(n,\varepsilon, f).
\]

Thus we can use (20.1.1.1) to conclude.

**Prop.(10.13.1.23).** The topological entropy doesn’t depend on the metric generating the topology.

**Proof:** This is because \( d' \) is a continuous function on \( (X \times X, d \times d) \), thus it is uniformly continuous as \( X \) is compact, so

\[
\text{cov}(n,\varepsilon, f) \leq \text{cov}(n,\delta(\varepsilon), f)
\]

where \( \delta(\varepsilon) \to 0 \) when \( \varepsilon \to 0 \). This shows the topological entropies are the same.
Cor. (10.13.1.24). Two conjugate dynamic systems have the same topological entropy.

Prop. (10.13.1.25) [Properties of Entropy]. Let \( f : X \to X \) be a continuous map of a compact metric space \( X \), \( g : Y \to Y \) be a continuous map of a compact metric space \( Y \), then

- \( h(f^m) = m \cdot h(f) \) for \( m > 0 \).
- If \( f \) is invertible, then \( h(f^{-1}) = h(f) \).
- Let \( A_i \) be a finite family closed forward \( f \)-invariant subsets of \( X \) whose union is \( X \), then
  \[
  h(f) = \max h(f|_{A_i}).
  \]
- \( h(f \times g) = h(f) + h(g) \), and if \( f \) is an extension of \( g \), then \( h(f) \geq h(g) \).

Proof: 1: Use two inequalities:

\[
\text{span}(n, \varepsilon, f^m) \leq \text{span}(mn, \varepsilon, f), \quad \text{span}(n, \delta(\varepsilon), f^m) \geq \text{span}(mn, \varepsilon, f)
\]

where \( \delta(\varepsilon) \to 0 \) if \( \varepsilon \to 0 \), and (10.13.1.21).

2: Because \((n, \varepsilon)\)-separated sets for \( f \) and \((n, \varepsilon)\)-separated sets for \( f^{-1} \) corresponds via \( f^n \).

3: Use two inequalities:

\[
\text{span}(n, \varepsilon, f) \leq \sum_{i=1}^{k} \text{span}_i(n, \varepsilon, f) \leq k \cdot \max \text{span}_i(n, \varepsilon, f),
\]

\[
\text{sep}(n, \varepsilon, f) \geq \max \text{sep}(n, \varepsilon, f).
\]

4: Noticing two inequalities:

\[
\text{cov}(n, \varepsilon, f \times g) \geq \text{cov}(n, \varepsilon, f) \cdot \text{cov}(n, \varepsilon, g),
\]

\[
\text{sep}(n, \varepsilon, f \times g) \geq \text{sep}(n, \varepsilon, f) \cdot \text{sep}(n, \varepsilon, g).
\]

and the proof of the last assertion is similar to that of (10.13.1.23). \(\square\)

Prop. (10.13.1.26). Let \( f : X \to X \) be an expansive homeomorphism of a compact metric space of expansiveness constant \( \delta \), then \( h(f) = h_\varepsilon(f) \) for \( \varepsilon < \delta \).

Proof: For \( 0 < \gamma < \varepsilon < \delta \), we show that \( h_{2\gamma}(f) = h_\varepsilon(f) \). For this, it suffices to prove \( \leq \). By expansiveness, if \( x \neq y \), then there is some \( i \in \mathbb{Z} \) that \( d(f^i(x), f^i(y)) \geq \delta > \varepsilon \). Since the set \( \{(x, y) \in X \times X | d(x, y) \geq \gamma\} \) is compact, there is a \( k = k(\gamma, \varepsilon) \) that if \( d(x, y) \geq \gamma \), then \( d(f^k(x), f^k(y)) > \varepsilon \) for some \( |i| \leq k \). Thus if \( A \) is a \((n, \gamma)\)-separated set, then \( f^{-k}(A) \) is a \((n + 2k, \varepsilon)\)-separated set. Hence by (10.13.1.21), \( h_{2\gamma}(f) \leq h_\varepsilon(f) \). \(\square\)

Application to Ramsey Theory

Def. (10.13.1.27) [IP-System]. Let \( \mathcal{F} \) be the collection of all finite non-empty subset of \( \mathbb{N} \). For \( \alpha, \beta \in \mathcal{F} \), write \( \alpha < \beta \) if every element of \( \alpha \) is smaller than that of \( \beta \).

For a commutative group \( G \), an IP-system in \( G \) is a map \( T : \mathcal{F} \to G \) that \( T_{i_1, \ldots, i_k} = T_{i_1} \cdots T_{i_k} \).

Prop. (10.13.1.28) [Furstenberg-Weiss]. Let \( G \) be a commutative group acting minimally on a compact topological space \( X \), then for any open subset \( U \) of \( X \), \( n > 0 \) and \( \alpha \in \mathcal{F} \), and any IP-systems \( T^1, \ldots, T^n \) on \( G \), there is a \( \beta \in \mathcal{F} \) that \( \alpha < \beta \), and

\[
U \cap T^1_\beta(U) \cap \ldots \cap T^n_\beta(U) \neq \emptyset.
\]
Proof:  Cf.[Dynamic System, P49].

\textbf{Cor. (10.13.1.29).} Let \( G \) be a commutative group acting homeomorphically on a compact metric space \( X \) and \( T^1, \ldots, T^m \) be IP-systems on \( G \), then for any \( \alpha \in \mathcal{F} \) and \( \varepsilon > 0 \), there are \( x \in X \) and \( \beta > \alpha \) that \( d(x, T^i_\beta(x)) < \varepsilon \) for any \( i \).

\textit{Proof:}  Just need to find a minimal closed subset of \( X \) for \( G \), but this is easy by finite intersection theorem.

\textbf{Cor. (10.13.1.30) [Multiple Recurrence Property].} Let \( T \) be a homeomorphism of a compact metric space \( X \), then for any \( \varepsilon > 0 \) and \( q > 0 \), there are \( p > 0 \) and \( x \in X \) that \( d(T^{jq}(x), x) < \varepsilon \) for \( 0 \leq j \leq q \).

\textit{Proof:}  This is a special case of(10.13.1.29), by taking \( G = \{ T^k \} \), and \( T^i_\alpha = T^{i|\alpha|} \), where \( |\alpha| \) is the sum of elements in \( \alpha \).

\textbf{Cor. (10.13.1.31) [Generalized van der Waerden Theorem].} For each finite partition \( \mathbb{Z} = \bigcup_{i=1}^m S_k \), one of the the subset \( S_k \) contains arbitrarily long arithmetic progressions.

More generally, let \( A \) be a finite subset of \( \mathbb{Z}^d \), then for each partition \( \mathbb{Z}^d = \bigcup_{i=1}^m S_k \), there are some \( k, z_0 \in \mathbb{Z}^d \) and \( n > 0 \) that \( z_0 + na \in S_k \) for any \( a \in A \).

\textit{Proof:}  Consider the product space \( \Sigma_m = \{ 1, 2, \ldots, m \}^\mathbb{Z} \) with the 2-adic metric with shifting \( \sigma \). Then a partition of \( \mathbb{Z} \) can be viewed as an element \( \xi \in \{ 1, 2, \ldots, m \}^\mathbb{Z} \), with \( \xi_i = k \) if \( i \in S_k \).

Let \( X = \bigcup_{i=-\infty}^\infty \sigma^i(\xi) \). Let \( A_k = \{ \omega \in X | \omega_0 = k \} \), then if \( x \in A_k \), \( y \in X \) with \( d(x, y) < 1 \), then \( y \in A_k \) also. Thus for any \( q > 0 \), we can use(10.13.1.30) to show that there is an \( \omega \in X \) that \( d(\sigma^{jq}(\omega), \omega) < 1 \) for \( 0 \leq i \leq q \), thus there is an \( r \in \mathbb{Z} \) that \( \xi_j = \omega_0 \) for \( j = r, r + k, \ldots, r + pq \). And this proves the theorem.

The proof of the general case is similar.

\section{2 Symbolic Dynamics}

\textbf{Def. (10.13.2.1)[Subshifts].} A \textbf{subshift} is a closed subset \( X \subset \Sigma_m \) that is invariant under the shift \( \sigma \) and \( \sigma^{-1} \). A map between to subshifts of \( \Sigma_m \) is called a \textbf{code} if it commutes with \( \sigma \).

\textbf{Prop. (10.13.2.2).} Let \( X \) be a subshift of \( \Sigma_m \), let \( W_n(X) \) be the set of words of length \( n \) that occurs in \( X \), \( \sigma|_X \) is clearly expansive of constant 1, thus we have

\[ h(\sigma|_X) = \lim_{n \to \infty} \frac{1}{n} \log |W_n(X)|. \]

\textit{Proof:}  This is because every element in \( W_n \) appears in the first \( n \) term of some \( \omega \in X \), and elements in a set of \( d_n \)-diameter< 1 has first \( n \) entries the same. For the other direction, notice a \((n, 1)\)-separated set has the first \( n \)-entries not the same, thus contribute to different elements in \( W_n(X) \), thus \( \text{sep}(n, 1, \sigma|_X) < W_n(X) \).

\textbf{Def. (10.13.2.3)[block code].} Let \( X \) be a subshift, \( k, l \geq 0, n = k + l + 1 \), and \( \alpha \) be a map from \( W_n(X) \) to \( \{ 0, 1, \ldots, m' - 1 \} \), then a \((k, l)\)-block code is a morphism from \( X \) to \( \Sigma_{m'} \) that maps \( x \) to the sequence \( a_\alpha(x) \) that \( a_\alpha(x)_i = \alpha((x_{i-k}, \ldots, x_{i+l})) \).

When \( \{ 0, 1, \ldots, m' - 1 \} \) is chosen to be \( W_n(X) \) itself, then this is called a \textbf{higher block presentation} of \( X \).
Prop. (10.13.2.4) [Curtis–Lyndon–Hedlund]. [Every Code is a block code] Every code \( c : X \to Y \) is a block code.

Proof: Let \( \mathcal{A} \) be the symbol set of \( Y \), define \( \hat{c} : X \to \mathcal{A} : x \mapsto c(x) \). This is a continuous map, and \( X \) is compact thus it is uniformly continuous, thus there exists a \( \delta > 0 \) such that \( \hat{c}(x) = \hat{c}(y) \) if \( d(x, y) < \delta \). Thus there is a large \( k \) that \( \hat{c} \) only depends on the first \( 2k + 1 \) term, and it commutes with shifting, thus it is a block code.

Def. (10.13.2.5) [SFT]. A subshift of finite type or SFT of \( k \)-step, \( k > 0 \) is a subshift \( X \) that are defined to be the elements in \( \Sigma_m \) that doesn’t contain some set of words of length \( k + 1 \). When \( k = 1 \), this is also called a topological Markov chain.

Prop. (10.13.2.6). Every SFT is isomorphic to a vertex shift.

Proof: For this SFT \( X \) of step \( k \), construct a graph, whose vertices are \( W_k(X) \), and two element of \( W_k(X) \) are connected by an edge if they adjoint to an element in \( W_{k+1}(X) \).

Cor. (10.13.2.7). Every SFT is isomorphic to an edge shift. This is because every vertex shift can be \( 2 \)-block isomorphic to its edge shift.

Prop. (10.13.2.8) [Perron].

Sofic Shifts and Data Transmission

Def. (10.13.2.9) [Sofic Shifts]. A subshift \( X \subset \Sigma_m \) is called sofic if it is a factor of a subshift of finite type.

Prop. (10.13.2.10). A subshift \( X \subset \Sigma_m \) is sofic if it is isomorphic to an infinite path shift for some directed graph \( \Gamma \) (Notice that different edge in \( \Gamma \) can be labeled the same).

Proof: Clearly such a path shift is a factor of the edge shift of \( \Gamma \), thus it is sofic. Conversely, A sofic shift is a factor of some edge shift \( c : \Sigma_A \to X \), by (10.13.2.7), and \( c \) is a block code, by (10.13.2.3). Composing with the higher block code presentation, we may assume \( c \) is a \((0, 1)\)-block code.

3 Ergodic Theory

Prop. (10.13.3.1) [Poincaré’s Recurrence Theorem]. Let \( T \) be a measure-preserving transformation of a finite measure space \( X \), if \( A \) is a measurable set, then for a.e. \( x \in A \), there is some \( n > 0 \) that \( T^n(x) \in A \).

Proof: Let \( B \) be the set of points contradicting this property, \( B = A \setminus \cup_{k>0} T^{-k}A \), thus all the preimages \( T^{-k}B \) are disjoint, measurable and have the same measure as \( B \), thus it must has measure 0 as \( X \) has finite measure.

Cor. (10.13.3.2) [Derivave Transformation]. Given a finite measurable space and a measure-preserving map \( T : X \to X \) and a measurable subset \( A \) of finite measure, then the derivative transformation \( T_A : A \to A : x \mapsto T^k(x) \), where \( k > 0 \) is the first integer that \( T^k(x) \in A \). By Poincaré’s Recurrence theorem, the derivative transformation is defined on a subset of full measure.

Prop. (10.13.3.3). Let \( X \) be a second countable metric space and \( \mu \) a Borel probability measure on \( X \), and \( f : X \to X \) is a measure preserving continuous map, then a.e. point \( x \in X \) is recurrent, i.e. \( \text{Supp} \mu \subset \mathcal{R}(f) \).
Proof: There is a countable family of basis \( \{ U_i \} \) of nbhds of \( X \), and for each \( U_i \), elements in \( U_i \) returns to \( U_i \) except for a set \( X_i \) of measure 0. Then \( R(f) = X \setminus \bigcup_i X_i \) has full measure. \( \square \)

**Def. (10.13.3.4)[Ergodicity].** A measure-preserving transformation \( T \) is called **ergodic** if any essentially \( T \)-invariant measurable subset has measure 0 or full measure.

**Prop. (10.13.3.5).** Let \( T \) be a measure-preserving transformation on a finite measure space \( X \) and \( p \in (0, \infty] \), then \( T \) is ergodic iff every essentially \( T \)-invariant function \( f \in L^p(X, \mu) \) is constant.

Proof: \( \square \)

**Prop. (10.13.3.6).** Let \( X \) be a measure space and \( f \) is an essentially invariant function for a measure-preserving map or flow \( T \) on \( X \), then there is a strictly invariant measurable function \( \hat{f} \) that \( f = \hat{f} \) a.e..

Proof: [Dynamic System P74]. \( \square \)

**Def. (10.13.3.7).** A measure-preserving transformation or flow on a probability space \( X \) is called **mixing** if
\[
\lim_{t \to \infty} \mu(T^{-t} A \cap B) = \mu(A)\mu(B).
\]

It is called **weak mixing** if
\[
\lim_{n \to \infty} \frac{1}{n} \sum_{i=0}^{n-1} |\mu(T^{-i} A \cap B) - \mu(A)\mu(B)| = 0.
\]
or
\[
\lim_{t \to \infty} \frac{1}{t} \int_0^t |\mu(T^{-t} A \cap B) - \mu(A)\mu(B)| = 0.
\]

**Prop. (10.13.3.8).** Mixing transformation is weak mixing, and weak mixing is ergodic.

Proof: For a weak mixing transformation, if \( A \) is essentially invariant, then \( \mu(A) = \mu(A)^2 \), thus \( \mu(A) = 1 \) or 0. \( \square \)

**Prop. (10.13.3.9)[Mixing and Topological Mixing].** Let \( X \) be a compact metric space, \( T : X \to X \) be a continuous map and \( \mu \) a \( T \)-invariant Borel measure on \( X \), then
- If \( T \) is ergodic, then the orbit of a.e. point \( x \in X \) is dense in \( \text{Supp} \mu \).
- If \( T \) is mixing, then \( T \) is topologically mixing on \( \text{Supp} \mu \).

Proof: 1: Let \( U \) be an open subset intersecting \( \text{Supp} \mu \), then the \( T \)-invariant subset \( \cup_{k>0} T^{-k}U \) has full measure, thus the forward orbit of a.e. \( x \) intersect \( U \). Then take a countable open basis of \( X \), thus the forward orbit of a.e. \( x \) is dense in \( \text{Supp} \mu \).

2: Because \( \lim_{t \to \infty} T^{-t}(A) \cap B = \mu(A)\mu(B) > 0 \), so does \( \lim_{t \to \infty} A \cap T^t(B) \). \( \square \)
Ergodic Theorems

Prop.(10.13.3.10)[von Neumann Ergodic Theorem]. If \( U \in L(H) \) is unitary and \( x \in H \), then the average \( A_n x = \frac{1}{n} (x + Ux + \ldots + U^{n-1}x) \) converges to some \( Px \), where \( P \) is the projection to the fixed space of \( U \).

**Proof:** Define \( a_n = \frac{1}{n} (1 + \lambda + \ldots + \lambda^{n-1}) \) on the unit circle, and \( b(1) = \chi_\{1\} \), then if \( y = b(U)x = P(x) \), then \( ||y - A_n x||^2 = \int_{\sigma(U)} |b - a_n|^2 dE_{x,x}(\lambda) \). But this integral converges to 0 by dominated convergence theorem. \( \square \)

Prop.(10.13.3.11)[Birkhoff Ergodic Theorem]. If \( T \) is a measure-preserving transformation of a finite measure space \((X, \mu)\), and let \( f \in L^1(X, \mu) \), then the limit

\[
\overline{f}(x) = \lim_{n \to \infty} \frac{1}{n} \sum_{i=0}^{n-1} f(T^i(x))
\]

exists for a.e. \( x \) and is \( \mu \)-integrable and \( T \)-invariant, and satisfies

\[
\int_X \overline{f}(x)d\mu = \int_X f(x)d\mu
\]

In addition, if \( f \in L^2(X, \mu) \), then \( \overline{f} \) is just the projection of \( f \) to the subspace of \( T \)-invariant measures.

The same thing is true for a measure-preserving flow.

**Proof:** Let

\[
A = \{x \in X | f(x) + f(T(x)) + \ldots + f(T^k(x)) \geq 0, \ \exists k \geq 0\}. \tag{10.13.3.11}
\]

Then firstly we have \( \int_A f(x) d\mu \geq 0 \): Cf.[Dynamic System, P82]. \( \square \)

Cor.(10.13.3.12). A measure-preserving map \( T : X \to X \) in a finite measure space \((X, \mu)\) is ergodic iff for each \( f \in L^1(X, \mu) \),

\[
\lim_{n \to \infty} \frac{1}{n} \sum_{i=0}^{n-1} f(T^i(x)) = \frac{1}{\mu(X)} \int_X f(x)d\mu, \text{a.e.} \ x.
\]

I.e., the time average equals the space average for any \( L^1 \)-function.

**Proof:** If \( T \) is ergodic, then the function \( \overline{f} \) defined in(10.13.3.11) is a constant, thus the equation. Conversely, if this equation holds, then if \( f \) is \( T \)-invariant, the RHS is constant. \( \square \)

Cor.(10.13.3.13). Taking a dense subset of \( L^2(X, \mu) \) in the above corollary, we see that a measure-preserving map \( T : X \to X \) is ergodic iff for any measurable subset \( A \) and a.e. \( x \in X \),

\[
\lim_{n \to \infty} \frac{1}{n} \sum_{i=0}^{n-1} \chi_A(T^i(x)) = \frac{\mu(A)}{\mu(X)}.
\]

Invariant Measure for a Transformation

4 Hyperbolic Dynamics

5 Complex Dynamics
11 Differential Geometry

11.1 Geometric Analysis

Basic references are [Lee13], [Differential Topology Pollack](Good) and [Geometric Analysis Jost].

All manifolds in this section is assumed to be smooth over $\mathbb{R}$ or $\mathbb{C}$. Where the complex case is just the complex analytic manifold.

1 Smooth Manifolds

Def. (11.1.1.1) [Smooth manifolds].

Prop. (11.1.1.2) [Collar Neighborhood Theorem]. If $X$ is a smooth paracompact manifold with boundary, then there is a nbhd of $\partial X$ in $X$ which is diffeomorphic to the product $\partial X \times [0,1]$.

Proof: □

Prop. (11.1.1.3) [Rank Theorem]. Let $F: M \to N$ be a smooth map between manifolds of dimensions $m$ and $n$ with constant rank $r$. Then for any $p \in M$, there exists smooth charts centered at $p, F(p)$ that the coordinate representation of $F$ is

$$F(x^1, \ldots, x^r, x^{r+1}, \ldots, x^m) \mapsto (x^1, \ldots, x^r, 0, \ldots, 0).$$


Def. (11.1.1.4) [Immersion]. A smooth immersion of manifolds $f: M \to N$ is a smooth map that the differential is injective at every point.

A smooth submersion of manifolds $f: M \to N$ is a smooth map that the differential is surjective at every point.

Def. (11.1.1.5) [Local Diffeomorphism]. A local diffeomorphism $f: M \to N$ is a smooth map that for any $p \in M$, there exists an open subset $U$ that $U \to f(U)$ is a diffeomorphism.

Prop. (11.1.1.6) [Local Section Theorem]. Let $F: M \to N$ be a smooth map between smooth manifolds, then $\pi$ is a smooth submersion iff each point of $M$ is in the image of a local section of $F$.

Proof: If each point of $M$ is in the image of a local section of $F$, the differential is surjective at every point. Conversely, use the rank theorem (11.1.1.3). □

Prop. (11.1.1.7). A smooth submersion $F: M \to N$ is an open map, and a surjective smooth submersion is a quotient map.
Proof: Let $W \subset M$, and $q = \pi(p)$ where $p \in W$, then there is a local section $\sigma : U \to M$ that $\sigma(q) = p$ (11.1.1.6), thus $\sigma^{-1}(W)$ is open in $N$. But for any $y \in \sigma^{-1}(W)$, $y = \pi(\sigma(y)) \in \pi(W)$. So $p \in \sigma^{-1}(W) \subset \pi(U)$, which means $\pi(W)$ is open, and $\pi$ is an open map. The last assertion follows as any open surjective map is a quotient map (3.6.1.9).

Prop.(11.1.1.8) [Characteristic Property of Surjective Smooth Submersions]. Let $\pi : M \to N$ be a smooth submersion of manifolds, $P$ another smooth manifold, then

- Any map $F : N \to P$ is smooth iff $F \circ \pi$ is smooth.
- Any smooth map $\tilde{F} : M \to P$ that is constant on the fibers of $\pi$ induces a smooth map $F : N \to P$ that $\tilde{F} = F \circ \pi$.

Proof: 1: Use local section theorem (11.1.1.6).
2: There is a constant map $F : N \to P$ that $\tilde{F} = F \circ \pi$ by (11.1.1.7) and universal property of quotient maps, and it is smooth by item1.

Def.(11.1.1.9) [Smooth Covering Space]. A smooth covering space of a smooth manifold $X$ is a space $\tilde{X}$ together with a smooth map $\pi : \tilde{X} \to X$ that there is a covering $U_\alpha$ of $X$ that for each $\alpha$, $\pi^{-1}(U_\alpha)$ is a disjoint union of open subsets of $\tilde{X}$, each of which is mapped diffeomorphically onto $U_\alpha$.

Prop.(11.1.1.10) [Proper Free Action]. Let $\pi : E \to M$ be a smooth covering map, then with the discrete topology, $\text{Aut}_\pi(E)$ is a discrete Lie group acting smoothly, freely and properly on $E$.

Conversely, suppose $M$ is a smooth manifold and $\Gamma$ is discrete group acting smoothly, freely and properly on a manifold, then the quotient space $M/\Gamma$ is a topological manifold, and it has a unique smooth structure that the quotient map $\pi : M \to M/\Gamma$ is a smooth normal covering map.

Proof: If $\pi : E \to M$ is a smooth covering map, then the action is continuously, freely and properly by (3.11.1.28). Smoothness can be seen by applying (11.1.1.8). $\text{Aut}_\pi(E)$ is a Lie group because it is countable: Let $q \in M$, and $U$ an evenly covered nbhd of $q$, then $\pi^{-1}(U)$ is a union of open subsets each containing one element of $\pi^{-1}(q)$. So $|\pi^{-1}(q)|$ is countable, and because $\text{Aut}_\pi(E)$ acts freely, it is also countable.

Because this action is a covering map action by (3.8.1.19), (11.1.1.31) shows this is a normal covering map. The quotient space is locally Euclidean, and also Hausdorff by (3.8.1.12)(3.8.1.10), so it is a topological manifold. The smooth structure is clear.

Def.(11.1.1.11) [Smooth Embedding]. A smooth embedding of manifolds $f : M \to N$ is a smooth immersion that is also a homeomorphism onto its image.

Prop.(11.1.1.12) [Global Rank Theorem]. Let $F : M \to N$ be a smooth map of manifolds of constant tank, then:
- if it is an injection, then it is a submersion.
- if it is an surjection, then it is a submersion.
- if it is a bijection, then it is a diffeomorphism.

Proof: Cf. [Lee Smooth Manifold P83].

Prop.(11.1.1.13)[Local Embedding Theorem]. If $F : M \to N$ is a smooth morphism of manifolds, then it is a smooth immersion if it is locally a smooth embedding on the source.

Proof: Let $p \in M$, then there exists a nbhd $U_1$ of $p \in M$ that $F$ is injective. Now choose another precompact nbhd $U$ of $p$ that $\overline{U} \subset V$, then $F|_U$ is an injective map with compact domain, so it is a topological embedding by (3.6.2.11). Thus $F|_U$ is a smooth embedding.
Submanifolds

Def.(11.1.1.14)[Submanifolds]. For a smooth manifold $M$, an **embedded submanifold** $S \subset M$ is a subset $S$ that is a manifold in the induced topology together with a smooth structure that the inclusion is a smooth embedding of manifolds(11.1.1.11).

An **immersed submanifold** $S \subset M$ is a subset endowed with a topology and a smooth manifold structure that the inclusion is a smooth immersion(11.1.1.4).

An **weakly embedded submanifold** $S \subset M$ is an immersed submanifold that any smooth map $F : N \to M$ from some space $N$ that has image in $S$ is smooth as a map from $N$ to $S$.

Remark(11.1.1.15). Examples of immersed submanifolds that is not an embedded submanifolds are the 8-figure and the dense curve in a torus. However, an immerse submanifold is locally embedded on the source, by(11.1.1.13).

Def.(11.1.1.16)[Slice Charts]. Let $U \subset \mathbb{R}^n$, then a $k$-slice of $U$ is the set $S = \{(x^1, \ldots, x^n) \in U | x^{k+1} = \ldots = x^n = 0\}$.

Let $M$ be a manifold, a **slice chart** of a subset $S \subset M$ is a smooth char $(U, \varphi)$ that $\varphi(U \cap S)$ is a $k$-slice of $\varphi(U)$ for some $k$.

Prop.(11.1.1.17)[Local Slice Criterion for Embedded Submanifolds]. Let $M$ be a smooth $n$-manifold and $S$ an embedded $k$-submanifold, then each point of $S$ is contained in the domain of a slice chart. Conversely, if $S \subset M$ is a subset that each point of $S$ is contained in the domain of a slice chart, then the induced topology makes $S$ a topological manifold, and there is a smooth structure on $S$ that makes it an embedded submanifold of $M$.

*Proof:* Suppose $S$ is an embedded submanifold, then the rank theorem(11.1.1.3) shows there exists coordinates that the image of $i(S)$ is contained in a $k$-slice of $M$. Shrinking the open subset a little bit, we get a slice chart of $S$.

Conversely, if each point of $S$ is contained in the domain of a slice chart, then we can use these smooth charts to get an atlas for $S$, which makes $S$ an embedded topological submanifold of $M$. The transition maps are also smooth because they are restrictions of the corresponding transition map of $M$, so $S$ is an embedded submanifold of $M$. $\Box$

Prop.(11.1.1.18). If $M$ is a compact manifold, then any injective immersion $f : M \hookrightarrow M$ is an embedding of submanifolds.

*Proof:* The topology of $M$ is equivalent to the induced topology by(3.6.2.10). $\Box$

Prop.(11.1.1.19)[Immersed Submanifolds are Locally Embedded]. If $S \subset M$ is an immersed submanifold, then for any $p \in S$, there is a nbhd $U$ of $p \in S$ that $U \subset M$ is an embedded submanifold.

*Proof:* This follows immediately from(11.1.1.13). Notice that the topology on $U$ must be the induced topology, because it is a smooth embedding thus a homeomorphism onto its image(11.1.1.11). $\Box$

Lemma(11.1.1.20). If $i : S \hookrightarrow M$ is an immersed submanifold, if $F : N \to M$ is a smooth morphism of manifolds that has image in $S$, if $F : N \to S$ is continuous, then $N \to S$ is smooth.
Proof: Let \( p \in N \) mapping to \( q = F(p) \). By (11.1.1.19), there is a nbhd \( V \) of \( q \in S \) that \( i|_V \) is a smooth embedding. Thus there is a slice chart (11.1.1.17) \((W, \psi)\) of \( M \) that \((V_0, \sim)\) is a smooth chart for \( V \), where \( V_0 = W \cap V \) and \( \sim = \pi \circ \psi \), where \( \pi \) is the projection \( \mathbb{R}^n \rightarrow \mathbb{R}^k \) onto the first \( k \) coordinates, and also a smooth chart for \( S \).

Let \( U = F^{-1}(V_0) \) be open in \( F \), then there is a smooth chart of \( N \) contained in \( U \). Now the coordinate representation of \( F \) in the slice chart of \( S \) is just the representation of \( F : N \rightarrow M \) composed with the projection \( \pi \), so it is smooth. \( \square \)

Remark (11.1.21). \( N \rightarrow S \) being continuous is a necessary condition, otherwise consider the figure 8.

Prop. (11.1.22) [Restricting Codomain of Smooth Morphism]. If \( S \) is an embedded submanifold in \( M \), if if \( N \rightarrow M \) is a smooth that has image in \( S \), then \( N \rightarrow S \) is smooth.

Proof: Because in this case, \( S \) has the induced topology, so it is easily seen that \( N \rightarrow S \) is continuous. \( \square \)

Sard’s Theorem

Lemma (11.1.23) [Invariance of Measure Zero Sets]. If \( S \in \mathbb{R}^n \) has measure zero, then for any smooth map \( g : \mathbb{R}^n \rightarrow \mathbb{R}^m, g(S) \) has measure zero.

Thus the notion of measure zero is definable for arbitrary smooth manifolds.

Lemma (11.1.24). Cf. [Pollack Appendix A].

Def. (11.1.25). For a map of schemes \( f : X \rightarrow Y \), a point \( y \in Y \) is called critical iff \( df_x \) is not surjective, for some \( x \in f^{-1}(y) \), otherwise it is called a regular value.

Prop. (11.1.26) [Regular Value Theorem]. If \( y \) is a regular value for a map \( f : X \rightarrow Y \), then \( f^{-1}(Y) \) has a natural submanifold structure.

Proof: \( \square \)

Prop. (11.1.27) [Stack of Records Theorem]. If \( y \) is regular value of a map \( f : X \rightarrow Y \), where \( X \) is compact and \( \dim X = \dim Y \), then \( f \) is a covering map locally on \( f^{-1}(U) \) for some nbhd \( U \) of \( y \).

Proof: \( \square \)

Prop. (11.1.28) [Sard Theorem]. For a map \( X \rightarrow Y \) of smooth manifolds, the set of critical values is of measure zero \( Y \).

Proof: Cf. [Pollack Appendix A]. \( \square \)

Prop. (11.1.29) [Whitney Embedding Theorem]. Any \( k \)-dimensional manifold \( M \) can be embedded into \( \mathbb{R}^{2k+1} \).

Proof: Cf. [Pollack P51]. \( \square \)

Cor. (11.1.30) [Whitney Immersion Theorem]. Any smooth manifold \( M \) of dimension \( k \) can be immersed into \( \mathbb{R}^{2k} \).

Proof: \( \square \)
1-dimensional Smooth Manifold with Boundaries

**Prop. (11.1.1.31).** Any smooth manifold of dimension 1 with boundary is isomorphic to $[0, 1]$ or $S^1$.

*Proof:* Cf. [Pollack Appendix].

**Cor. (11.1.1.32).** The boundary of any smooth manifold of dimension 1 consists of points of even number.

**Simplifications**

**Prop. (11.1.1.33).** For every vector field $X$ and every point $X(p) \neq 0$, there exists a coordinate nbhd $(x_1, \ldots, x_{n-1}, t)$ such that $X = \frac{\partial}{\partial t}$.

2 Smooth Vector Bundles

**Def. (11.1.2.1) [Smooth Vector Bundle].** A smooth vector bundle over a smooth manifold is a vector bundle over $X$ that the trivialization maps are all smooth.

**Def. (11.1.2.2) [Smooth Fiber Bundle].**

**Lemma (11.1.2.3) [Differential in Coordinates].** Let $F: U \to V$ be a smooth map where $U \subset \mathbb{R}^n$ and $V \subset \mathbb{R}^n$, with corresponding coordinates $(x^i)$ and $(y^j)$, then

$$dF_p\left(\frac{\partial}{\partial x^i}\right|_p = \sum_j \frac{\partial F^j}{\partial x^i}(p) \frac{\partial}{\partial y^j}|_{F(p)}.$$  

*Proof:* for any smooth function $f$,

$$dF_p\left(\frac{\partial}{\partial x^i}\right|_p(f \circ F) = \sum_j \frac{\partial f}{\partial y^j}(F(p)) \frac{\partial F^j}{\partial x^i}(p) = \left(\sum_j \frac{\partial F^j}{\partial x^i}(p) \frac{\partial}{\partial y^j}|_{F(p)}\right)(f).$$

**Lemma (11.1.2.4) [Change of Coordinates].** Suppose $(U, \varphi), (V, \psi)$ be two smooth charts of a smooth manifold, and the transition function on $U \cap V$ is denoted by

$$\psi \circ \varphi^{-1}(x) = (\tilde{x}^1(x), \ldots, \tilde{x}^n(x)),$$

then (11.1.2.3) shows

$$\frac{\partial}{\partial x^i}|_p = d(\varphi^{-1})(\varphi(p)) \frac{\partial}{\partial \tilde{x}^i}(\tilde{x}(p)) = d(\varphi^{-1})(\varphi(p)) \cdot d(\psi \circ \varphi^{-1})(\varphi(p)) \frac{\partial}{\partial \tilde{x}^i}|_{\varphi(p)}$$

$$= d(\psi^{-1})(\varphi(p)) \sum_j \frac{\partial \tilde{x}^j}{\partial x^i}(\varphi(p)) \frac{\partial}{\partial \tilde{x}^j}|_{\varphi(p)} = \sum_j \frac{\partial \tilde{x}^j}{\partial x^i}(\varphi(p)) \frac{\partial}{\partial \tilde{x}^j}|_p.$$

**Def. (11.1.2.5) [Tangent Vectors].** Let $M$ be a smooth manifolds, then a tangent vector at a point $p$ is a linear maps $v : C^\infty(M) \to \mathbb{R}$ satisfying:

$$v(fg) = f(p)v(g) + g(p)v(f).$$

The set of tangent vectors at $p$ is a vector space, denoted by $T_pM$. 
Def. (11.1.2.6) [Tangent Bundle]. Let $M$ be a $n$-dimensional smooth manifold, the tangent bundle of $M$ is defined to be the set $TM = \bigsqcup T_pM$. It has a smooth manifold structure that makes it into a $2n$-dimensional manifold, and the projection $\pi : TM \to M$ is smooth. And it is a $n$-dimensional vector bundle over $M$.

Proof: Let $(U, \varphi)$ be a smooth chart of $M$, with coordinate functions $\varphi^1, \ldots, \varphi^n$, then we define a map $\tilde{\varphi} : \pi^{-1}(U) \to \mathbb{R}^{2n}$ by

$$\tilde{\varphi}(\sum v^i \frac{\partial}{\partial x^i}|_p) = (x^1(p), \ldots, x^n(p), v^1, \ldots, v^n).$$

Then for two different open subset $U, V$, the transition map is

$$\psi \cdot \tilde{\varphi}^{-1}(x^1, \ldots, x^n, v^1, \ldots, v^n) = (\bar{x}^1(x), \ldots, \bar{x}^n(x), \sum_j \frac{\partial \bar{x}^1}{\partial x^j}(x)v^j, \ldots, \sum_j \frac{\partial \bar{x}^n}{\partial x^j}(x)v^j)$$

which is clearly smooth. So this defines a smooth vector bundle over $M$, called the tangent bundle of $M$. □

Def. (11.1.2.7) [Cotangent Bundle]. The cotangent bundle $T^*M$ of a smooth manifold $M$ is the dual of the tangent bundle $TM$.

Def. (11.1.2.8) [Parallelizable manifold]. A manifold is called parallelizable iff the tangent bundle is trivial.

Vector Fields

Def. (11.1.2.9) [Smooth Vector Field]. A smooth vector field on a smooth manifold is a smooth global section of the tangent bundle $TM \to M$ (11.1.2.6).

Prop. (11.1.2.10) [Check Smoothness]. Let $M$ be a smooth manifold and $X$ be a section of the vector bundle $TM \to M$, then $X$ is a smooth vector field iff for any $f \in C^\infty(M)$, $Xf \in C^\infty(M)$.

Proof: If for any $f \in C^\infty(M)$, $Xf \in C^\infty(M)$, let $U$ be a trivializing nbhd of $M$ with coordinate functions $x^i$, then near any point $p \in U$, we can use bump function to extend $x^i$ to a smooth function on $M$. Then $X(x^i) = X^i$ near $p$, thus the coordinates of $X$ in this trivialization are all smooth, so $X$ is smooth near $p$, thus smooth everywhere.

Conversely, for any $f \in C^\infty(M)$, in a trivializing nbhd $U$ of $M$, $Xf(x) = (\sum X^i(x)\frac{\partial}{\partial x^i}|_x)(f) = \sum X^i(x)\frac{\partial f}{\partial x^i}(x)$ is smooth. □

Def. (11.1.2.11) [Pushforward of Vector Fields]. Let $F : M \to N$ be a diffeomorphism, then for any $X \in \mathfrak{X}(M)$, there exists a $Y \in \mathfrak{X}(N)$ that $dF_p(X_p) = Y_{F(p)}$.

Proof: We just define $Y_q = dF_{F^{-1}(q)}(X_{F^{-1}(q)})$, it suffices to show this a smooth vector field. But $Y : N \to TN$ is the composition

$$N \xrightarrow{F^{-1}} M \xrightarrow{X} TM \xrightarrow{TF} TN,$$

so it is smooth. □

11.1. GEOMETRIC ANALYSIS

Prop. (11.1.2.13) [Pushforward of Lie Bracket]. Let $F : M \to N$ be a diffeomorphism and $X_1, X_2 \in \mathfrak{X}(M)$, then $F_*[X_1, X_2] = [F_*X_1, F_*X_2]$ (11.1.2.11).

Proof: For any $f \in C^\infty(N)$, $F_*X_i = Y_i$, then

$$[X_1, X_2](f \circ F) = X_1X_2(f \circ F) - X_2X_1(f \circ F) = X_1((Y_2(f) \circ F) - Y_1(f) \circ F) = Y_1Y_2(f) - Y_2Y_1(f) \circ F,$$

which means exactly $F_*[X_1, X_2] = [Y_1, Y_2]$. □

Tensor Fields


3 Differential Forms

Prop. (11.1.3.1) [Frobenius Theorem]. If $X$ is an involutive distribution on a manifold $M$, then there is a unique maximal integration manifold passing through it. Where a distribution is involutive if it is closed under Lie bracket.

Proof: The key to the proof is to prove that involutive is equivalent to integrable, i.e. flat locally as $\{ \frac{\partial}{\partial x^i} \}$ for some local coordinate. Cf. [李群讲义 项武义 P226] □

Cor. (11.1.3.2). $X, Y$ in a Lie algebra commute iff their corresponding vector fields commute.

Interior and Exterior Derivatives

Lie Derivatives

Def. (11.1.3.3). The Lie bracket of two vector fields $X, Y$ is defined to be $[X, Y](f) = (XY - YX)f$, then if $X = \sum a_i \partial/\partial x_i$, $Y = \sum b_i \partial/\partial x_i$, then $[X, Y] = \sum (X(b_i) - Y(a_i)) \partial/\partial x_i$.

Lemma (11.1.3.4). $[X, Y] = \frac{\partial}{\partial t}(d(\phi_t)Y)|_{t=0}$.

Proof: For any function $f$, set $g(t, q) = \frac{\phi_t(q) - f(q)}{t}, g(0, q) = Xf(q)$. Then $g$ is differentiable (because $g(t, q) = \int_0^1 Xf(\phi_{ts}(p)) ds$, and:

$$\lim_{t \to 0} d(\phi_{-t})Yf(p) = \lim_{t \to 0} \frac{Yf(p) - Y(\phi_t(p))}{t}$$

$$= \lim_{t \to 0} \frac{Yf(p) - Yf(\phi_t p) - Y(tg(-t, \phi_t(p))}{t}$$

$$= ((XY - YX)f)(p)$$

$$= [X, Y]f(p)$$

□


Proof: Direct from the definition (11.1.3.3). □

Prop. (11.1.3.6) [Derivative formula].

$$d\omega(X, Y) = X\omega(Y) - Y\omega(X) - \omega([X, Y]).$$
Proof:

\[ L_X\omega = \iota_X(d\omega) + d(\iota_X\omega) \]

\[ \iota([X,Y]) = [L_X,\iota_Y] \]

Proof: Notice that four of them are derivatives (check because \( \iota_X(w\wedge v) = \iota_X w\wedge v + (-1)^{|w|} w\wedge \iota_X v) \). So by induction, we only has to verify them on dimension 0 and 1.

Prop. (11.1.3.8) [Stoke’s theorem].

\[ \oint \Omega d\omega = \oint_{\partial \Omega} \iota^* \omega \]

In a 3-dimensional Riemannian manifold, if we set:

\[ df = \omega_1^{\text{grad } f}, \quad d\omega_A^1 = \omega_2^{\text{curl } A}, \quad d\omega_A^2 = (\nabla A)\omega_3, \]

Then:

\[ f(y) - f(x) = \int_{l} \text{grad } f \cdot dl. \]

\[ \int_{l} A \cdot dl = \int_{S} \text{curl } A \cdot dn. \]

\[ \oint_{U} \nabla \cdot FdV = \oint_{\partial U} F \cdot ndS. \]

Proof:

Hodge Star

Def. (11.1.3.9) [Hodge Star Operator]. Given a volume-form \( \omega \) on a vector space, the Hodge star operator \( * \) is an operator from \( \bigwedge^k V \rightarrow \bigwedge^{n-k} V \) such that:

\[ \alpha \wedge (*\beta) = \langle \alpha, \beta \rangle \omega. \]

On a closed oriented Riemannian manifold, given a volume form \( \omega \), the star operator satisfies:

\[ (\alpha, \beta) = \int_M \langle \alpha, \beta \rangle \omega = \int_M \alpha \wedge *\beta. \]

And \( ** = (-1)^{p(n-p)} \) on \( \Omega^p M \).

Def. (11.1.3.10). For an operator \( d \) on \( \Omega^* M \), we define the adjoint \( d^* = (-1)^{n(p+1)+1} * d * \) on \( \Omega^p \), which satisfies the adjoint property by calculation:

\[ (d^* \alpha, \beta) = (\alpha, d\beta). \]

The laplacian \( \Delta = d^* d + dd^* \). It can be verified that \( \Delta \) commutes with \( * \) and \( d \).
4 Differential Topology

Transversality

Def. (11.1.4.1) [Transversality].

Prop. (11.1.4.2) [Transversal Stable under Perturbations]. The property of transversality for a map $f : X \to Y$ for a compact manifold $X$ to a fixed submanifold $Z$ of $Y$ is stable under smooth deformation.

Proof: We can assume the submanifold is defined by a slice, so the transversality is in fact equivalent to locally submersion in the vertical direction. Thus it is clearly stable under deformation. □

Prop. (11.1.4.3). If a smooth map $f : X \to Y$ is transversal to a submanifold $Z \subset Y$ of codimension $r$, then the preimage $f^{-1}(Z)$ is a submanifold of $X$ of codimension $r$.

Proof: Cf. [Pollack P28]. □

Cor. (11.1.4.4). If two submanifolds are transversal at every point is again a submanifold, and the codimension is the sum of them.

Prop. (11.1.4.5) [Parametric Transversality Theorem]. Suppose $N$ and $M$ are smooth manifolds, $X \subset M$ is an embedded submanifold, and $F_s$ is a smooth family of maps from $N$ to $M$. If the map $F : N \times S \to M$ is transverse to $X$, then for almost every $s$, the map $F_s : N \to M$ is transverse to $X$.

Proof: Cf. [Smooth Manifold Lee T6.35]. □

Prop. (11.1.4.6) [Transversality Homotopy Theorem]. Suppose $N$ and $M$ are smooth manifolds and $X \subset M$ is an embedded submanifold. Every smooth map $f : N \to M$ is homotopic to a smooth map $g : N \to M$ that is transverse to $X$.

Proof: Embed $M$ into an $R^k$ and take a tubular neighbourhood, then we can construct a $N \times D^k$ transversal to $M$. Cf. [Smooth Manifold Lee T6.36]. □

Prop. (11.1.4.7) [Transversality Extension Theorem]. Let $X$ is a manifold with boundary and $C \subset X$ is a closed subscheme, $Z$ is a closed submanifold of $Y$. If $f : X \to Y$ is a smooth map that is transversal to $Z$ on $C$ and transversal to $Z$ on $C \cap \partial X$, then there is a map $g : X \to Y$ that is homotopic to $f$, and $g = f$ on a nbhd of $C$.

Proof: Cf. [Pollack P72]. □

Intersection Numbers Modulo 2

Prop. (11.1.4.8) [Intersection Number Modulo 2]. Let $X$ be a compact manifold, and $Z$ is an closed submanifold of $Y$, where $\dim X + \dim Z = \dim Y$, then for any smooth map $f : X \to Y$ transversal to $Z$, define $I_2(f, Z)$ as the number of points of $f^{-1}(Z)$ modulo 2.

Prop. (11.1.4.9) [Boundary Theorem]. If $X$ is the boundary of a smooth manifold $W$, $Z$ is a closed subscheme of $Y$ that $\dim X + \dim Z = \dim Y$. If $g : X \to Y$ is a map of smooth manifolds that can be extended to $W \to Y$, then $I_2(g, Z) = 0$. 
Proof: Use extension theorem (11.1.4.7), (11.1.4.3) and (11.1.1.32).

Cor. (11.1.4.10). Let $X$ be a compact manifold, and $Z$ is an closed submanifold of $Y$, where $\dim X + \dim Z = \dim Y$, then for any smooth maps $f, g : X \to Y$ transversal to $Z$. If $f$ is homotopic to $g$, then $I_2(f, Z) = I_2(g, Z)$.

Proof: Immediate from boundary theorem (11.1.4.9).

Prop. (11.1.4.11) [Mod 2 Degree of Maps]. If $X, Y$ are manifolds of the same dimension and $X$ is compact, then $I_2(f, \{y\})$ is the same for each $y \in Y$, called the mod 2 degree of $f$. This number is 0 for the boundary of a map, by (11.1.4.9).

Proof: Cf. [Pollack P80].

Orientable Intersection Numbers

Prop. (11.1.4.12) [Preimage Orientation]. Let $X, Y$ is orientable and $Z$ is an orientable closed subscheme in $Y$. If $f : X \to Y$ is transversal to $Z$, then the orientation of $Z, Y, Z$ defines canonically an orientation on $f^{-1}(Z)$, called the preimage orientation of $f^{-1}(Z)$.

Def. (11.1.4.13) [Intersection Number]. If $X$ is an orientable smooth manifold, $Z$ is an orientable closed subscheme of an orientable manifold $Y$ that $\dim X + \dim Z = \dim Y$. If $g : X \to Y$ is a map of smooth manifolds that is transversal to $Z$, then we defined the $I(g, Z)$ to be the sum of the orientations of $f^{-1}(Z)$.

Lemma (11.1.4.14) [Boundary Theorem]. If $X$ is the boundary of an orientable compact smooth manifold $W$, $Z$ is an orientable closed subscheme of an orientable manifold $Y$ that $\dim X + \dim Z = \dim Y$. If $g : X \to Y$ is a map of smooth manifolds that is transversal to $Z$ and can be extended to $W \to Y$, then $I(g, Z) = 0$.

Proof: The same as the proof of (11.1.4.9).

Prop. (11.1.4.15). Homotopic transversal maps always have the same intersection number w.r.t $Z$.

Prop. (11.1.4.16) [Degree of Maps]. If $X, Y$ are orientable manifolds of the same dimension and $X$ is compact, then $I_2(f, \{y\})$ is the same for each $y \in Y$, called the degree of $f$. This number is 0 for a boundary map, by (11.1.4.14).

Proof: The same as that of (11.1.4.11).

Cor. (11.1.4.17). The only finite group $G$ that can act freely on $S^{2n}$ is $\mathbb{Z}/2\mathbb{Z}$ or 1.

Proof: Consider the degree map, then it is a homomorphism from $G$ to $\mathbb{Z}$, thus the image is just $\pm 1$. Now it is by Lefschetz fixed point theorem that $\deg(g) = -1$ for $g \neq 1$, thus it is injective to $\pm$.

Prop. (11.1.4.18) [General Intersection Number]. The intersection number can be generalized to the case that $g : Z \to Y$ is an arbitrary map of the complementary dimension, and we can define $I(f, g)$. Then:

- $f, g$ are transversal iff $f \times g$ are transversal to $\Delta_Y$.
- $I(f, g) = (-1)^{\dim Z}(f \times g, \Delta_Y)$. 
Cor.(11.1.4.19). If \( f' \sim f, g' \sim g \), then \( I(f, g) = I(f', g') \) if they are definable. This is because \( f \times g \sim f' \times g' \).

Prop.(11.1.4.20). \( I(f, g) = (-1)^{\dim X \cdot \dim Z} I(g, f) \). This is obvious from the definition.

Cor.(11.1.4.21). This shows that the intersection number of an odd-dimensional orientable submanifold of an orientable submanifold with itself is 0. If this fails, then the ambient space is not orientable, for example the Möbius band with the central circle.

Prop.(11.1.4.22). The Euler character of an orientable compact manifold \( Y \) equals the intersection of the diagonals \( I(\Delta, \Delta) \).

Proof: For this, we use the Poincare-Hopf theorem(11.1.4.24). It is clear that on a triangulation, we can place a source on the center of each face/edge/..., thus producing a smooth vector fields, thus it is clear the sum of their indices equals both the combinatorial Euler character and the defined character.

Cor.(11.1.4.23). The Euler character of an odd dimensional compact manifold \( Y \) is 0.

Prop.(11.1.4.24)[Poincare-Hopf Index theorem]. In a compact manifold \( M \), any vector field \( V \) with isolated zeros has sum of its index equal to \( \chi(M) \). Where the index of a singularity is the mapping degree of \( V \) on a surrounding sphere.

Proof: Should use Euler character defined in(11.1.4.22), Cf.[Pollack].

5 Flow

Def.(11.1.5.1)[Integral Curves]. Let \( V \) be a vector field over a smooth manifold \( M \), then an integral curve of \( V \) is a smooth curve \( \gamma : \Delta \rightarrow M \) that \( \gamma'(t) = V_{\gamma(t)} \) for any \( t \in \Delta \).

Def.(11.1.5.2)[Flow]. Let \( M \) be a manifold, then a flow on \( M \) is a continuous map \( \theta : D \rightarrow M \), where

- \( D \in \mathbb{R} \times M \) is an open subset.
- for any \( p \in M, D^p = \{ t | (t, p) \in D \} \) is an open interval containing 0.
- When it is defined, \( \theta(s, \theta(t, p)) = \theta(s + t, p) \).

If \( \theta \) is a flow, we define \( \theta_t(p) = \theta^{(p)}(t) = \theta(t, p) \).

If \( \theta \) is smooth, then we can define the infinitesimal generator of \( \theta \) to be the vector field \( V_p = \theta^{(p)}(0) \).

Def.(11.1.5.3)[Complete Vector Fields]. A complete vector field on a smooth manifold is a vector field that generates a global flow.

Prop.(11.1.5.4). If \( \theta : D \rightarrow M \) is a smooth flow, then the infinitesimal generator \( V \) of \( \theta \) is a smooth vector field, and each \( \theta^{(p)} \) is an integral curve of \( V \).


Prop.(11.1.5.5)[Isotopy Extension Theorem]. Let \( M \) be a manifold and \( A \) be a compact subset. Then an isotopy \( F : A \times I \rightarrow M \) can be extended to an diffeotopy of \( M \).

Proof: Consider \( F(A \times I) \subset M \times I \) is a compact set, and \( TM \times I \rightarrow M \times I \) is a vector bundle. The time lines generate a section \( F(A \times I) \rightarrow TM \times I \), so guarantees an extension \( M \times I \rightarrow TM \times I \), and because manifolds are locally compact, this section can be chosen to be compactly supported, then the flow it generates is a diffeotopy.
6 Distributions and Foliations


7 Spin Structure

Prop.(11.1.7.1) [Spin Structure Obstruction]. For a oriented real bundle, its transformation map can be chosen to be in $SO(n)$, and constitute a Cech Cohomology $H^1(X, SO(n))$, and by exact sequence of

$$0 \to \pm 1 \to \text{Spin}(n) \to SO(n),$$

this can be lifted to a $H^1(X, \text{Spin}(n))$ iff its image $w$ in $H^2(X, \mathbb{Z}/2\mathbb{Z})$ is 0. and then its inverse image will be parametrized by $H^1(X, \mathbb{Z}/2\mathbb{Z})$ (By the non-commutative spectral sequence of Čech).

We have $w = w_2$, the Whitney class, (Just need to reduce to $sk_2X$ and in this case, check they both equivalent to the bundle can be lifted). Cf.[XieYi 几何学专题]. Or we can use the Postnikov system of $BO(n)(3.10.5.2)$.

**Proof:** First prove that if $E \oplus R^n$ is spin, then $E$ is spin, and then pull $H^2(X, \mathbb{Z}/2\mathbb{Z})$ into $H^2(sk_2(X), \mathbb{Z}/2\mathbb{Z})$, this is in a injection, and the homology is natural, so we only have to prove this for $sk_2(X)$. But $E$ on $sk_2(X)$ can decompose into a $E'$ of dimension on more than 2, and for this, we see $E$ is Spin iff it is the square of another bundle, so $w$ and $w_2$ are the same. □

Prop.(11.1.7.2). For a Spin bundle $E$, the Spin-principal bundle with the Spinor representation(11.6.4.12) will generate a bundle $S$ called the **Spinor bundle**. And the Ad action of Spin($n$) on $Cl_{n,0}$ will generate a **Clifford bundle** $Cl(E)$. The Spin($n$) actions are compatible, so the Clifford bundle can act on the spinor bundle. bundle. The act of the chirality operator on the Spinor bundle will generate two half spinor bundles $S^\pm$. Then $TM$ will maps $S^\pm \to S^\mp$ for $n$ even,(because of anti-commutative with $\Gamma$).

Prop.(11.1.7.3)[Spin’-structure]. The group Spin’ is the covering space of $SO(n) \times S^1$ (n>2) that corresponds to the group of elements mod 0 mod 2 in $\mathbb{Z}_2 \times \mathbb{Z}$, i.e. Spin$(n) \times S^1/(\pm 1)$.

For example, Spin’(4) = $\{ (A_1, A_2) \in U(2) \times U(2) | \det A_1 = \det A_2 \}$, and Spin’(3) = $U(2)$.

Then a $SO(n)$ bundle can be lift to be a Spin’-bundle if the line bundle determined by $S^1$ is determine the same $w_2$ as it, i.e. $w_2 = c_1(L)$ mod 2. This is equivalent to $w_2$ is in the image of $H^2(X, \mathbb{Z})$, and this is equivalent to the Bockstein image of it is zero.

Use a variant of Wu’s formula: $w_2(TM)[\alpha] = \alpha \cdot \alpha (mod 2)$ for $M$ orientable of dimension 4, we have any orientable manifold of dimension 4 has a Spin’-structure. Cf.[XieYi 几何学专题 Homework3].

There is a connection on the Clifford bundle and on the Spinor bundle induced by the Levi-Civita connection of $M(11.2.3.2)$. This is compatible with the Clifford action. and it is also metric because the connection 1-form is in $\mathfrak{so}(n)$ because the action of $SO(n)$ preserves metric.

8 Young-Mills Euqation & Seiberg-Witten Equation

Def.(11.1.8.1) [Yong-Mills]. The Young-Mills functional on connections $A$ on a bundle $E$ on a compact oriented space:

$$YM(A)^2 = \| F_A \|^2 = - \int_X \tr(F_A \wedge *F_A)$$

it is a critical point when $d_A * F_A = 0$ and $d_A F_A = 0$. 

Prop. (11.1.8.2)[2-dim Case]. ∗F ∈ Ω^0(su(E)) is parallel thus its characteristic spaces is orthogonal and a stable under parallel transport. So an irreducible YM SU(2)-connection must by flat, thus correspond to irreducible SU(2) representation of π_1(X).

Prop. (11.1.8.3)[4-dim Case]. ** = (−1)^{2g^2} = id on Ω^2(E) on E a SU(n)-bundle, so Ω^2(E) = Ω^+ ⊕ Ω^-.

Weizenbock Formula.

Prop. (11.1.8.4)[Anti-Instanton Connection on Complex Line Bundle].

Prop. (11.1.8.5)[Anti-Instanton Connection on Complex Line Bundle]. For a U(1)-bundle, d_A F_A = dF_A, so F_A is harmonic, thus c_1(L) = [\frac{1}{2\pi i} F_A] ∈ H^2(X, Z) ∩ H^2(X, R), In fact, this is equivalent to the existence of a anti-self-dual connection on this bundle.

Lemma (11.1.8.5)[Weizenbock Formula]. On a Riemannian manifold M, the Laplace operator has the form:

\[ \Delta = -\nabla^2_{\xi_i} - \delta^i \wedge \iota(e_j) R(e_i, e_j) \]

where \( \nabla^2_{X,Y} = \nabla_X \nabla_Y - \nabla_{X,Y} \).

If M is a spin manifold, then the Dirac operator D satisfies:

\[ D^2 = -\nabla^2_{\xi_i} + \frac{1}{4} R \]

where R is the scalar curvature form on M. If M is a Spin^c manifold with a Spin^c connection \( \nabla_A \), then the Dirac operator satisfies

\[ D^2_A = -\nabla^2_{\xi_i} + \frac{1}{4} R + \frac{1}{2} F_A \]

Cf.[Geometric Analysis Jost P143,153].

Prop. (11.1.8.6)[Seiberg-Witten]. The Seiberg-Witten equation functional for a unitary connection A on the determinant bundle of a Spin^c structure of M and a section of \( S^+ \) is:

\[ SW(\varphi, A) = \int \left( |\nabla_A \varphi|^2 + |F_A^+|^2 + \frac{R}{4} |\varphi|^2 + \frac{1}{8} |\varphi|^2 \right) Vol. \]

\[ = \int \left( |D_A \varphi|^2 + |F_A^+|^2 - \frac{1}{4} (e_j e_k \varphi, \varphi) e^j \wedge e^k |^2 \right) Vol \]

So the Seiberg-Witten equation is the lowest topological possible value of the Seiberg-Witten functional. It writes:

\[ D_A \varphi = 0, \quad F_A^+ = \frac{1}{4} (e_j e_k \varphi, \varphi) e^j \wedge e^k. \]

Cf.[Jost Chapter 7].
Cor. (11.1.8.7). If a compact oriented Spin\(^c\) manifold \(M\) has nonnegative scalar curvature, then the only possible solution is \(\varphi = F^+_A = 0\). (See from the equivalence of forms of Seiberg-Witten functional.)

9 Chern-Weil Theory

Prop. (11.1.9.1) [Chern-Weil]. An Invariant polynomial of \(M_n(k)\) is one that is invariant under the conjugation action (2.2.19).

For any connection on \(E\), the Chern-Weil map \(CW\) from invariant polynomial ring to \(H^*(X): P \mapsto |P(\Omega)|\) is a ring homomorphism independent on the connection \(A\).

There are relations between \(c_i\) and \(\text{tr}(\Omega^k)\), they can be derived formally by considering diagonal elements.

Proof: To prove \(P(\Omega)\) is closed, notice by (2.2.19), it suffice to show \(\text{tr}(\Omega^k)\) is closed. By (11.2.3.7),
\[
d\text{tr}(\Omega^k) = \text{tr}(\omega \wedge \Omega^k - \Omega^k \wedge \omega) = 0,
\]
which is zero because \(\Omega\) is of even dimension.

For the independence of connections, use (3.10.3.28). For two connection \(\nabla_i, \nabla = t\nabla_0 + (1 - t)\nabla_1\) (you can smooth it) is a connection on the vector bundle \(\pi^*E\) on \(M \times I\), and the section 0 and 1 induces the connection \(\nabla_0\) and \(\nabla_1\). Thus \(s^*_0\) and \(s^*_1\) are the same map, thus \(CW_M(p) = s^*_iCW_{M \times I}(p)\) are all the same map. □

Cor. (11.1.9.2). For a complex line bundle of degree \(r\) over a complex manifold,
\[
det(1 - \frac{1}{2\pi i} F_A) = 1 + c_1 + \ldots + c_r
\]
gives out the Chern class, because it satisfies the axioms of Chern class (3.11.4.16). In other words, \(c_k = \text{tr}((-\frac{1}{2\pi i} F_A)^k)\).

For a real line bundle of degree \(r\),
\[
det(1 - \frac{1}{2\pi i} F_A) = 1 + p_1 + \ldots + p_{[\frac{r}{2}]}
\]
gives out the Pontryagin class, where \(p_k \in H^{4k}(X)\). (Notice the \(\omega\) thus \(\Omega\) can be chosen to be skew-symmetric, thus for odd \(k\) the classes \(\text{tr}(\Omega^k)\in H^{2k}(X)\) vanish).

For an oriented real bundle of degree \(2r\), the \(\omega\) and thus \(\Omega\) can be chosen to be skew-symmetric and the transformation matrix in \(SO(2r)\), then
\[
Pf(\frac{1}{2\pi i} \Omega) \in H^{2r}(X)
\]
is well-defined and closed and gives the Euler class \(e(E)\) (recall \(e(E)^2 = p_r(E)\)). (Use \(Pf^2 = \det\) to get that \([\frac{\partial Pf}{\partial \Omega_{ij}}]^t\) commutes with \(\Omega\), then calculate \(dPf(\Omega) = 0\)).

Proof: In fact, the construction is natural w.r.t the connection because connection can be pulled back and summed. Then the only task is the normality, which is direct calculation on \(\mathbb{CP}^1\). □

Cor. (11.1.9.3).
\[
c_1(E) = c_1(\wedge^{\dim E} E).
\]

Direct from the formula.
Cor. (11.1.9.4) [Whitney Product Formula].

\[ c(E \oplus F) = c(E)c(F), \quad p(E \oplus F) = p(E)p(F) \]

Directly form the product connection on \( E \oplus F \).

Prop. (11.1.9.5) [Chern Character]. The Chern character

\[ ch(E) = \left[ \text{tr} \exp \left( i \frac{2\pi}{2} F \right) \right] \]

satisfies \( ch(E \oplus F) = ch(E) + ch(F) \) and \( ch(E \otimes F) = ch(E)ch(F) \) by simple calculation. So it defines a ring homomorphism from \( K(X) \) to \( H^*(X) \).

Prop. (11.1.9.6) [Chern-Gauss-Bonnet]. For a 2n-dimensional orientable manifold \( M \),

\[ \int_M e(TM) = \chi(M). \]

Prop. (11.1.9.7). For a vector bundle and a flat connection \( d_A \) on a manifold, i.e. \( d_A^2 = 0 \), we have a deRham like cohomology, and there is a sheaf of flat sections.

\[ H^*(X, A) = H^*(X, E). \]

10 Index Theorems (Atiyah-Singer)

References are [Heat equation and the Index Theorem Atiyah] and [Index Theorem].

Prop. (11.1.10.1) [Gilkey]. For a natural transformation \( \omega \) from the functor \( p : M \rightarrow \) the Riemannian structure on \( M \) to the functor \( q : M \rightarrow k \)-forms on \( M \), if it is homogenous of weight 0 w.r.t to metric \( g \) (i.e. \( \omega(\lambda^2 g) = \omega(g) \)) and in local coordinates it has the coefficients of \( \omega(g) \) generated by \( g_{ij} \) and \( \det g^{-1} \) and their derivatives, then is is a polynomial of Pontryagin classes of the given dimension. (not only up to homology).

\[ Proof: \] Cf. [Heat equation and the Index Theorem Atiyah P284]. \( \square \)

Prop. (11.1.10.2) [Gilkey Generalized]. For a natural transformation \( \omega \) from the functor \( p : M \rightarrow \) Riemannian structures on \( M \) with a Hermitian bundle \( E \) with a Hermitian connection and the functor \( q : M \rightarrow k \)-forms on \( M \), if it is homogenous of weight \((0, 0)\) w.r.t to metric \( g, h \) and the Hermitian structure (i.e. \( \omega(\lambda^2 g, \mu^2 \xi) = \omega(g, \xi) \)) and in local coordinates it has the coefficients of \( \omega(g, \xi) \) generated by \( g_{ij}, h_{ij}, \det h^{-1}, \det g^{-1} \) and \( \Gamma^j_k \) (the connection form) and their derivatives, then is is a polynomial of Pontryagin classes and Chern classes of \( E \) of the given dimension. (not only up to homology).

\[ Proof: \] Cf. [Heat equation and the Index Theorem Atiyah P290]. \( \square \)

Cor. (11.1.10.3). For a natural transformation \( \omega \) from the functor \( p : M \rightarrow \) Hermitian bundle \( E \) on \( M \) with a Hermitian connection and the functor \( q : M \rightarrow k \)-forms on \( M \), if it is homogenous of weight 0 w.r.t to metric \( h \) and the Hermitian structure (i.e. \( \omega(\mu^2 \xi) = \omega(\xi) \)) and in local coordinates it has the form \( \omega(g, \xi) \) generated by \( h_{ij}, \det h^{-1} \) and \( \Gamma^j_k \) (the connection form) and their derivatives, then is is a polynomial of Chern classes of \( E \) of the given dimension. Because when composed with the forgetful functor, it gives a transformation as above. And it is obviously independent of \( g \).
Prop.(11.1.10.4)[Hodge]. For any differential operator \( A \) from a vector bundle \( E \) to a vector bundle \( F \), we form two operators \( AA^* \) and \( A^*A \), then they are both self adjoint elliptic operators, let these corresponding eigenspace be \( \Gamma_\lambda(E) \) and \( \Gamma_\lambda(F) \), then \( A \) and \( A^* \) define an isomorphism between \( \Gamma_\lambda(E) \) and \( \Gamma_\lambda(F) \).

Proof:

Prop.(11.1.10.5)[Hirzebruch Signature Formula]. On a \( 4n \)-dimensional orientable manifold \( M \), the Poincare duality defines a bilinear pairing \( H^{2n}(M) \times H^{2n}(M) \to \mathbb{R} \), its signature \( \sigma(M) \) is given by:

\[
\sigma(M) = \int_M L_n(p_1, \ldots, p_n).
\]

Where \( L_n \) is the degree \( n \) part of the Taylor expansion of \( \prod_{i=1}^r \frac{\sqrt{x_i}}{\tanh \sqrt{x_i}} \) in terms of the symmetric polynomial.

Proof: We consider the operator \( \tau : \alpha \mapsto i^{l+p(p-1)} \alpha, \tau^2 = 1 \), thus \( \Gamma^* \) is decomposed into two eigenspaces of \( \tau \). We define the signature operator \( A \) as the restriction of \( \Delta = d - \tau d\tau \) to \( \Gamma^+ \). \( \Delta \) anti commutes with \( \tau \) thus maps \( \Omega^+ \) to \( \Omega^- \), then we have \( \ker A = \ker \Delta \cap \Omega^+ \), which is the positive harmonic forms \( H^+ \). So

\[
\text{Ind} A = \dim H^+ - \dim H^-.
\]

And we notice the positive and negative harmonic forms neutralize each other unless on the \( 2n \)-forms, so only need to consider them. In fact, if we consider \( 4n + 2 \) manifolds, then \( \tau \) is pure imaginary and the conjugation neutralize even the \( 2n + 1 \) forms, so there are no signature.

Now the inner product \( \alpha \to \int \alpha \wedge *\alpha \) is positive definite for a real form \( \alpha \), so this index of \( A \) is just the signature of the intersection form defined by cup product.

Cor.(11.1.10.6). For a \( 4n \)-dimensional \( M \) which is a boundary of a manifold, its signature is 0.

Proof: By Stokes theorem, if \( M \) is a boundary of a manifold, then all its Pontryagin numbers, i.e. \( \int_M \prod p_i^{n_i}, \sum n_i = n \), vanish.

Prop.(11.1.10.7)[Generalized Hirzebruch Signature Formula]. Let \( M \) be a \( 2l \) dimensional smooth manifold and \( E \) be a Hermitian bundle over \( M \), then The index of the generalized signature operator is giving by

\[
\text{Ind} A_\eta = 2^l \cdot ch(E) L(p_1, \ldots, p_l).
\]

where \( L(M)(p_i) = \prod \frac{x_i/2}{\tanh x_i/2} \).

Prop.(11.1.10.8)[Hirzebruch-Riemann-Roch]. For a \( n \)-dimensional complex line bundle \( L \) over a compact Kähler manifold \( M \),

\[
\chi(M, L) = \int_M [ch(E) \td(T^{1,0}M)]_n.
\]

Where \( \chi(M, L) = \sum_{q=0}^n (-1)^q \dim H^q(M, E) \), \( ch \) is the Chern character(11.1.9.5) and \( \td(T^{1,0}M) \) is the Todd polynomial, i.e. Taylor expansion of \( \prod_{i=1}^r \frac{t_i}{1 - e^{-t_i}} \) in terms of the symmetric polynomial, applied to \( c_i(T^{1,0}M) \).
Cor. (11.1.10.9)[Riemann-Roch]. For a $n$-dimensional complex vector bundle $E$ over a Riemann Surface $M$, let $\deg E = \int_M c_1(E)$, then
\[
\chi(M, E) = H^0(M, E) - \dim H^1(M, E) = \deg E + \text{rk}(E)(1 - g).
\]
Cf.[Index Theorem P115].

Hodge Theory

Prop. (11.1.10.10)[Hodge]. By (10.11.8.12), if we investigate the Laplace operator $\Delta_d$ on a compact orientable Riemannian manifold, we get that
\[
\Omega^i = \mathcal{H}^i \oplus \text{Im} \Delta_d = \mathcal{H}^i \oplus \text{Im} d \oplus \text{Im} d^*.
\]
Thus $\mathcal{H}^i$ can be uniquely represented by elements of $\mathcal{H}^i$.

Proof: It suffice to prove $\Delta_d$ is self-adjoint elliptic.

$\text{Im} \Delta_d \subset \text{Im} d \oplus \text{Im} d^*$, and the result follows if we show $\mathcal{H}^i, \text{Im} d, \text{Im} d^*$ are orthogonal. In fact, let $\omega$ be harmonic, then $(\omega, d^* \xi) = (d\omega, \xi) = 0$, $(\omega, d\eta) = (d^* \omega, \eta) = 0$, $(d\eta, d^* \xi) = (dd\eta, \xi) = 0$. □

Cor. (11.1.10.11)[Poincare Duality for deRham Cohomology]. If $M$ is a $n$-dimensional oriented Riemannian manifold, then
\[
H^p_{dR}(M) \cong H^{n-p}_{dR}(M)
\]
Induced by $\ast$, because $\ast = \pm 1$ and $\ast$ commutes with $\Delta_d$ (11.1.3.10), so it induce an isomorphism $\mathcal{H}^p \cong \mathcal{H}^{n-p}$.

Moreover, $\ast$ in fact induces a perfect pairing:
\[
H^k_{dR}(M) \times H^{n-k}(M) \to \mathbb{R}
\]
induced by the map
\[
\ast : \mathcal{H}^k(M) \times \mathcal{H}^{n-k}(M) \to \mathbb{R} : (\alpha, \beta) \mapsto \int_M \alpha \wedge \ast \beta
\]
As $\int_M \alpha \wedge \ast \alpha = ||\alpha||^2 \neq 0$.

Prop.(11.1.10.12). On a compact complex manifold, the formal adjoint of $\overline{\partial}$ is $\ast \partial \ast$. (By direct calculation). Also $d^* = (-1)^{n(p+1)+1} \ast d \ast = - \ast d \ast$.

Prop. (11.1.10.13)[Hodge]. Given a compact Hermitian complex manifold $(X, J, g)$ and a holomorphic line bundle $E$ over it, there is a Hermitian metric on $A^{p,q} E$, and an operator $\overline{\partial}$ on it. Then $\overline{\partial}$ has a formal adjoint $\overline{\partial}^*$, and $\Delta_{\overline{\partial} E}$ can be defined. Let $\mathcal{H}^p_{E}$ be the kernel of $\Delta_{\overline{\partial} E}$ on $A^{p,q} E$, called the $E$-valued $(p, q)$-forms, then there is a orthonormal decomposition
\[
A^{p,q} E = \mathcal{H}^{p,q}_{E} \oplus \text{Im} \Delta_{\overline{\partial} E} = \mathcal{H}^{p,q}_{E} \oplus \text{Im} \overline{\partial} E \oplus \text{Im} \overline{\partial}^* E
\]
And thus $H^{p,q}(X, E) \cong H^{p,q}_{\overline{\partial} E}(X, E)$.

Proof: It suffice to prove $\Delta_{\overline{\partial} E}$ is self-adjoint elliptic. The rest is verbatim as the proof of(11.1.10.10). □

Cor. (11.1.10.14)[Hodge]. In case $E = \mathcal{O}_X$, $\mathcal{H}^{p,q}(X) \cong H^{p,q}_{\overline{\partial} E}(X)$.

Cor. (11.1.10.15)[Kodaira-Serre Duality]. For a Hermitian line bundle over a compact Hermitian complex manifold $X$, from Hodge theorem and (11.7.5.2), we get
\[
H^p(X, \Omega^q(E)) \cong H^{n-p}(X, \Omega^{n-q}(E^*))
\]
induced by $\overline{\partial}$ and $\overline{\partial}^*$. 

11 Knots and Links

Prop. (11.1.11.1) [Linking Number]. For two knots $A, B$ in $\mathbb{R}^n$, we can choose a $D \cong D^2$ with boundary $A$, then define their linking number as the intersection number of $D$ with $B$.

This can be extended to higher dimensions.
11.2 Riemannian Geometry

Basic references are [Riemannian Geometry Do Carmo], [Geometric Analysis Jost] and [Differential Geometry Loring Tu].

1 $\mathbb{R}^3$-Geometry

Different Coordinates

Prop. (11.2.1.1). In a polar coordinate,

$$g_{11} = 1, g_{12} = 0, g_{22} = |\frac{\partial f}{\partial \theta}|^2, \quad K = -\frac{(\sqrt{g_{22}})_{\rho \rho}}{\sqrt{g_{22}}}$$

And $\sqrt{g_{22}} \sim \rho$. (Use the formula relating Jacobi Field with curvature)

Moving Frame Method

Prop. (11.2.1.2)[Theorema Egregium].

$$R_{1212} = K(g_{11}g_{22} - g_{12}^2)$$

Which is a special case of the definition of curvature.

Prop. (11.2.1.3)[Gauss-Bonnet]. Let $M$ be a compact oriented 2-dimensional Riemannian manifold, then

$$\chi(M) = \frac{1}{2\pi} \int_M K \text{Vol.}$$

Proof: Should be an direct corollary of (11.1.9.6). \hfill \Box

Topology and Geometry

Prop. (11.2.1.4). Every compact orientable surface of genus $p > 1$ can be provided with a metric of constant negative curvature.

Remark (11.2.1.5)[Hilbert Theorem]. There exist complete surfaces with $K \leq 0$ in $\mathbb{R}^3$, but the hyperbolic surface cannot be immersed into $\mathbb{R}^3$.

2 Basics

Prop. (11.2.2.1). If the metric tensor on the tangent space is $g$ in a coordinate, then it is $g^{-1}$ in the cotangent space. (Follows from??).

3 Connections

Def. (11.2.3.1)[Affine Connection]. An affine connection on a vector bundle $E$ is a map $D : \Gamma(E) \to \Gamma(E) \otimes \Gamma(TM)$ that satisfies differential-like properties, it can be written as $D = d + \omega$, with $\omega \in \Omega^1(\text{End}(E))$. 
Def. (11.2.3.8) [Christoffel Symbol]. The Christoffel symbol of a connection is defined by the equations: $\nabla_X X_j = \sum_k \Gamma^k_{ij} X_k$.

The geodesic equations is $\frac{D}{dt} \left( \frac{dx^i}{dt} \right) = \nabla_k x^i = 0 \quad \forall k$.

Def. (11.2.3.9). The torsion tensor of a connection $\nabla$ on $TM$ is defined as $T(X,Y) = \nabla_X Y - \nabla_Y X - [X,Y]$. The connection is called torsion-free if $T = 0$. This is equivalent to $\Gamma^k_{ij} = \Gamma^k_{ji}$.

A connection is called metric if it preserves metric. i.e. $\nabla g = 0$.
Proof: $T$ is a tensor because it is skew-symmetric, and

$$T(fX,Y) = f\nabla_X Y - f\nabla_Y X - df(Y)X - (f[X,Y] - df(Y))X = fT(X,Y),$$

where (11.1.3.5) is used.

**Prop. (11.2.3.10).** If $\nabla$ is torsion-free connection on $TM$, then its induced connection on $T^*M$ satisfies

$$(da)(v_1,\ldots,v_k) = \sum (-1)^i (D_{v_i}a)(v_1,\ldots,\hat{v_i},\ldots,v_k).$$

**Proof:**

**Def. (11.2.3.11) [Curvature Tensor].** The curvature of a (affine) connection $d_A$ is $F_A = d_A \circ d_A \in \Omega^2(\text{End}(E))$. The curvature tensor it induced is

$$F_A(Z)(X,Y) = R(X,Y)Z = D_Y D_X Z - D_X D_Y Z + D_{[X,Y]}Z.$$  

In particular, the curvature depends only on the point, and locally $F_A = d\omega + \omega \wedge \omega$

In two coordinates $e = ea$ for $a : U \to GL(r, \mathbb{R}), F_A = a^{-1} F_A a$.

The connection is called **flat** if $F_A = 0$.

**Prop. (11.2.3.12) [Flat coordinate].** A connection on $TM$ assumes near every point a flat coordinate, i.e. $\nabla(\partial/\partial x^i) = 0$, iff it is flat and torsion-free.

**Proof:** One side is easy because its Christoffels vanish. On the other side, use integrability theorems (10.11.6.2). Cf.[Jost P115].

**Prop. (11.2.3.13).**

$$\Delta \langle \varphi, \varphi \rangle = 2(\langle D^* D \varphi, \varphi \rangle - \langle D \varphi, D \varphi \rangle).$$

**Proof:** Cf.[Jost P118].

**Prop. (11.2.3.14).** For a flat connection, there is a bundle isomorphism (Gauge transform) that transforms $d_A$ into natural $d$.

**Proof:** Because $d_A g(s) = g d_A (g^{-1}(s)), d_A = d - dg \cdot g^{-1} + g \cdot \omega \cdot g^{-1}$. Solve this PDE direvtly. (Cf.[Topics in Geometry Xie Yi week3]).

**Cor. (11.2.3.15).** For a flat connection, by (11.2.3.14), the parallel transportation only depends on the homotopy type of the loop, thus gives an action of $\pi(X)$ on $SO(T_p(X))$ (or $SU(T_p(X))$. (because it is locally constant).

In this way, connections module gauge equivalence (preserving matric) equals representation of $\pi(X)$ module conjugations. The reverse map is giving by principal bundle.

**Proof:**
Levi-Civita Connection

**Def. (11.2.3.16) [Levi-Civita Connection].** The Levi-Civita connection is the unique connection on $M$ that is metric and torsion-free:

$$X(Y, Z) = \langle \nabla_X Y, Z \rangle + \langle Y, \nabla_X Z \rangle, \quad \nabla_X Y - \nabla_Y X = [X, Y].$$

It satisfies:

$$\langle Z, \nabla_Y X \rangle = \frac{1}{2} \left( X(Y, Z) + Y(Z, X) - Z(X, Y) - \langle [X, Z], Y \rangle - \langle [Y, Z], X \rangle - \langle [X, Y], Z \rangle \right).$$

Then

$$\Gamma^m_{ij} = \frac{1}{2} \sum_k \{g_{jk,i} + g_{ki,j} - g_{ij,k} \} g^{km}$$

Thus geodesic is a solution that only depends on the metric (11.2.3.8), so a local isometry preserves geodesics.

**Prop. (11.2.3.17).** Now the Lie derivative has the form:

$$L_X(S)(Y_1, \ldots, Y_p) = \nabla_X(S)(Y_1, \ldots, Y_p) + \sum_{i=1}^p S(Y_1, \ldots, Y_{i-1}, \nabla_{Y_i}X, \ldots, Y_p).$$

The exterior derivative $d$ and its adjoint $d^*$ has the form:

$$d\omega(Y_i) = \sum (-1)^p \nabla_{Y_i} \omega(\tilde{Y}_p), \quad d^*\omega(Y_i) = -\sum \nabla_{e_i} \omega(e_j, Y_i)$$

where $e_i$ is an orthonormal basis. Cf. [Jost P140].

**Prop. (11.2.3.18) [Covariant Differential Symmetry].** For a parametrized surface: $s : (u, v) \to M$,

$$\frac{D}{\partial u} \frac{\partial s}{\partial v} = \frac{D}{\partial v} \frac{\partial s}{\partial u}.$$

Proof:

$$\frac{D}{\partial u} \frac{\partial s}{\partial v} = \frac{D}{\partial u} \left( \sum \frac{\partial s_i}{\partial v} X_i \right) = \frac{\partial^2 s_i}{\partial u \partial v} + \sum \frac{\partial s_i}{\partial v} \left( \sum \frac{\partial s_j}{\partial u} \nabla_j X_i \right) = \frac{\partial^2 s_i}{\partial u \partial v} + \sum \frac{\partial s_i}{\partial v} \frac{\partial s_j}{\partial u} \nabla_j X_i$$

But now the Levi-Civita connection is symmetric, thus $\nabla_j X_i = \nabla_i X_j$, showing the symmetry in $u$ and $v$. □

**Lemma (11.2.3.19) [Gauss].** Let $p \in M$ and $v \in T_p M$ s.t. $\exp_p v$ is defined, $w \in T_p M$, then

$$\langle (d\exp_p)_v(w), (d\exp_p)_v(w) \rangle = \langle v, w \rangle.$$

Proof: Cf. [Do Carmo P69]. □

**Prop. (11.2.3.20) [Geodesic Locally Minimizing].** In a normal nbhd of $p$, the geodesic starting at $p$ is the minimal line.
11.2. RIEMANNIAN GEOMETRY 1067

Proof: And curve \( c(t) \) can be written as \( \exp_p(r(t)v(t)) = f(r(t), t) \), where \( f(s, t) = \exp_p(sv(t)) \), so by Gauss lemma, \( \langle \frac{\partial f}{\partial r}, \frac{\partial f}{\partial t} \rangle = 0 \). Now \( dc/dt = \partial f/\partial r r'(t) + \partial f/\partial t \), so

\[
|dc/dt|^2 = |r'(t)|^2 + |\partial f/\partial t|^2 \geq |r'(t)|^2.
\]

Integrate this will give us the desired result. \( \square \)

**Prop. (11.2.3.21)** [Totally normal nbhd]. For any point \( p \), there exists a nbhd \( W \) and a number \( \delta > 0 \) s.t. for every \( q \in W \), \( \exp_q \) is a diffeomorphism on \( B_\delta(0) \) and \( \exp_q(B_\delta(0)) \supset W \). Thus, fine cover exists in every smooth manifold, because Riemannian metric exists on these manifolds.

**Proof:** Cf.[Do Carmo P72]. \( \square \)

- **(Geodesic Frame)** In a neighborhood of every point \( p \), there exists \( n \) vector fields, orthonormal at each point, and \( \nabla_{E_i} E_j(p) = 0 \). (Choose normal nbhd and parallel a orthonormal basis to every point. (WARNING: this is not a flat coordinate, it only helps when dealing with point-wise properties).

**Def. (11.2.3.22)** [Killing Fields]. A **Killing field** is a vector field which generates an infinitesimal isometry. \( X \) is killing \( \iff L_X g = 0 \iff \langle \nabla_Y X, Z \rangle + \langle \nabla_Z X, Y \rangle = 0 \) for all \( Y, Z \), which is called the **Killing equation**.

**Proof:** Use Lie formula,

\[
L_X(g(Y, Z)) = X(Y, Z) - \langle [X, Y], Z \rangle - \langle Y, [X, Z] \rangle
\]

and Levi-Civita connection is torsion-free. \( \square \)

**Prop. (11.2.3.23).** Let \( M \) be a compact Riemannian manifold of even dimension with positive sectional curvatures, then every Killing field on \( M \) has a singularity.

**Proof:** Cf.[Do Carmo P104]. \( \square \)

**Def. (11.2.3.24)** [Geometric Differential Notions].

- The **gradient** is defined to be \( \langle \nabla f(p), X \rangle = X(f)(p) \).
- The **divergence** is defined to be \( \text{div}X(p) = \text{trace of the linear map } Y(p) \to \nabla_Y X(p) = \sum_i \langle \nabla_{E_i} X, E_i \rangle \). It measures the variation of the volume and it depends only on the point.
- The **Hessian** is defined to be \( \text{Hess} f \) is a self-adjoint operator that \( (\text{Hess} f)Y = \nabla_Y \nabla f \) as well as a symmetric form \( (\text{Hess} f)(X, Y) = \langle (\text{Hess} f)X, Y \rangle \).
- The **Laplacian** is defined to be \( \Delta f = \text{div} \nabla f = \text{trace Hess} f \).

**Prop. (11.2.3.25).** In a geodesic frame,

\[
\nabla f(p) = \sum_{i=1}^n (E_i(f)) E_i
\]

\[
\text{div}X(p) = \sum_{i=1}^n E_i(f_i)(p), \text{where } X = \sum_i f_i E_i.
\]

\[
\Delta f = \sum_i E_i(E_i(f))(p).
\]
Cor. (11.2.3.26). \[ \Delta(f \cdot g) = f\Delta g + g\Delta f + 2\langle \text{grad} f, \text{grad} g \rangle, \]
because these only depends on the point.

Prop. (11.2.3.27). \[ d(i(X)m) = (\text{div}X)m. \] where \( m \) is the volume form.

Proof: Choose a geodesic frame \( E_i, \theta_i \) is a dual form of \( E_i \), let \( X = \sum f_i E_i \), then
\[ d(i(X)m) = \sum (-1)^{|i|+1}f_i \theta_i, \]
so
\[ \sum (-1)^{|i|+1}d f_i \wedge \theta_i + \sum (-1)^{|i|+1}f_i \wedge d \theta. \]
Notice that \( d \theta_i = 0 \), because \( d \theta_k(E_i, E_j) = E_i \theta_k(E_j) - E_j \theta_k(E_i) - \theta_k([E_i, E_j]) = 0 \).

Prop. (11.2.3.28) [Hopf theorem]. If \( f \) is a differentiable function on a compact orientable manifold with \( \Delta f \geq 0 \), then \( f \) is constant.

Proof: Let \( \text{grad}(f) = X \), then
\[ \int_M \Delta f dm = \int_M \text{div}(X)dm = \int_M d(i(X)dm) = 0. \]
So \( \Delta f = 0 \). Now
\[ 0 = \int_M \Delta(f^2/2)dm = \int_M f\Delta fdm + \int_M \|\text{grad}(f)\|^2 dm \]
by (11.2.3.26), thus \( \text{grad}(f) = 0 \), so \( f \) is constant.

Def. (11.2.3.29) [Riemannian Curvatures].
- The sectional curvature \( K(X, Y) = \frac{\langle R(X,Y)X,Y \rangle}{|X\wedge Y|^2} \).
- The Ricci curvature \( \text{Ric}(x) = \text{Ric}(x, x) \), where \( \text{Ric}(x, y) \) is the symmetric form of \( 1/n \) of trace of the map \( z \rightarrow R(x, z)y \).
  Thus \( \text{Ric}_p(x) = \frac{1}{n-1} \sum \langle R(x, z_i)x, z_i \rangle \), for \( x \) a unit vector, where \( z_i \) is an orthonormal basis orthogonal to \( x \).
- The scalar curvature \( K(p) = 1/n \sum \text{Ric}_p(z_i) \), where \( z_i \) is an orthonormal basis.
The curvatures only depends on the point (11.2.3.11).

Lemma (11.2.3.30).
\[ \frac{D}{D_t} \frac{D}{D_s} V - \frac{D}{D_s} \frac{D}{D_t} V = R(\frac{\partial f}{\partial s} \cdot \frac{\partial f}{\partial t}) V. \] (obvious because \( \frac{\partial}{\partial s} \cdot \frac{\partial}{\partial t} \) commutes)

Proof:

Prop. (11.2.3.31) [Sectional Curvature Define Curvature]. The curvature tensor is determined by its sectional curvature.
In particular, if \( M \) is isotropic at a point \( p \) (The sectional curvature depends only on the point), then
\[ R(X, Y, W, Z) = K_0(\langle X, W \rangle \langle Y, Z \rangle - \langle X, Z \rangle \langle Y, W \rangle). \]
11.2. RIEMANNIAN GEOMETRY

Proof: Cf.[Do Carmo P95], should use the cyclicity of the first three terms. □

Prop. (11.2.3.32) [Bianchi Identities]. Recall the covariant differential \( \nabla R(Y_i, Z) = Z(R(Y_i)) - \sum_i R(\nabla Z Y_i, Y_j) \).

- (Bianchi Identity) \( \sum(X,Y,Z) R(X,Y)Z = 0 \).
- (Second Bianchi Identity) \( \sum(Z,W,T) \nabla R(X,Y,Z,W,T) = 0 \).

Proof: 1: Cf.[Do Carmo P91], should reduce to Jacobi identity.

Prop. (11.2.3.33) [Schur’s Theorem]. Let \( M \) be a manifold of dimension \( n \geq 3 \), suppose the sectional curvature only depends on \( p \), then \( M \) has constant curvature.

Proof: Use the second Bianchi Identity and geodesic frame and (11.2.3.31). Cf.[Do Carmo P106]. □

Def. (11.2.3.34) [Eisenstein Curvature]. A manifold \( M \) is called a Eisenstein manifold iff its Ricci curvature \( \lambda(p) \) only depends on the point. Then

- If \( M \) is connected and Eisenstein of dimension \( \geq 3 \), then it has constant Ricci curvatures everywhere every direction.
- If \( M \) is connected and Eisenstein of dimension \( 3 \), then it has constant sectional curvatures.

Proof: 1: Cf.[Do Carmo P108].

2: Now it has constant Ricci curvature, then

\[ R_{1212} + R_{1313} = \lambda = R_{1212} + R_{2323} = R_{1313} + R_{2323}. \]

So we can solve these curvatures out. □

Prop. (11.2.3.35) [Riemannian Curvature Identities].


Proof: Cf.[DO Carmo P91]. □

- \( B(X,Y) = \nabla_X Y - \nabla_Y X \). It is bilinear and symmetric.
- \( H_\eta(x,y) = \langle B(x,y), \eta \rangle \). Thus \( B(x,y) = \sum H_i(x,y) E_i \) for an orthonormal frame \( E_i \) in \( \mathfrak{X}(U) \).
- \( S_\eta(x) = -(\nabla_\eta)T \). It satisfies: \( \langle S_\eta(x), y \rangle = H_\eta(x,y) = \langle B(x,y), \eta \rangle \). It is self-adjoint. When codimension 1, it is the derivative of the Gauss mapping.

- (Gauss Formula): let \( x,y \) be orthonormal tangent vector. Then:

\[ K(x,y) - \overline{K}(x,y) = \langle B(x,x), B(y,y) \rangle - |B(x,y)|^2. \]

- An immersion is called geodesic at \( p \) if the second fundamental form \( S_\eta \) is zero for all \( \eta \), (which means \( \nabla_X Y \) has no normal component). It is called minimal if the trace of \( S_\eta \) is zero.

- An immersion is called umbilic if there exists a normal unit field \( \eta \) s.t. \( \langle B(X,Y), \eta \rangle(p) = \lambda(p)\langle X,Y \rangle \).
• If the ambient space has constant sectional curvature and the immersed manifold is totally umbilic, then \( \lambda \) is constant.

• Mean curvature tensor of immersion \( f = 1/n \sum_i (\text{tr} S_i) E_i = 1/n \text{tr} B \). It is zero if \( f \) is minimal.

• Normal connection \( \nabla_X^\perp \eta = (\nabla_X \eta)^N = \nabla_X \eta + S_\eta(X) \).

**Prop.(11.2.3.36).**  
• (Gauss equation) 
\[ \langle R(X,Y)Z,T \rangle = \langle R(X,Y)Z,T \rangle - \langle B(Y,T),B(X,Z) \rangle + \langle B(X,T),B(Y,Z) \rangle. \]

• (Ricci equation) 
\[ \langle R(X,Y)\eta,\zeta \rangle - \langle R^\perp(X,Y)\eta,\zeta \rangle = \langle [S_\eta,S_\zeta]X,Y \rangle. \]

• (Codazzi equation) 
\[ \langle R(X,Y)Z,\eta \rangle = (\nabla_Y B)(X,Z,\eta) - (\nabla_X B)(Y,Z,\eta). \] (Lie bracket)

**Parallel Transportation**

**Def.(11.2.3.37)[Parallel Transportation].**

**Def.(11.2.3.38)[Holonomy Group].** The **holonomy group** \( \text{Hol}_x(g) \) of a Riemannian manifold \( M \) w.r.t to the Levi-Civita connection is defined to be the subgroup of \( O(T_x(M)) \) induced by the parallel transportation along a loop. If \( M \) is connected, for different points, holonomy groups are conjugate, so holonomy group is defined up to conjugation.

**Prop.(11.2.3.39)[Trivial Holonomy Group].** If \( M \) is a Riemannian manifold and the holonomy group is trivial, then for any \( X,Y,Z \in X(M) \), \( R(X,Y)Z = 0 \).

**Proof:** Cf.[Do Carmo P105]. \( \square \)

**Prop.(11.2.3.40)[Berger],** in fact, the groups that can be realized as a holonomy group of a simply connected complete Riemannian manifold can be classified.

**Proof:** Cf.[Complex geometry Daniel P214]. \( \square \)

**Def.(11.2.3.41).** The **Geodesic flow** for a connection on \( TM \) is the flow on \( TM \) whose trajectories are \( t \mapsto (\gamma(t),\gamma'(t)) \), where \( \gamma \) is a geodesic on \( M \).

**Prop.(11.2.3.42)[The smoothness of geodesics].** For every point \( p \), there exists a nbhd \( V \) and a \( C^\infty \) mapping 
\[ \gamma : (-\delta,\delta) \times V \times B(0,\epsilon) \to M, \]

s.t. \( \gamma(t,q,v) \) is the geodesic passing through \( p \) with velocity \( v \).

**Prop.(11.2.3.43)[Curvature and Metric, Cartan].** Let \( M,\widetilde{M} \) be two Riemannian manifold of dimension \( n \) and let \( p \in M,\widetilde{p} \in \widetilde{M} \). Choose a linear isometry \( i : T_p(M) \cong T_{\widetilde{p}}(\widetilde{M}) \). Let \( V \) be a normal neighbourhood of \( p \) that \( \exp_p^{-1} \) is defined on \( i \circ \exp_p^{-1}(V) \). Define a mapping \( f : V \to \widetilde{M} \) by 
\[ f(q) = \exp_{\widetilde{p}}^{-1} \circ i \circ \exp_p^{-1}(q). \]

For any \( q \in V \), there is a unique normalized geodesic \( \gamma : [0,t] \to M \) that \( \gamma(0) = p, \gamma(t) = q \). Denote by \( \tilde{P}_t \) the parallel transportation along \( \gamma \), and the map \( \varphi_t : T_q(M) \to T_{\tilde{P}_t(q)}(\widetilde{M}) \) by \( \varphi_t(v) = \tilde{P}_t \circ i \circ \tilde{P}_t^{-1}(v) \).
If for all $q \in V$ and all $x, y, u, v \in T_q(M)$, we have
\[
\langle R(x, y)u, v \rangle = \langle \tilde{R}(\varphi_t(x), \varphi_t(y))\varphi_t(u), \varphi_t(v) \rangle,
\]
then $f : V \to f(V) \subset \tilde{M}$ is an isometry and $df_p = i$.

Proof: Cf. [Do Carmo P157]. Use Jacobi fields. The point is that the hypothesis implies that the map of a Jacobi field is also a Jacobi field. □

Cor. (11.2.3.44). Let $M, \tilde{M}$ be Riemannian manifolds with the same dimension $n$ in which parallel transportation preserves sectional curvature. Let $p \in M, \tilde{p} \in \tilde{M}$. If there is a linear isometry $i : T_p(M) \cong T_{\tilde{p}}(\tilde{M})$ s.t. $K(p, E) = K(\tilde{p}, i(E))$ for any 2-dimensional subspace $E \subset T_p(M)$, then there exist nbhd $V$ of $p$, nbhd $\tilde{V}$ of $\tilde{p}$ and an isometry $f : V \to \tilde{V}$ that $df_p = i$.

Cor. (11.2.3.45). If in situation (11.2.3.44), $M$ and $\tilde{M}$ are moreover complete and simply connected, then there is a unique isometry $f : M \to \tilde{M}$ s.t. $f(p) = \tilde{p}$ and $df_p = i$.

**Complete manifold**

Prop. (11.2.3.46)[Hopf-Rinow theorem]. The following is equivalent definition of completeness.

1. $\exp_p$ is defined for all of $T_p(M)$ and all $p \in M$.
2. The closed and bounded sets of $M$ are compact.
3. $M$ is complete as a metric space.
4. $M$ is $\sigma$-compact and if $q_n \notin K_n, d(p, q_n) \to \infty$.
5. The length of any divergent (compact escaping) curve is unbounded.

and if $M$ is complete, then for any $p, q \in M$, there exists a minimizing geodesic between $p, q$. In particular, any compact submanifold of a complete manifold is complete.

Proof: Cf. [Do Carmo P147]. □

- For any two manifold of the same constant curvature and any two orthogonal basis, there is a local isometry (It is locally isotropic).
- Any complete manifold with a sectional curvature is like $\tilde{M}/\Gamma$, where $\tilde{M}$ is $\mathbb{H}^n, \mathbb{R}^n$ or $\mathbb{S}^n$.

Prop. (11.2.3.47)[Cartan]. in any nontrivial homotopy class in a compact manifold, there exists a closed geodesic.

Proof: □

**4 Jacobi Field and Comparison Theorems**

Def. (11.2.4.1)[Jacobi Field]. The Jacobi field equation along a normalized geodesic $\gamma$ is defined to be
\[
D^2 J(t) + R(\dot{\gamma}(t), J(t))\dot{\gamma}(t) = 0.
\]
It is defined by its initial condition $J(0)$ and $J'(0)$. It can be used to detect the sectional curvature, the critical point of $\exp_p$, and calculate variation of energy.
Prop. (11.2.4.2) [Constant Curvature Case]. On a manifold with constant curvature $K$, the Jacobi field equation for a vector field $J$ normal to $\gamma$ is equivalent to

$$D^2 J(t) + KJ(t) = 0.$$ 

Proof: Use (11.2.3.31), we have

$$\langle R(\gamma', J)\gamma', T \rangle = K\{\langle \gamma', \gamma' \rangle \langle J, T \rangle - \langle \gamma', T \rangle \langle J, \gamma' \rangle \} = K\langle J, T \rangle$$

So $R(\gamma', J)\gamma' = KJ$. □

Prop. (11.2.4.3). The Jacobi field along a point with initial velocity $0$ all has the form

$$J(t) = (d\exp_p)_t(0)(t\dot{J}(0)).$$

Proof: Cf. [Do Carmo P113]. Should use uniqueness theorem of ODE. □

Cor. (11.2.4.4) [Conjugate Points]. If two points $p, q$ are connected by a geodesic $\gamma$, and $q = \exp_p(v_0)$, then $p, q$ are called conjugate along $\gamma$, if there is a non-trivial Jacobi field on $\gamma$ that $J(p) = J(q) = 0$.

Then $q$ is conjugate to $p$ iff $v_0$ is the critical point of $\exp_p$, and the multiplicity of conjugacy is equal to the kernel of $(\exp_p)_v$.

Prop. (11.2.4.5). For a Jacobi field $J$ along $\gamma$, $\langle J(t), \gamma'(t) \rangle$ is linear in $t$.

Proof: Take second derivatives. □

• If $J$ is a Jacobi field $J(t) = (d\exp_p)_t(tw), |v| = |w| = 1$, then

$$|J(t)| = t - \frac{1}{6}K_p(v, w)t^3 + o(t^3).$$

Prop. (11.2.4.6). There are no conjugate points on a Riemannian manifold of non-positive curvature.

Proof: Cf. [Do Carmo P119]. □

Prop. (11.2.4.7) [Killing Field is everywhere Jacobi]. A Killing field is a Jacobi field along geodesics.

And if $X(p) = 0$, then $X$ is tangent to the geodesic sphere near $p$, because $X$ preserves length.

Proof: □

Energy Analysis

Def. (11.2.4.8) [Energy]. The energy of a geodesic $\gamma$ is defined to be

$$E(s) = \int_0^a |\frac{\partial f}{\partial t}(s, t)|^2 dt.$$ 

Prop. (11.2.4.9). A minimizing geodesic must minimize energy.

• (First Variation of Energy)

$$1/2E'(0) = -\int_0^a \langle V(t), D\dot{c}(t) \rangle dt + \langle V(a), \dot{c}(a) \rangle - \langle V(0), \dot{c}(0) \rangle.$$ 

A piecewise differentiable curve is a geodesic iff every proper variation has first derivative 0.
11.2. RIEMANNIAN GEOMETRY

- **(Second Variation of Energy)** If \( \gamma \) is a geodesic,
  \[
  1/2E''(0) = \int_0^a \{\langle DV(t), DV(t) \rangle - \langle R(\dot{\gamma}, V) \dot{\gamma}, V \rangle \} dt + \langle D_s V(a), \dot{\gamma}(a) \rangle - \langle D_s V(0), \dot{\gamma}(0) \rangle.
  \]

- A variation is equivalent to a vector field along the curve, and a variation that \( f_s(t) \) are all piecewise geodesics corresponds to a piecewise Jacobi field (choose a normal partition).

Prop. (11.2.4.10) [Rauch Comparison theorem]. Let \( M \) and \( \tilde{M} \) be manifolds, \( \dim \tilde{M} \geq \dim M \). If \( J \) and \( \tilde{J} \) be two normal Jacobi fields along geodesics \( \gamma \) and \( \tilde{\gamma} \) that \( |J(0)| = |J'(0)| = 0 \) and \( |\tilde{J}(0)| = |\tilde{J}'(0)| \). If \( \tilde{\gamma} \) has no conjugate point or focal point free and \( K(\tilde{x}, \tilde{\gamma}(t)) \geq K(x, \gamma) \) for any vector \( x, \tilde{x} \), then \( |\tilde{J}| \leq |J| \).

Cor. (11.2.4.11) [Injectivity Radius Estimate]. If the sectional curvature of \( M \) satisfies: \( 0 \leq L < K \leq H \), then the distance between any two conjugate points satisfies:
  \[
  \frac{\pi}{\sqrt{H}} \leq d \leq \frac{\pi}{\sqrt{L}}.
  \]

Prop. (11.2.4.12). If two manifold \( M \) and \( M' \) satisfy \( K \leq K' \), then in a normal nbhd of a point \( p \) in \( M \) and a nbhd of \( p' \) that exp is nonsingular, the transformation of a curve \( c \) shortens length.

Note that this is not Toponogov theorem, because if you try to map from a large curvature manifold to a small curvature, then you cannot guarantee that the mapped curve is the shortest.

Cor. (11.2.4.13). In a complete simply connected manifold of non-positive curvature,
  \[
  A^2 + B^2 - 2AB \cos \gamma \leq C^2
  \]

thus \( \alpha + \beta + \gamma \leq \pi \).

Prop. (11.2.4.14) [Moore theorem]. Let \( \overline{M} \) be a complete simply connected manifold of sectional curvature \( \overline{K} \leq -b \leq 0 \), \( M \) a compact manifold of sectional curvature satisfying \( K - \overline{K} \leq b \). If \( \dim \overline{M} < \dim M \), \( M \) cannot be immersed into \( \overline{M} \). (Use Hadamard theorem to choose the furthest geodesic and calculate the second variation of energy and use Gauss formula).

Cor. (11.2.4.15). Let \( \overline{M} \) be a complete simply connected manifold of sectional curvature \( \overline{K} \leq 0 \), \( M \) a compact manifold of sectional curvature satisfying \( K \leq \overline{K} \). If \( \dim \overline{M} < \dim M \), \( M \) cannot immerse into \( \overline{M} \).

Lemma (11.2.4.16) [Klingenberg Lemma]. Let \( M \) be a complete manifold of sectional curvature \( K \geq K_0 \), let \( \gamma_0, \gamma_1 \) be two homotopic geodesics from \( p \) to \( q \), then there exists a middle curve \( \gamma_s \) s.t.
  \[
  l(\gamma_0) + l(\gamma_s) \geq \frac{2\pi}{\sqrt{K_0}}.
  \]

**Proof:** Assume \( l(\gamma_0) < \frac{2\pi}{\sqrt{K_0}} \), otherwise we are done. Then by Rauch comparison (11.2.4.10), the exp: \( T_p M \to M \) has no critical point in the open ball \( B \) of radius \( \pi/\sqrt{K_0} \). Now we want to lift \( \gamma_s \) to \( T_p M \). It is clear that we cannot lift \( \gamma_1 \), because otherwise it is not a curve. Hence for every \( \varepsilon > 0 \), there is a curve \( \alpha_{l(\varepsilon)} \) that can be lifted and has a point with distance smaller than \( \varepsilon \) to the boundary \( \partial B \), otherwise the \( s \) that can be lifted will be open and closed in \([0, 1]\), thus containing 1.

So now if we choose a sequence of lifts curves \( \gamma_s \) converging to the boundary, then \( s \) has a convergent point, then we have \( l(\gamma_0) + l(\gamma_s) \geq \frac{\pi}{\sqrt{K_0}}. \)
Prop. (11.2.4.17) [Klingenberg]. Let $M$ be a simply connected compact manifold of dimension $n \geq 3$ such that $\frac{1}{4} < K \leq 1$, then $i(M)$ (The infimum of distance to the cut locus) $\geq \pi$.

Cor. (11.2.4.18). If $M$ is a compact orientable manifold of even dimension satisfying $0 < K \leq 1$, then $i(M) \geq \pi$.

Prop. (11.2.4.19) [1/4-pinched Sphere Theorem]. Let $M$ be a compact simply connected manifold satisfying $0 < 1/4K_{\text{max}} < K \leq K_{\text{max}}$, then $M$ is homeomorphic to a sphere.

(Cf. Klingenberg Theorem, this is a special case of diameter geodesic sphere theorem).

Cf. (11.2.4.29).

Remark (11.2.4.20). $0 < 1/4K_{\text{max}} < K$ cannot be changed to $\geq$. In fact, the Funibb-Study metric on $CP^n$ has sectional curvature $1 \geq K \geq 4$. Cf. ??

Hess$\rho(X,Y)$ where $\rho$ is the distance to a fixed point, is important.

Prop. (11.2.4.21). Hess$\rho(X,Y)$ is positive definite on the tangent space of the geodesic sphere within the injective radius, and its principal value is $|\frac{J'}{J}|$ for a Jacobi field in that direction. And it is zero on the normal direction.

So there would be a Riccati comparison theorem on the eigenvalue of $\Pi_2 : \lambda' \leq -K - \lambda^2$, Hess$\rho(\rho)$ is bounded.

Proof: Notice that

$$\text{Hess}\rho(X,Y) = (\nabla_X \text{grad}\rho, Y) = XY\rho - (\nabla_X Y)\rho$$

so if choose a normal geodesic $\gamma$ of initial vector $X$, then

$$\text{Hess}\rho(X,X) = X(\langle \gamma', d\rho \rangle \rho - (\nabla_X \gamma')\rho = X(\langle \gamma', d\gamma, d\rho \rangle) = E''(0)$$

$$= I_q(X,X) = ((\nabla_X X)(q), X(q)) = \frac{\langle J', J \rangle}{|J|^2}$$

□

Prop. (11.2.4.22) [Toponogov]. Let $M$ be a complete manifold with $K \geq H$.

If a hinge satisfies $\gamma_1$ is minimal and $\gamma_2 \geq \frac{\pi}{\sqrt{H}}$ if $H > 0$, then on $M^H$ the same hinge has smaller distance of endpoints than this hinge

Proof: Cf. [Cheeger Comparison Theorems in Riemannian Geometry P42]. And there is another triangle version: For a minimal geodesic triangle, the comparison triangle has smaller angles. NOTE this theorem cannot be derived from Rauch Comparison Theorem.

□

Critical Point for Distance Function

Prop. (11.2.4.23). The critical point for distance function on a complete manifold is that for every direction $v$, there is a minimal geodesic $\gamma$ s.t. $\langle \gamma'(l), v \rangle \leq \frac{\pi}{2}$.

The set of regular point is open and there exists a smooth gradient like vector field (i.e. acute angle with every minimal geodesic) on this open subset.
Prop. (11.2.4.24) [Berger’s Lemma]. A maximal point for the distance function is a critical point.

Proof: If not, choose a convergent point \( v \) of the minimal geodesics with endpoint in a curve of that direction, then \( \exp \) near \( v \) will generate a Jacobi field with endpoint Jacobi is the same of that direction. So the distance will increase by \( \cos \theta \) along that direction, contradiction. \( \square \)

Prop. (11.2.4.25) [Soul Lemma]. Let \( M \) is a Riemannian manifold and \( A \) is a closed submanifold. If \( \text{dist}(A, -) \) has no critical point on \( D(A, R) \setminus A \), then \( B(A, R) \) is diffeomorphic to the normal bundle of \( A \to M \).

Proof: \( A \) has a normal \( \exp \) radius \( \epsilon \), and we can vary the gradient-like vector field to be identical to the normal vector near \( A \), and use Morse lemma (the flow) to get a diffeomorphism. \( \square \)

Cor. (11.2.4.26) [Disk Theorem]. If \( A \) is a point then \( M \) is diffeomorphic to a disk.

Lemma (11.2.4.27) [Generalized Schoenflies Theorem]. Easy to do, just use the fact that \( \exp \) is continuous to find a boundary sphere depending continuously on the direction (both \( p \) and \( q \)).

Prop. (11.2.4.28) [Sphere Theorem]. If \( M \) is a closed manifold and has a distance function with only one critical point (the furthest one), then \( M \) is homeomorphic to a twisted ball.

Proof: There exists a \( \epsilon \) and \( r \) that \( B(q, \epsilon) \) and \( B(p, r) \) covering \( M \), (Use the convergent point argument). Then use the generalized Schoenflies theorem. \( \square \)

Prop. (11.2.4.29) [Diameter Sphere Theorem]. If a closed manifold \( M \) satisfies \( \sec M \geq K > 0 \), and \( \text{diam}(M) > \frac{\pi}{2 \sqrt{K}} \), then \( M \) is homeomorphic to \( S^n \).

Proof: First, if there are two maximal distance point, then use Toponogov to show contradiction. Second, at other points \( x \),

\[
\angle pxq > \frac{\pi}{2}
\]

(Regular domain) because of Toponogov and The formula

\[
\cos \tilde{a} = \frac{\cos l - \cos l_1 \cos l_2}{\sin l_1 \sin l_2}.
\]

So the geodesic direction \( \vec{xq} \) will serve as a geodesic-like vector field (might need paracompactness). \( \square \)

Prop. (11.2.4.30) [Critical Principle]. In a complete manifold \( M \) of sectional curvature \( > K \), if \( q \) is a critical point of \( p \), then for any point \( x \) with \( d(p, x) > d(p, q) \) and any minimal geodesic from \( p \) to \( x \), the \( \angle xpq \) is smaller than the \( \cosh_K^{-1} \left( \frac{d(p, x)}{d(p, q)} \right) \).

Proof: Use Toponogov for the hinge \( xpq \). Then notice that there is a different minimal geodesic from \( p \to q \) that makes the \( \angle pqx < \pi/2 \) by the definition of critical point, thus there is another Toponogov inequality, this two inequality contradicts. \( \square \)

Cor. (11.2.4.31). For a complete open manifold whose \( K \) are lower bounded, then it is homeomorphic to the interior of a manifold with boundary. (Use Soul lemma, otherwise there will be a sequence of critical point whose angles are big).

Prop. (11.2.4.32) ray construction and Line construction?
**Prop.(11.2.4.33) [Soul Theorem]**. If $M$ is an open manifold with $K \geq 0$, then there is a totally geodesic submanifold $S$ that $M$ is diffeomorphic to the normal bundle over $S$.

*Proof:* Use the ray construction to get a totally convex compact subset, hence it is a manifold or with boundary, if it has boundary, then find to set of maximal distance to the distance to boundary, the distance to the boundary is a convex function, so it is a smaller totally geodesic manifold. So a $S$ without boundary must exist and this constitutes a stratification, all the level set is strongly convex. Thus all point outside $S$ is not critical, hence the soul lemma applies. Cf. [GeJian Comparison theorems in Riemannian Geometry Lecture7]. □

**Prop.(11.2.4.34) [Perelman]**. There is a distance non-increasing contraction unto the soul, and it must be just the projection along the normal bundle. Moreover, for any geodesic on the soul and a parallel vector field in the normal bundle along it, it spans a flat surface (by Rauch comparison).

**Cor.(11.2.4.35) [Soul Conjecture]**. For an open (non-compact) complete manifold $M$ with $K \geq 0$, if it has a point $p$ s.t. sectional curvature at $p$ are all positive, then $M$ is diffeomorphic to $\mathbb{R}^n$. (It’s enough to show that its soul is a point, otherwise for any point, it must has a direction that is flat, $K = 0$).

## 5 Curvature Inequalities and Topology

### Sectional Curvature

**Prop.(11.2.5.1) [Hadamard theorem]**. $M$ a complete simply connected Riemann manifold of sectional curvature $\leq 0$, then $\exp_p : T_p M \to M$ is an isomorphism of $M$ to $\mathbb{R}^n$. (negative sectional curvature to show $\exp$ is a local isomorphism, complete to show it is a covering map)

**Prop.(11.2.5.2) [Liouville Theorem]**. Any conformal mapping for an open subset of $\mathbb{R}^n, n > 2$ is restriction of a composition of isometry, dilations and/or inversions, at most once.

**Prop.(11.2.5.3) [Positive Curved, Closed Geodesic not Minimal]**. If $M$ is an even dimensional orientable Riemannian manifold with positive sectional curvature, let $\sigma : [0, 1] \to M$ be a closed geodesic curve, then there exists an $\varepsilon > 0$ that parametrized closed curves $F; [0, 1] \times (-\varepsilon, \varepsilon) \to M$ near $\sigma$ with lengths less than that of $\sigma$.

*Proof:* Cf. [Solution to Yau Test Geometry Individual2013 Prob5]. □

**Prop.(11.2.5.4) [Synge]**. $f$ is an isometry of a compact oriented manifold $M^n$ of positive sectional curvature, $f$ alter orientation by $(-1)^n$, then $f$ has a fixed pt.

*Proof:* Cf. [Do Carmo P203]. □

**Cor.(11.2.5.5)**. $M$ a compact manifold of positive sectional curvature, then

1. If $M$ is orientable and $n$ is even, then $M$ is simply connected. So If M is compact and even dimension, then $\pi(M) = 1$ or $\mathbb{Z}/2$.
2. If $n$ is odd, then $M$ is orientable.

(Use the universal cover and covering transformation.)

**Conj.(11.2.5.6) [Hopf Conjecture]**. If $M$ is a compact Riemannian manifold of even dimension that $K > 0$, then it has positive Euler characteristic.
Morse Index

**Prop.(11.2.5.7)[Index Lemma].** Among the piecewise differentiable vector fields along a geodesic without conjugate point or without focal point, with initial value $0$ and fixed end value, the Jacobi field attain minimum of the index form:

$$I_a(V,V) = \int_0^a \{\langle DV(t), DV(t) \rangle - \langle R(\dot{\gamma}, V)\dot{\gamma}, V \rangle \}dt.$$  

**Cor.(11.2.5.8).** $I_l(J,J) = \langle J, J' \rangle(l)$ for a Jacobi field.

**Prop.(11.2.5.9).** a focal point is a critical value of $\exp^\perp$. For an embedded manifold, the focal point equals $x + 1/\theta$, where $\theta$ is a vertical vector and $t$ is a principal value of $S_t a$.

**Prop.(11.2.5.10)[Morse Index theorem].** The index of the the index form $I_a(V,W)$ on the space of vector fields $0$ at the endpoints, equal to the number of points conjugate to $\gamma(0)$ in $[0,a)$.

**Cor.(11.2.5.11).** If $\gamma$ is minimizing, $\gamma$ has no conjugate points on $(0,a)$, $\gamma$ has a conjugate point, it is not minimizing.

**Prop.(11.2.5.12)[Morse].** If $M$ is complete with non-negative sectional curvature, then $\pi_1(M)$ have no finite non-trivial cyclic group and $\pi_k(M) = 0$.

**Proof:** because universal cover of $M$ is contractible, so the higher homotopy group vanish and $\pi_k(M) = H^k(\pi_1(M))$, so if a subgroup is finite cyclic, its homology is periodic, contradiction. □

**Prop.(11.2.5.13)[Preissman].** For a compact manifold with $K < 0$, any nontrivial abelian subgroup of $\pi_1$ is infinite cyclic.

**Prop.(11.2.5.14).** If $M$ is compact and $K < 0$, $\pi_1(M)$ is not abelian.

Assuming $M$ complete,

- The cut point of $p$ along $\gamma$ is the maximum $\gamma(t)$ s.t. $d(p, \gamma(t)) = t$. It is either the first conjugate point of $p$ or the intersection of two minimizing geodesics.

- Conversely, if a point is a conjugate point of $p$ or is intersection of two geodesics of equal length, then there is a cut point before it. So, if intersection of two minimizing geodesics happens, it must happen before the occurrence of conjugate point.

- thus the cut point relation is reflexive, and if $q \in M \setminus C_m(p)$, then there exists a unique minimizing geodesic joining $p$ and $q$.

- $M \setminus C_m(p)$ is homeomorphic to an open ball through exp.

- the distance of $p$ to the cut locus is continuous, thus $C_m(p)$ is closed.

- If $M$ is complete and there is a $p$ which has a cut point for every geodesic, then $M$ is compact.

- for $q$ the closest of $C_m(p)$ to $p$, either there exists a minimizing geodesic and $q$ is conjugate to $p$ or there is to minimizing geodesic connecting at $q$.

**Prop.(11.2.5.15).** The index of a geodesic will decrease when transferred to a manifold of smaller sectional curvature $K$.

**Prop.(11.2.5.16).** In a complete manifold, if there is a sequence of points $\{p_i\}$ converging to a point $p$, choose for each point a minimal geodesic, then a subsequence of them will converge to a minimal geodesic to $p$.

**Proof:** The convergence is by smoothness and of exp and Hadamard. The minimality is by comparing distance.
Ricci Curvature

Prop. (11.2.5.17) [Ricci Comparison]. Volume comparison, Laplacian Comparison, Mean Curvature comparison. Cf. [葛健 Week13].

Prop. (11.2.5.18) [Bishop-Gromov]. Let $M$ be an open manifold with $\text{Ric} \geq H$, let $\tilde{M}(H)$ be a complete simply connected manifold of constant sectional curvature $H$, then

$$\text{Vol}(B_r(x)) \leq \text{Vol}(B_r(\tilde{p})),$$

$$\frac{\text{Vol}(B_R(x))}{\text{Vol}(B_r(x))} \leq \frac{\text{Vol}(B_R(\tilde{p}))}{\text{Vol}(B_r(\tilde{p}))}.$$  

Cf. [葛健 Week13].

Prop. (11.2.5.19) [Bonnet-Myer]. $M$ a complete manifold of Ricci curvature $\text{Ric}_p(v) \geq \frac{1}{r^2}$, Then $M$ is compact and have diameter $\leq \pi r$.

And if the identity is achieved, $M \cong S^n$.

Proof: Use Laplacian comparison $\Delta r \leq (n - 1) \cot r$. Cf. [葛健 week13]. □

Cor. (11.2.5.20) [Positive Ricci Finite Fundamental Groups]. $M$ is a complete manifold of Ricci curvature $\geq \delta > 0$, then the universal cover is compact thus $\pi_1(M)$ is finite. This can be seen as an obstruction for a compact manifold to have positive Ricci curvature.

Cor. (11.2.5.21) [Calabi-Yau]. For an open manifold with non-negative Ricci curvature, for any point, $\text{Vol}(B(p, r)) \geq c_p r$.

Prop. (11.2.5.22) [Milnor]. Let $M$ be an open manifold of non-negative Ricci curvature of dimension $n$, then any f.g. subgroup of $\pi_1(M)$ has polynomial growth $\leq n$. Milnor conjectured that $\pi_1(M)$ in fact is f.g..

Prop. (11.2.5.23) [First Betti Number Theorem]. There is a number $f(n, \lambda, D)$, $f(n, 0, D) = n$, $f(n, \lambda, D) = 0$ for $\lambda > 0$ that for a manifold of diameter $\leq D$ and Ricci curvature $\geq \lambda$, $b_1(M) \leq f(n, \lambda, D)$.

Cor. (11.2.5.24) [Splitting Theorem]. The universal cover of a compact Riemannian manifold with non-negative Ricci curvature splits isometrically as a product $\tilde{M} = N \times \mathbb{R}^k$ where $N$ is a compact manifold manifold.

Scalar Curvature
11.3 Low Dimensional Topology

1 Morse Theory

Main references are [Supersymmetry and Morse Theory, Witten].

Morse Theory (Milnor)

Def. (11.3.1.1) [Non-Degenerate Critical Point]. For a smooth map \( f : X \to \mathbb{R} \), a critical point is called a **non-degenerate critical point** iff the Hessian matrix is non-singular at \( x \).

The notion of non-degenerate critical is independent of the coordinate chosen.

Proof: Cf. [Pollack P42]. □

Prop. (11.3.1.2) [Non-Degenerate Critical General]. Non-degenerate critical points are the general situation in the following sense: For a manifold \( M \subset \mathbb{R}^n \), for any smooth function \( f \) on \( M \), consider the functions \( f_a = f + \sum a_i x_i \), then for almost all \( (a_i) \), all critical points of \( f_a \) is non-degenerate.

Proof: Cf. [Pollack P43] □

Prop. (11.3.1.3) [Morse Lemma]. In a non-degenerate critical point of \( f \), there is a coordinate that

\[
 f = f(p) + x_1^2 + \cdots + x_{n-\lambda}^2 - y_1^2 - \cdots - y_\lambda^2.
\]

Proof: Just extract the first order part out and reform the bilinear form one-by-one. Cf. [Milnor Morse Theory lemma 2.2]. □

Prop. (11.3.1.4). If \( f \) is a smooth function that \( f^{-1}([a, b]) \) is compact and have no critical points, then \( M^a \) is a deformation retracts of \( M^b \) using \( |\text{grad} f| \).

Prop. (11.3.1.5) [Morse Main Lemma]. If \( f \) is a smooth function with \( p \) a non-degenerate critical point and \( \lambda \) downward pointing direction. If for some \( f^{-1}([c - \epsilon, c + \epsilon]) \) is compact, then \( M^{c+\epsilon} \) is homotopic to \( M^{c-\epsilon} \) gluing a \( \lambda \) dimensional cell.

Proof: Cf. [Milnor Prop3.2]. □

Prop. (11.3.1.6). For an embedded manifold and almost all point \( p \), the distance to \( p \) is a Morse function. (Use Sard theorem and degenerate \( \iff \) \( p \) is a focal point.

Cor. (11.3.1.7). smooth manifold has CW type; on a compact manifold any vector field with discrete singular points has its index sum equal to \( \chi(M) \) (Hopf-Rinow), and there exists one.

Prop. (11.3.1.8) for \( \Omega(p, q)^c \) the path space of energy \( < c \), the piecewise geodesic path space \( B \) (piece fixed), the energy function is smooth and \( B^a \) is compact and is the deformation contraction of \( \text{int} \Omega^a \) for \( a < c \). \( E \) has the same critical point and same index and nullity on \( B \) and \( \Omega^c \). (Just geodesicrize any path in \( \Omega \).

So for two point not conjugate in \( B^a \), \( \Omega^a \) has a finite CW complex type and a \( \lambda \)-dimensional cell for every geodesic of index \( \lambda \) in \( B^a \).

Prop. (11.3.1.9) [Morse Main Theorem]. If \( p \) and \( q \) are not conjugate along any geodesic, then \( \Omega(p, q) \) has a countable CW complex type and has a \( \lambda \)-cell for every geodesic of index \( \lambda \).

If \( M \) has nonnegative Ricci curvature, then \( M \) has only finite cell for every dimension.
Proof: Cf. [Milnor Morse Theory Prop17.3]. □

**Cor. (11.3.1.10).** The path space homotopy type only depend on the homotopy type of $M$ (use the two homotopy to id to get a composition of homotopy of the two path space), so one can get the information of path space of $M$ by looking at the homotopy type of $M$.

**Prop. (11.3.1.11)** [Minimal Geodesics]. If $p, q$ in a complete manifold $M$ has distance $\sqrt{d}$ and the minimal geodesics form a topological manifold, and if all non-minimal geodesic has index $\geq \lambda$, then for $0 \leq i < \lambda$, $\pi_i(\Omega, \Omega^d) = 0$.

**Lemma (11.3.1.12).** In $SU(2m)$, the minimal geodesic from $I$ to $-I$ is homeomorphic to Grassmanian $G_m(C^{2m})$ and any non-minimal geodesic has index $\geq 2m + 2$.

Similarly, The space of minimal geodesic from $I$ to $-I$ in $O(2m)$ is homeomorphic to the space of complex structures in $R^{2m}$, and any non-minimal geodesic has index $\geq 2m - 2$.

Proof: Cf. [Milnor Morse Theory Lemma23.1 Lemma24.4]. □

**Lemma (11.3.1.13).** $\Omega_{k+1}$ is homotopic to the space of minimal geodesics in $\Omega_k$ from $J$ to $-J$. (The same way, calculate the index of geodesics from $J$ to $-J$ and use (11.3.1.11)). Cf. [Milnor Morse Theory Prop24.5] for definition of $\Omega_{k+1}$.

2 Floer Homology

**Def. (11.3.2.1)** [Witten Complex]. Let $M \in \text{Diff}_{cpct}$ and $f \in C(M)$ is a Morse function, then at each critical point $P$ of $f$, the Hessian $H_P(f)$ is a non-degenerate quadratic form with signature $n_P^+, n_P^-$. We define the Witten complex $C$ as follows:

- For $0 \leq q \leq \dim M$, $C_q$ is the free group generated by the critical points with $n_P^+ = q$.
- Choose a metric on $M$, define the flow generated by $\text{grad} f$. Then for critical points $P, Q$ with $n_P = q, n_Q = q - 1$, the number of trajectories under $\text{grad} f$ from $P$ to $Q$ is finite, and this gives the boundary map coefficients $\partial_{P,Q}$.

References are [Supersymmetry and Morse Theory, Witten].

**Casson Invariants**

**Def. (11.3.2.2)** [Casson Invariants]. Let $Y$ be a homological 3-sphere, the Casson invariant $\lambda(Y)$ of $Y$ is defined to be the half of the number of isomorphism classes of irreducible representation $\pi_1(Y) \to SU(2)$.

**Prop. (11.3.2.3).** For a homological 3-sphere $Y$, let

- $\mathcal{A}$ be the space of $SU(2)$-connections for the trivial bundle on $Y$,
- $\mathcal{G}$ be the group of gauge transformations $Y \to SU(2)$,
- $\mathcal{C} = \mathcal{A}/\mathcal{G}$.

Then $\mathcal{C}$ is an infinite-dimensional manifold, and the connection map $F : A \mapsto F_A$ defines a 1-form $F$ on $\mathcal{C}$.

Proof: □

**Prop. (11.3.2.4)** [Taubes]. Situation as in (11.3.2.3), the zeros of $F$, i.e. the set of flat connections, corresponds to irreducible representations $\pi_1(Y) \to SU(2)$. And we can use Fredholm perturbation to calculate the number, i.e. $2\lambda(Y)$.

Proof: □
Floer Homology Groups

Remark (11.3.2.5) [Relative Morse Indices]. The difficulty to construct Morse theory for $Y$ lies in the fact that the Hessian of $f : C \to \mathbb{R}/\mathbb{Z}$ at critical points has both Morse indices $n^+, n^-$ infinite. The way around is to notice for critical points $P, Q$, the relative Morse index $n^+_{P,Q} = n^+_P - n^-_Q$ is finite.

Prop. (11.3.2.6) [Floer Homology Theory]. Using the flow generated by $\text{grad} f$, we can get construct a chain complex with $(\text{mod } 8)$-grading, which is a finite complex with the critical points of $f$ as simplexes. The corresponding homology groups are called the Floer homology $HF_q(Y)$, denoted by $HF_q(Y)$, where $q \in \mathbb{Z} \triangleleft (8)$.

Notice reversing the orientation of $Y$ induces an action on $HF_*(Y)$ corresponding to Poincaré duality.

Prop. (11.3.2.7) [Floer Homologies and Casson Invariants]. It is clear now that $2\lambda(M) = \sum_{q=0}^7 \dim HF(Y)$. Thus the Floer homology groups form a refinement of $\lambda(Z)$.

3 Gauge Theory

4 Donaldson-Floer Theory

Main references are [Geometry of 4-Manifolds, Donaldson, ICM1987].

Prop. (11.3.4.1) [Hodge]. For an algebraic surface $S/\mathbb{C}$, the signature $b_2^+$ of the intersection form on $H_2(S(\mathbb{C}))$ satisfies

$$b_2^+ = 1 + 2p_g(S).$$

Def. (11.3.4.2) [Donaldson Invariants]. Let $Z$ be an oriented simply-connected differentiable 4-manifold, let $b_2^+, b_2^-$ be the signature of the intersection form on $H_2(Z)$. Assume $b_2^+ > 1$ is odd, the Donaldson invariants are a sequence of integral polynomials $\varphi_k$ on $H_2(Z)$ for $k$ sufficiently large, and $\deg(\varphi_k) = 4k = 3b_2^+ + 1$?

Thm. (11.3.4.3). If $Z = Z_1 \# Z_2$ is a connected sum with $b_2^+(Z_i) \neq 0$, then $\varphi_k(Z) = 0$ for all $k$.

Proof:

Thm. (11.3.4.4). If $Z$ is an algebraic surface, then for $k$ sufficiently large, $\varphi_k(Z(\mathbb{C})) \neq 0$. In particular, $Z$ is essentially indecomposable.

Proof:

Prop. (11.3.4.5) [\Lambda-Splitting]. Suppose the intersection form on $H_2(Z)$ decomposes as $H_2(Z) = A_1 \oplus A_2$, where $A_i^+ > 0$. If $\varphi_k(Z) \neq 0$ for some $k$, then by (11.3.4.3), $Z$ cannot be decomposed to a connected sum $Z_1 \# Z_2$ having intersection form $A_1$. However, there exists such a decomposition $Z = Z_1 \amalg_Y Z_2$ where $Y$ is a homotopy 3-sphere.

Proof: Cf. [Freeman and Taylor, \Lambda-Splitting 4-Manifolds].

Prop. (11.3.4.6). For a \Lambda-splitting $Z = Z_1 \amalg_Y Z_2$, the Donaldson invariant polynomials are related to the Floer homology groups of $Y$.?
11.4 Differential Forms in Algebraic Topology (Bott-Tu)

This section is dedicated to the analysis of algebraic geometry, using the tool of differential forms.

Basic references are [Differential Forms in Algebraic Geometry Bott-Tu].

1 Basics

Prop. (11.4.1.1) [Cohomological Generator of Sphere]. Let \( v : x \mapsto x/|x| \) be the outward-pointing vector field on \( \mathbb{R}^n \setminus \{0\} \), then the differential form

\[
i(v)(dm) = \frac{1}{|x|} \sum x_i (-1)^{i-1} dx_1 \wedge dx_2 \wedge \ldots \wedge \hat{dx}_i \wedge \ldots dx_n
\]

restricts to a differential form on \( S^{n-1} \) that is a generator of \( H^{n-1}(S^{n-1}) \).

Proof: First we calculate \( d(i(v)(dm)) = \text{div}(v)dm = \frac{n-1}{|v|} dm \). Consider using Stoke's formula:

\[
\int_{\partial B_1} i(v)(dm) - \int_{\partial B_2} i(v)(dm) = \int_{B(0,1) - B(0,\varepsilon)} \frac{n-1}{|v|} dm = 0
\]

Leting \( \varepsilon \to 0 \), \( \int_{\partial B_2} i(v)(dm) \) converges to 0 as \( |i(v)(dm)| \) is bounded and \( V(B_\varepsilon) \) converges to 0. And using the polar coordinate \( dm = r^{n-1} drd\omega \), the right hand side is just

\[
\int_{S^{n-1}} \int_0^1 (n-1)r^{n-2} drd\omega = V(S^{n-1}).
\]

\( \square \)

Prop. (11.4.1.2) [Degree Formula]. If \( f : X \to Y \) is an arbitrary map of two compact oriented manifolds of dimension \( k \), then for any \( k \)-form \( \omega \) on \( Y \),

\[
\int_X f^* \omega = \text{deg}(f) \int_Y \omega.
\]

Proof: \( \text{deg} \) is defined in (11.1.4.16). Cf. [Pollack P188]?

\( \square \)

Prop. (11.4.1.3) [Hopf Invariant]. Let \( n > 1 \), given a map \( S^{2n-1} \to S^n \), let \( \alpha \) be a generator of \( H^n(S^n) \), then \( f^*\alpha = d\omega \) on \( S^{2n-1} \) for some \( \omega \). Define the Hopf invariant of \( f \) to be \( H(f) = \int_{S^{2n-1}} \omega \wedge d\omega \), then:

- The definition of Hopf invariant is independent of \( \omega \) chosen.
- For odd \( n \), the Hopf invariant is 0.
- Homotopic maps \( f, g \) have the same Hopf invariant.

Proof: 1: If \( d\omega = d\omega' \), then

\[
\int_{S^{2n-1}} \omega' \wedge d\omega' - \int_{S^{2n-1}} \omega \wedge d\omega = \int_{S^{2n-1}} (\omega' - \omega) \wedge d\omega = \pm \int_{S^{2n-1}} d((\omega' \wedge \omega)).
\]

2: If \( n \) is odd, then \( \omega \) is of even dimensional, thus \( \omega \wedge d\omega = \frac{1}{2} d(\omega \wedge \omega) \), so \( H(f) = 0 \) by Stokes.

3: If \( F : S^{2n-1} \times I \to S^n \) is a homotopy of \( f, g \), then \( F^*\alpha = d\omega \) for some \( \omega \) on \( S^{2n-1} \times I \). Thus consider

\[
H(f) - H(g) = \int_{S^{2n-1} \times I} \omega_1 \wedge d\omega_1 - \int_{S^{2n-1} \times I} \omega_0 \wedge d\omega_0 = \int_{\partial (S^{2n-1} \times I)} \omega \wedge d\omega = \int_{S^{2n-1} \times I} d\omega \wedge d\omega,
\]

But \( d\omega \wedge d\omega = F^*(\alpha \wedge \alpha) \), and \( \alpha \wedge \alpha = 0 \).

\( \square \)
11.5 Symplectic Geometry

Cf. [Methods in Classical Mechanics Arnold Chapter 8], [辛几何讲义 范辉军].

1 Basics

Symplectic Forms

Def. (11.5.1.1). A symplectic form $\omega$ is a closed 2-form that is non-degenerate on any point. A smooth manifold with a symplectic form is called a symplectic manifold. A symplectic manifold must be even dimensional and orientable.

Prop. (11.5.1.2). A hamiltonian phase flow preserves the symplectic form. $g^* \omega = \omega$.

Proof: by Cartan’s magic formula,

$$\frac{d}{dt} (g^t)^* \omega = L_X \omega = \iota_X (d \omega) + d (\iota_X \omega) = d (\iota_X \omega)$$

because $\omega$ is closed. And by definition, $d (\iota_X \omega)(\eta) = \omega (J \partial H, \eta) = \langle d H, \eta \rangle$, so $d (\iota_X \omega) = d H$. Thus the theorem.

For the following Cf. [辛几何讲义 范辉军 讲座3].

Prop. (11.5.1.3) [Moser’s Stability]. If $\omega_t$ is a smooth family of cohomologous forms on a closed manifold $M$, then there exists an isotopy $\Psi_t$ s.t.

$$\Psi_t^* \omega_t = \omega_0.$$

Prop. (11.5.1.4) [Relative Moser Stability]. If $M$ is a closed manifold and $S$ is a compact submanifold, then if two closed 2-form equals on $S$, there is an open neighborhood $N_0, N_1$ of $S$ and a diffeomorphism $\Psi : N_0 \to N_1$ that

$$\Psi | S = \text{id}, \ \Psi^* \omega_1 = \omega_0.$$

Cor. (11.5.1.5) [Darboux’s Theorem]. Every symplectic form $\omega$ on $M$ is locally diffeomorphic to the standard form $\omega_0$ on $\mathbb{R}^{2n}$.

Proof: Choose $S = \text{pt}$ and uses relative Moser stability.

Prop. (11.5.1.6). For a compact symplectic manifold $M$, its even dimensional cohomology groups doesn’t vanish, because $\omega^k$ are nontrivial.

Proof: This is because $\omega^n$ is a volume form on $M$ that never vanish, so it gives $M$ an orientation and $\int_M \omega^n \neq 0$. If $\omega^k$ is exact, then $\omega^n$ is exact, so $\int_M \omega^n = 0$ by Stokes’, contradiction.
11.6 Lie Groups

Main references are [Eti21], [Lee13], [Kna96].

1 Basics

Def.(11.6.1.1) [Lie Groups]. Let $K = \mathbb{R}$ or $\mathbb{C}$, a Lie group is a group object in the category of smooth $K$-manifolds. Notice it suffices to check that multiplication is smooth. The left and right translations $L_g, R_g$ are all smooth morphisms hence diffeomorphisms.

A homomorphism of Lie groups is a smooth morphism that is also a group homomorphism. By translation invariance, a group homomorphism always has constant ranks, so a homomorphism of Lie groups that is a bijection is an isomorphism by global rank theorem (11.1.1.12).

The tangent space of $G$ at $e$ is denoted by $g$.

Proof: We show if a topological group $G$ that is a smooth manifold satisfies $m : G \times G \to G$ is smooth, then $G$ is a smooth manifold: consider the map $F : G \times G \to G \times G : (g, h) \mapsto (g, gh)$, it is a smooth map that is bijective.

The tangent map of $F$ at $(g, h)$ is $(X, Y) \mapsto (X, (dR_h)g(X) + (dL_g)h(Y))$, which is surjective because $L_g$ is a diffeomorphism by (11.1.1.12). Then $F^{-1} : G \times G \to G \times G : (g, h) \mapsto (g, g^{-1}h)$ is smooth, and $g \mapsto g^{-1}$ is smooth.

Prop.(11.6.1.2). A connected Lie group is automatically second countable.

Proof: This follows from the fact that a connected Lie group is a manifold hence locally second-countable and it is a union of products of a nbhd of $e$ (3.8.1.3).

Prop.(11.6.1.3). Any homomorphism of smooth manifolds has constant rank.

Proof: $F$ being a homomorphism means that $F \circ L_g = L_{F(g)} \circ F$. Taking derivative and noticing the fact $L_g, L_{F(g)}$ are diffeomorphisms shows $dF_{g_0}$ and $dF_e$ have the same rank for any $g$.

Prop.(11.6.1.4) [Discrete Subgroups]. Any discrete subgroup $\Gamma$ of a Lie group $G$ is a closed Lie subgroup of dimension 0.

Proof: Firstly $\Gamma$ is countable: Let $U$ be a nbhd of $e$ containing no other points, choose another nbhd of $e$ that $VV \subset U$, then $\{gV\}_{g \in \Gamma}$ is a family of disjoint open subsets of $G$, so there are countably many because $G$ is second countable. Secondly $\Gamma$ is closed in $G$, because $\Gamma$ is closed in $G$: Let $U$ be a nbhd of $e$ containing no other points, choose another nbhd of $e$ that $VV \subset U$, then $\{gV\}_{g \in \Gamma}$ is a family of disjoint open subsets of $G$ each containing an element of $\Gamma$. Then it is clear $\Gamma$ is closed. Then (11.6.1.22) shows $\Gamma$ is a closed Lie subgroup of dimension 0.

Def.(11.6.1.5) [Adjoint Representation]. For a Lie group $G$, the conjugation map $C_g : G \to G : h \mapsto ghg^{-1}$ is a Lie group homomorphism. Let $\text{Ad}(g) : \mathfrak{g} \to \mathfrak{g}$ denote its derivative, then $\text{Ad} : g \mapsto \text{Ad}(g)$ is an action of $G$ on $\mathfrak{g}$, because $C_{g_1g_2} = C_{g_1}C_{g_2}$, $\text{Ad}(g_1g_2) = \text{Ad}(g_1)\text{Ad}(g_2)$.

Prop.(11.6.1.6). Let $G$ be a connected Lie group, and $\Gamma \subset G$ be a discrete normal subgroup. Show that $\Gamma$ is in the center of $G$.

Proof: For $\gamma \in \Gamma$, consider the map $G \to G : g \mapsto g\gamma g^{-1}$, then it is a map with images in $\Gamma$. But $\Gamma$ is discrete, so its image must be a single point, which is $\gamma$ because $e\gamma e^{-1} = \gamma$. This means $\gamma$ is in the center of $G$. □
\textbf{Prop. (11.6.1.7)} [Aut(\mathfrak{g})]. Let \( \mathfrak{g} \) be a f.d. Lie algebra, then Aut(\( \mathfrak{g} \)) is a closed Lie subgroup of GL(\( \mathfrak{g} \)), and its Lie algebra is Der(\( \mathfrak{g} \)). Denote Int(\( \mathfrak{g} \)) = Der(\( \mathfrak{g} \))\(^0\).

\textit{Proof:} For the Lie algebra, it suffices to show for \( A \in \text{End}(\mathfrak{g}) \), \( [e^{tA}X, e^{tA}Y] = e^{tA}[X, Y] \) iff \( A([X, Y]) = [A(X), Y] + [X, A(Y)] \).

One direction is by taking derivative w.r.t. \( t \), for the other, we can show \( y_1(t) = [e^{tA}X, e^{tA}Y] \) and \( y_2(t) = e^{tA}[X, Y] \) both satisfy the ordinary differential equation \( y_i(t)' = Ay_i(t) \).

**Exponential Map**

\textbf{Def. (11.6.1.8)} [One-Parameter Subgroup]. A \textbf{one-parameter subgroup} of a Lie group \( G \) over \( K \) is a Lie group homomorphism \( K \rightarrow G \).

\textbf{Prop. (11.6.1.9)}. Let \( X \in \mathfrak{g} \), then there exists a unique morphism of Lie groups \( \gamma : K \rightarrow G \) that \( \gamma'(0) = X \).

\textit{Proof:} If \( \gamma \) is such a group homomorphism, then \( \gamma(s + t) = \gamma(s)\gamma(t) \). Differentiating for \( s \), we get

\[ \gamma(t)' = d(L_{\gamma(s)})_0(X). \]

Thus \( \gamma \) is an integral curve of the left-invariant vector field on \( G \) corresponding to \( X(11.6.3.3) \), which is unique.

Now to construct such a homomorphism, we use ODE theorems to construct a \( \gamma \) satisfying this for \( |t| < \varepsilon \), and then check \( \gamma(s + t) = \gamma(s)\gamma(t) \) because they are both integral curves for \( t \) starting at \( \gamma(s) \). In particular, \( d(L_{\gamma(t)})(X) = d(R_{\gamma(t)})(X) \). Now we can extend this \( \gamma \) to whole of \( K \) by defining \( \gamma(2^n s) = \gamma(s)^{2^n} \), then we check by induction on \( n \) that

\[ \gamma'(t) = \frac{1}{2} (d(R_{\gamma(\frac{t}{2})})\gamma' \left( \frac{t}{2} \right) + d(L_{\gamma(\frac{t}{2})})\gamma' \left( \frac{t}{2} \right))(X) = d(R_{\gamma(\frac{t}{2})})d(R_{\gamma(\frac{t}{2})})(X) = d(R_{\gamma(t)})(X). \]

\textbf{Cor. (11.6.1.10)} [One-Parameter Subgroup and Lie Algebras]. Let \( G \) be a Lie group, then the one-parameter subgroups of \( G \) correspond to maximal integral curves of left invariant vector fields starting at \( e \). In particular, the one-parameter subgroups of \( G \) corresponds to \( \mathfrak{g} \) and also \( T_e(G) \).

Also, the flow of the right-invariant vector field \( R_X \) is given by \( (g, t) \mapsto \exp(tX)g \), and the flow of the left-invariant vector field \( L_X \) is given by \( (g, t) \mapsto g \exp(tX) \).

\textbf{Def. (11.6.1.11)} [Exponential Map]. Let \( G \) be a Lie group with Lie algebra \( \mathfrak{g} \), then we can define an \textbf{exponential map} \( \exp : \mathfrak{g} \rightarrow G \) that for any \( X \in \mathfrak{g} \), \( \exp(X) = \gamma_X(1) \), where \( \gamma_X \) is the one-parameter subgroup of \( G \) generated by \( X(11.6.1.10) \). It can be shown that \( \gamma(sX) \) is the one-parameter subgroup of \( G \) generated by \( X \).

\textbf{Prop. (11.6.1.12)} [Properties of Exponential Map].

1. \( \exp : \mathfrak{g} \rightarrow G \) is a smooth map which is a local diffeomorphism near \( 0 \) that \( \exp(0) = e, \exp_* = \text{id}_\mathfrak{g} \).
2. \( \exp(s + t) = \exp(s)\exp(t) \) for \( s, t \in K \).
3. For any group homomorphism \( \varphi : G \rightarrow H \) and \( X \in \mathfrak{g} \), \( \varphi(\exp(X)) = \exp(\varphi_*(X)) \).
4. \( g \exp(tX)g^{-1} = \exp(\text{Ad}(g)X) \). Also, \( \text{Ad}_* = \text{ad} \), or equivalently by item3, \( \text{Ad}(\exp(X)) = \exp(\text{ad}(x)) \) as operators.
5. If we identify \( \mathfrak{gl}_n(K) \) with \( GL_n(K) \), then we can check directly that the exponential map of \( GL_n(K) \) is

\[
\exp(A) = \sum_{k=0}^{\infty} \frac{1}{k!} A^k.
\]

\textbf{Proof:} 1: The smoothness follows from the smoothness of the solution of ODE. The smooth inverse theorem shows it is a local diffeomorphism at identity.

2: trivial.

3: Both \( \varphi(\exp(tX)) \) and \( \exp(t\varphi_*(X)) \) are integral curves of the vector field \( L_{\varphi_*}(X) \) and have the same initial point.

4: The first assertion is just item 3 applied to the conjugate action \( C_g \). For the Lie algebra homomorphism,

\[
d(Ad)(X)Y = \frac{\partial}{\partial s} \exp(sX) \exp(tY) \exp(-sX) = [X,Y]
\]

by (11.6.1.14). \( \square \)

\textbf{Prop. (11.6.1.13).} Let \( G \) be a Lie group with Lie algebra \( \mathfrak{g} \), and \( \mathfrak{g} = A \oplus B \) a decomposition as subspaces, then the map

\[
F : A \oplus B \to G : (X,Y) \mapsto \exp(X) \exp(Y)
\]

is a local diffeomorphism at \( 0 \in \mathfrak{g} \).

\textbf{Proof:} Identify \( \mathfrak{g} \) and the tangent space of \( G \) at \( e \), then the differential \( F \) is identity, so it is a local diffeomorphism. \( \square \)

\textbf{Prop. (11.6.1.14) [Baker-Campbell-Hausdorff].} Let \( G \) be a Lie group with Lie algebra \( \mathfrak{g} \), \( X, Y \in \mathfrak{g} \), then

\[
\exp(tX) \exp(tY) = \exp\left( \sum_{n=1}^{\infty} \frac{t^n}{n!} \mu_n(X,Y) \right).
\]

where \( \mu_n(X,Y) \) can be written as \( \mathbb{Q} \)-Lie polynomials of \( X \) and \( Y \) that is invariant of \( G \).

In particular, \( \mu_1(X,Y) = X + Y \), \( \mu_2(X,Y) = \frac{1}{2} t^3([X,[X,Y]] + [Y,[Y,X]]) \) and so on.

\textbf{Proof:} By the Lie correspondence (11.6.3.15), we can first assume that \( G \) is simply-connected, then there is a mapping of \( G \) onto some subgroup of \( GL(n, K) \) with discrete kernel. If we can prove the formula for \( G = GL(n,K) \), then \( \exp(\sum_{n=1}^{\infty} \frac{t^{n}}{n!} \mu_n(X,Y)) \exp(tY)^{-1} \exp(tX)^{-1} \) is contained in the kernel, but it is a smooth function in \( t \), and its value is 1 for \( t = 0 \), thus it holds for any \( t \).

Now let \( TK^2 = K(x,y) \) be the free non-commutative algebra in variables \( x, y \), the series \( \exp(x) = \sum_{n=0}^{\infty} \frac{x^n}{n!} \) can be viewed as an element in \( K(x,y) \). Then we can define

\[
\mu = \log(\exp(x) \exp(y)) \in \widehat{K(x,y)},
\]

where \( \log(A) = -\sum_{n=1}^{\infty} \frac{(1-A)^n}{n!} \). Then \( \mu = \sum_{n=1}^{\infty} \frac{\mu_n}{n!} \), where \( \mu \in K(x,y) \) are polynomials in \( x, y \) of degree \( n \) with coefficients in \( \mathbb{Q} \).

Then it remains to show that \( \mu_n \) can be written as Lie polynomials in \( x, y \). Notice \( \Delta(x) = x \otimes 1 + 1 \otimes x \), thus \( \Delta(\exp(x)) = \exp(x) \otimes \exp(x) \), thus \( \Delta(\exp(x) \exp(y)) = \exp(x) \exp(y) \otimes \exp(x) \exp(y) \), and

\[
\Delta(\log(\exp(x) \exp(y))) = \log(\Delta(\exp(x) \exp(y))) = \log((\exp(x) \exp(y) \otimes 1)(1 \otimes \exp(x) \exp(y)))
\]
\[ = \log(\exp(x) \exp(y)) \otimes 1 + 1 \otimes \log(\exp(x) \exp(y)). \]

then by separating degrees, each \( \mu_n \) is primitive(2.9.1.3), thus they are contained in the free Lie-algebra generated by \( x, y \), by(2.5.8.15) and(2.5.8.18).

The calculation is invariant of \( n \) in \( GL(n, \mathbb{R}) \), thus it is invariant of \( G \). □

Cor. (11.6.1.15). Let \( G \) be a Lie group with Lie algebra \( \mathfrak{g} \), \( X, Y \in \mathfrak{g} \), then
\[
\lim_{n \to \infty} (\exp(\frac{1}{n}X) \exp(\frac{1}{n}Y))^n = \exp(X + Y).
\]

Proof:
\[
(\exp(\frac{1}{n}X) \exp(\frac{1}{n}Y))^n = (\exp(\frac{1}{n}(X + Y) + O(\frac{1}{n^2})))^n = \exp(X + Y + O(\frac{1}{n})).
\]
Taking \( n \to \infty \), we get the desired result. □

Prop. (11.6.1.16). Let \( K = \mathbb{R} \) or \( \mathbb{C} \) and \( H, G \) be Lie groups over \( K \), then

- A continuous homomorphism \( \gamma : K \to H \) is smooth.
- A continuous homomorphism between smooth Lie groups \( F : G \to H \) is smooth.
- There is at most one smooth structure on a Lie group \( G \) that makes it a Lie group.

Proof: 1: Let \( V \) be a nbhd of \( 0 \in \mathfrak{h} \) that \( \exp \) is a diffeomorphism on \( 2V(11.6.1.12) \). Choose \( t_0 \) small that \( \gamma(t) \in \exp(V) \) for any \( |t| \leq t_0 \), and let \( X \in V \) that \( \exp(X) = \gamma(t_0) \), then we can show \( \gamma(t) = \exp(tX) \) for any \( t = \frac{m}{2n} \), so this holds for any \( t \) by continuity/analyticity, and \( \gamma \) is smooth.

2: By the proof of 1, we can construct a map(not necessary continuous) \( F_\ast : \mathfrak{g} \to \mathfrak{h} \) with commutative diagram
\[
\begin{array}{ccc}
\mathfrak{g} & \xrightarrow{F_\ast} & \mathfrak{h} \\
\downarrow \exp & & \downarrow \exp \\
G & \xrightarrow{F} & H
\end{array}
\]
is linear:
\[
\exp(F_\ast(X + Y)) = F(\exp(X + Y)) = F(\lim_{n \to \infty} \exp(\frac{1}{n}X) \exp(\frac{1}{n}Y))^n]
= \lim_{n \to \infty} (\exp(\frac{1}{n}F_\ast X) \exp(\frac{1}{n}F_\ast Y))^n = \exp(F_\ast(X + Y))
\]
Thus \( F \) is smooth at a nbhd of \( G \), and smooth everywhere by translation. □

Group Aspects

Def. (11.6.1.17)[Lie Subgroup]. A Lie subgroup of a Lie group \( G \) is a subgroup that is also an immersed submanifold(11.1.1.14).

An embedded Lie subgroup of a Lie group \( G \) is a subgroup that is also an immerge submanifold(11.1.1.14).

Prop. (11.6.1.18)[Lie subgroup is Weakly Embedded]. Any Lie subgroup of a Lie group \( G \) is weakly embedded.

Lemma (11.6.1.19). Let $G$ be a Lie group and $H$ a subgroup that is also an embedded submanifold, then $H$ is an embedded Lie subgroup.

Proof: We need to show the multiplication and inverse on $H$ is smooth: $H \times H \to G$ is smooth and has image in $H$, thus $H \times H \to H$ is also smooth, by (11.1.1.22).

Lemma (11.6.1.20). Let $G$ be a Lie group and $H \subset G$ a Lie subgroup, if $H$ is an embedded submanifold of $G$, then $H$ is closed in $G$.

Proof: Assume $H$ is an embedded submanifold of $G$, then it is locally compact in the induced topology, so (10.9.1.7) shows $H$ is closed in $G$.

Lemma (11.6.1.21). Let $G$ be a Lie group and $H$ a subgroup of $G$ that is also a closed subset of $G$, then $H$ is an embedded Lie subgroup.

Proof: By (11.6.1.20), it suffices to show that $H$ is an embedded submanifold of $G$. Let $\mathfrak{g}$ be the Lie algebra of $G$, and define a subspace $\mathfrak{h} \subset \mathfrak{g}$ that $\mathfrak{h} = \{X \in \mathfrak{g}| \exp(tX) \in H, \forall t \in \mathbb{R}\}$. By (11.6.1.15) and the fact $H$ is closed in $G$, $\mathfrak{h}$ is a linear subspace of $\mathfrak{g}$.

Next we show that there exists a nbhd $U$ of $0 \in \mathfrak{g}$ that $\exp$ is a diffeomorphism and also $\exp(U \cap \mathfrak{h}) = \exp(U) \cap H$: Let $U$ be any open nbhd of $0 \in \mathfrak{g}$ that $\exp$ is a diffeomorphism $U \to \exp(U)$, then $\exp(U \cap \mathfrak{h}) \subset \exp(U) \cap H$ by definition.

Let $b \subset \mathfrak{g}$ be chosen s.t. $\mathfrak{h} \oplus b = \mathfrak{g}$, then $F: \mathfrak{h} \oplus b \to G: (X,Y) \mapsto \exp(X) \exp(Y)$ is a local diffeomorphism. Choose nbhd $U$ of $0 \in \mathfrak{g}$ and $\bar{U}$ of $0 \in \mathfrak{h} \oplus b$ that both $\exp|_{\bar{U}}$ and $F|_{\bar{U}}$ are diffeomorphisms, and choose a countable nbhd basis $\{U_i\}$ of $0 \in \mathfrak{g}$. Denote $V_i = \exp(U_i)$ and $\bar{V}_i = F^{-1}(V_i)$, then $V_i$ is a nbhd basis of $e \in G$ and $\bar{V}_i$ is a nbhd basis of $0 \in \mathfrak{h} \oplus b$. We may assume $U_i \subset U$ and $\bar{U}_i \subset \bar{U}$.

If $\exp(U_i \cap \mathfrak{h}) \subset \exp(U_i) \cap H$ for any $i$, then we can choose $h_i = \exp(Z_i) \in H$ that $h_i \notin \exp(U_i \cap \mathfrak{h})$. Because $\exp(U_i) = F(\bar{U}_i)$, set $h_i = \exp(X_i) \exp(Y_i)$, where $(X_i,Y_i) \in \bar{U}_i$. Now $Y_i \neq 0$, otherwise $\exp(Z_i) = \exp(X_i)$, which implies $Z_i = X_i$ and $h \notin \exp(U_i \cap \mathfrak{h})$. Notice $\exp(Y_i) = \exp(X_i)^{-1}h_i \in H$.

Because $\bar{U}_i$ is a basis of $\mathfrak{h} \oplus b$, $Y_i \to 0$, Choose an inner product on $b$, and let $c_i = |Y_i|$, then $c_i^{-1}Y_i$ lies on the unit sphere of $b$. Replacing by a subsequence, we can assume $c_i^{-1}Y_i \to Y$ for some $Y \in b$. Then $|Y| = 1$ by continuity.

For any $t \in \mathbb{R}$, let $n_i = \lfloor \frac{c_i}{t} \rfloor$, then $|nc_i - t| \leq c_i \to 0$, which means $n_iY_i \to tY$, so $\exp(n_iY_i) \to \exp(tY)$. But $\exp(n_iY_i) = \exp(Y_i)^{n_i} \in H$, so $\exp(tY) \in H$ because $H$ is closed. Thus $Y \in \mathfrak{h}$, contradiction.

Thus in this way we can construct a slice chart $\varphi$ of $H$ at $e$, and for any $h \in H$, because $L_h((\exp(U) \cap H)) = L_h(\exp(U)) \cap H$,

$\varphi \circ L_{h^{-1}}$ is a slice chart of $H$ at $h$. Thus $H$ is an embedded submanifold of $G$ by (11.1.1.17).

Prop. (11.6.1.22) [Closed Subgroup Theorem]. Let $G$ be a Lie group and $H$ a subgroup of $G$, then the following are equivalent:

- $H$ is closed in $G$.
- $H$ is an embedded submanifold.
- $H$ is an embedded Lie subgroup.

Proof: $3 \to 2$ is trivial, $3 \to 1$ is (11.6.1.20). $1 \to 3$ is (11.6.1.21), $2 \to 3$ is (11.6.1.19).
Remark (11.6.1.23). The dense line of the torus is a Lie subgroup that is not a closed Lie subgroup.

Lemma (11.6.1.24) [One-Parameter subgroup of Subgroups]. Let $H \subset G$ be a Lie subgroup, then the one-parameter subgroups of $H$ are exactly those of $G$ with initial velocity in $T_e(H)$.

Proof: This is because a one-parameter subgroup of $H$ is naturally a one-parameter subgroup of $G$, and two one-parameter subgroups with the same initial velocity is identical. ☐

Prop. (11.6.1.25). Let $H \subset G$ be a Lie subgroup, then the exponential map of $H$ is the exponential map of $G$ restricted to $H$, and

$$ \mathfrak{h} = \{ X \in \mathfrak{g} | \exp(tX) \in H, \forall t \in \mathbb{R} \}. $$

Proof: The first assertion is an immediate corollary of (11.6.1.24). Now if $X \in \mathfrak{h}$, then the first assertion shows $\exp(tX) \in H$ for all $t$. Conversely, if $\exp(tX) \in H$ for all $t$, then $\exp(tX)$ is a smooth map to $H$, by (11.6.1.18), thus its derivative at $e$ is in $\mathfrak{h}$, which means $X \in H$. ☐

Prop. (11.6.1.26) [Semidirect Product]. Let $G$ acts via $\tau$ on $H$, then the Lie algebra of $G \ltimes_\tau H$ is $\mathfrak{g} \ltimes_d \mathfrak{h}$.

Proof: Notice the differential of the action $\tau(g)$ on $H$ defines a map $G \to GL(\mathfrak{h})$, and then the differential of this map gives a map $d\tau : \mathfrak{g} \to \text{Der}(\mathfrak{h})$, so we can form $\mathfrak{g} \ltimes_d \mathfrak{h}$. For the rest, Cf.[Knapp, P60]. ☐

Prop. (11.6.1.27). Let $G, H$ be simply-connected Lie groups with Lie algebra $\mathfrak{g}, \mathfrak{h}$, and let $\pi : \mathfrak{g} \to \text{Der}(\mathfrak{h})$ be a Lie algebra homomorphism, then there is an action $\tau$ of $G$ on $H$ by automorphisms that $d\tau = \pi$, and $G \ltimes_\tau H$ is a simply-connected Lie group with Lie algebra $\mathfrak{g} \ltimes_\pi \mathfrak{h}$.

Proof: Cf.[Knapp, P60]. ☐

Prop. (11.6.1.28) [Quotient Theorem for Lie Groups]. Let $G$ be a Lie group and $H$ a normal closed Lie subgroup, then the quotient $G/H$ is a Lie group, and the quotient map $\pi$ is a surjective Lie group homomorphism with kernel $H$.

Proof: By (11.6.2.6), $G/H$ is a smooth manifold that the quotient map is surjective, smooth, and is a group homomorphism with kernel $H$. It suffices to show the multiplication of $G/H$ is smooth, which is easy by (11.1.1.8). ☐

Prop. (11.6.1.29) [First Isomorphism Theorem for Lie Groups]. Let $\varphi : G \to H$ be a Lie group homomorphism, then there kernel of $F$ is an closed Lie subgroup of $G$ with Lie algebra $\ker(\varphi_*)$. The image of $\varphi$ has a unique smooth structure making it a Lie subgroup of $H$ that $G/\ker(F) \to \text{Im}(\varphi)$ is a diffeomorphism, and it is a closed Lie subgroup when it is embedded in $H$, e.g. when $\varphi$ induces a proper action (11.6.2.3).

Proof: This follows from (11.6.2.2) and (11.6.1.22). ☐

Def. (11.6.1.30) [Adjoint Group]. For a Lie group $G$, the center $Z(G)$ of $G$ is a closed Lie subgroup because it the kernel of $\text{Ad}(11.6.1.29)$. We call the group $G/Z(G)$ the adjoint group of $G$, which is an immersed subgroup of $GL(\mathfrak{g})$ by (11.6.1.29).
Lie Groups and Analytic Groups

Prop. (11.6.1.31). What condition makes a Lie group a complex Lie group?

Prop. (11.6.1.32). Any connected Lie group has a compact subgroup as deformation retraction.

Proof: □

Prop. (11.6.1.33) [Gleason; Montgomery-Zippin]. A real topological group \( G \) admits a (unique) Lie group structure iff the underlying topological space \( G \) is a topological manifold.


Prop. (11.6.1.34) [Lie Groups and Analytic Groups]. A real Lie group admits a unique real analytic structure, so it is not important to distinguish between a Lie group and an analytic Lie group, and call it analytic group if it is a connected Lie group. The uniqueness follows from (11.6.1.16).

Proof: Use (11.6.1.14) to show that in a local exp char \((U, \varphi)\) of \( U \), \( U \times U \to U \) is analytic, then we can choose an analytic atlas on \( G \) given by \( \{(gU, \varphi \circ L_{g^{-1}})\} \). This is an analytic atlas, because the transition function is \( \varphi L_{g^{-1}}h\varphi^{-1} \) on \( U \cap h^{-1}gU \). Because \( hU \cap gU \neq \emptyset \), let \( x = hu_1 = gu_2 \), then \( L_{g^{-1}h} = L_{u_2u_1^{-1}} \), which is analytic.

To show multiplication is analytic w.r.t. this atlas: ? □

Cor. (11.6.1.35). The proof above can be used to show that any \( C^k \)-group manifold be upgraded uniquely to a Lie group structure. So basically the study of \( C^0 \)-Group manifold and analytic groups are the same.

2 Homogeneous Spaces

Actions of Lie Groups

Prop. (11.6.2.1) [Fundamental Theorem on Lie Group Actions]. Let \( \theta \) be a right smooth action of a Lie group \( G \) on a smooth manifold \( M \), then we can define a complete Lie algebra homomorphism

\[
\tilde{\theta} : \mathfrak{g} \to \mathfrak{X}(M) : \theta(X)_p = \frac{d}{dt}\big|_{t=0} p \cdot \exp(tX) = d(\theta^p)_e(X_e),
\]

called the infinitesimal generator of \( \theta \). where a Lie homomorphism \( \tilde{\theta} : \mathfrak{g} \to \mathfrak{X}(M) \) is called complete iff for any \( X \in \mathfrak{g} \), \( \tilde{\theta}(X) \) is a complete vector field (11.1.5.3).

Conversely, if \( G \) is simply-connected and \( \tilde{\theta} : \mathfrak{g} \to \mathfrak{X}(M) \) is a complete Lie algebra homomorphism, then there exists a unique smooth right action \( \theta \) of \( G \) on \( M \) with infinitesimal generator \( \tilde{\theta} \).

Proof: \( \theta(X) \) is smooth because it is the infinitesimal generator of the smooth flow \( \mathbb{R} \times M \to M : (t, p) \mapsto p \exp(tX) \) (11.1.5.4). \( \tilde{\theta} \) is a Lie algebra homomorphism by (11.1.2.13). □

Prop. (11.6.2.2) [Isotropy Group and Orbits]. Let \( \theta \) be an action of \( G \) on a manifold \( M \), let \( \theta_x : \mathfrak{g} \to T_x M \) be given by \( \theta_x(X) = \theta(X)_x \). Then

- The stabilizer \( G_x \) is a closed subgroup of \( G \) with Lie subalgebra \( \mathfrak{g}_x = \ker(\tilde{\theta}_x) \).
11.6. LIE GROUPS

- $Gx$ has a unique smooth structure making it an immersed subgroup of $M$ that $G/G_x \to Gx$ is a diffeomorphism, and $T_x(Gx) \cong \text{Im}(\tilde{\theta}_x) \cong g/g_x$.


PROP. (11.6.2.3). If a Lie group $G$ acts properly on a manifold $M$, then each orbit is a closed submanifold of $M$, and each isotropy group is compact, by (3.8.1.15) and (3.8.1.17).

PROP. (11.6.2.4) [Quotient Map Theorem]. Let $G$ be a Lie group that acts smoothly, freely and properly on a manifold $M$, then the quotient space $M/G$ is a topological manifold with dimension $\dim M - \dim G$, and it has a unique smooth structure that $M \to M/G$ is a smooth submersion.


Homogeneous Spaces and Fiber Bundles

DEF. (11.6.2.5) [Homogeneous Spaces]. Let $G$ be a Lie group, then a homogeneous space for $G$ is a smooth manifold $M$ with a smooth transitive $G$-action.

PROP. (11.6.2.6) [Characterizing Homogeneous Spaces]. Let $G$ be a Lie group.

- if $H$ is a closed subgroup of $G$, then the left coset space $G/H$ is a topological manifold of dimension $\dim G - \dim H$, and has a unique smooth structure that the quotient map $G \to G/H$ is a smooth submersion. With this smooth structure, the left action of $G$ on $G/H$ turns it into a homogeneous space.

- If $M$ is a homogeneous $G$-space, and $p \in M$, then the isotropy group $G_p$ of $M$ is a closed subgroup of $G$, and $G/G_p \to M$ is a diffeomorphism of $G$-spaces.


COR. (11.6.2.7) [Homogeneous Space Structure on Sets]. Suppose $X$ is a set with a transitive action of a Lie group $G$ that for some point $p \in X$, the isotropy group $G_p$ is closed in $G$. Then $X$ has a unique smooth manifold structure with respect to which the given action is smooth. With this structure, $\dim X = \dim G - \dim G_p$.

Proof: This is because $G/G_p$ is a smooth manifold that is $G$-equivariantly isomorphism to $X$, and the uniqueness also follows from the proposition.

PROP. (11.6.2.8) [Quotients of Lie Groups by Discrete Subgroups]. Let $G$ be a Lie group and $\Gamma$ a discrete subgroup of $G$, then $G/\Gamma$ is a smooth manifold, and the quotient map $G \to G/\Gamma$ is a smooth normal covering.

Proof: (11.6.1.4) and the proof of (11.6.2.6) shows $\Gamma$ acts smoothly, freely, and properly on $G$ on the right. Then the theorem is a consequence of (11.1.1.10).

PROP. (11.6.2.9) [Contractible Homogeneous Space]. If $X$ is a homogeneous $G$-manifold that is contractible, $x \in X$, then $G$ is diffeomorphic to $G_x \times X$.

Proof:

PROP. (11.6.2.10) [Orientability of Homogenous Spaces]. Let $G$ be a Lie group and $X$ be a homogeneous manifold of $G$. Let $x \in X$ and $H = \text{Stab}_G(x)$.
1. \(X\) is orientable iff values of \(\text{Ad}(h)\) are of the same sign for any two element \(h_1, h_2 \in H\) lying in a same connected component of \(G\).

2. Show that when \(H\) is connected, \(X\) is orientable.

3. There exist a \(G\)-invariant volume form on \(X\) iff \(\text{Ad}(H) \subset SL(g/h)\).

**Prop. (11.6.2.11)** [Fiber Bundle of Homogenous Spaces]. Let \(G \in \mathcal{L} \text{ie}_\mathcal{Grt}_{\text{cpct}}, K \leq H \leq G\) be closed subgroups, then the map \(G/K \to G/H\) is a \(G\)-locally trivial fiber bundle.

**Proof:**

\[
\text{Gal}\{X_1, \ldots, X_n\} \leq K
\]

The **Grassmannian manifold** \(\text{Gr}(k, \mathbb{K}^n)\) is defined to be the set of \(k\)-dimensional spaces in \(\mathbb{K}^n\). \(U(n, \mathbb{K})\) acts transitively on \(\text{Gr}(k, \mathbb{K}^n)\), and the stabilizer is \(U(k, \mathbb{K}) \times U(n-k, \mathbb{K})\). Thus \(\text{Gr}(k, \mathbb{K}^n)\) is a homogeneous \(U(n, \mathbb{K})\)-space by (11.6.2.7), and \(U(n, \mathbb{K}) \to \text{Gr}(k, \mathbb{K}^n)\) is a fiber bundle with fiber \(U(k, \mathbb{K}) \times U(n-k, \mathbb{K})\) by (11.6.2.11).

- The **Stiefel manifold** \(V_k(\mathbb{K}^n)\) of orthonormal \(k\)-frames in \(\mathbb{K}^n\) is defined to be the set of tuples \((v_1, \ldots, v_k)\) in \(\mathbb{K}^n\) that \((v_i, v_j) = \delta_{ij}\). \(U(n, \mathbb{K})\) acts transitively on \(V_k(\mathbb{K}^n)\) with stabilizer \(U(n-k, \mathbb{K})\). Thus \(V_k(\mathbb{K}^n)\) is a homogeneous \(U(n, \mathbb{K})\)-space by (11.6.2.7), and \(U(n, \mathbb{K}) \to V_k(\mathbb{K}^n)\) is a fiber bundle with fiber \(U(n-k, \mathbb{K})\), and \(V_k(\mathbb{K}^n) \to \text{Gr}(k, \mathbb{K}^n)\) is a fiber bundle with fiber \(U(k, \mathbb{K})\).

- The **flag Variety**.

**Proof:**

1. Let \(\dim X = n\). \(X\) is orientable iff there is a non-vanishing \(n\)-form on \(X\). Because \(o_x : G \to X\) is submersive, choose \(n\) left invariant vector fields \(X_1, \ldots, X_n\) that \((d o_x)_e(v_i)\) generate \(T_x(X)\), then by homogeneity, \((d o_x)_g(X_{ig})\) generate \(T_gx(X)\) for any \(g \in G\). Thus \(X\) is orientable iff there is a \(n\)-form \(\omega\) on \(G\) that satisfies \(r^*_h \omega = \omega\). \(\omega_g = \Delta(g)^{\ast}l_{g^{-1}}^* \omega_e\) for some \(\Delta(g) \in \mathbb{R}^{*}\), and for any \(h \in H\), and \(\omega(X_1, \ldots, X_n) \neq 0\).

If such a form exists, then \(\Delta(gh)^{\ast}l_{(gh)^{-1}}^* \omega_e = r^*_h l_{g^{-1}}^* \omega_e\), which is equivalent to \(\Delta(g) \text{Ad}(h)^{\ast} \omega_e = \Delta(gh)^{\ast} \omega_e\) for any \(h \in H\), thus values of \(\text{Ad}(h)\) are of the same sign for any two element \(h_1, h_2 \in H\) lying in a same connected component of \(G\).

Conversely, if values of \(\text{Ad}(h_i)\) are of the same sign for any two element \(h_1, h_2 \in H\) lying in a same connected component of \(G\), then we can define \(\omega\) as above, where \(\Delta(h) = \text{det}(\text{Ad}(h)[(g/h)])\), and extend \(\Delta\) to \(G\) that satisfy \(\Delta(gh) = \Delta(g)\Delta(h)\). This can be because \(G\) is a fiber bundle over \(G/H\).

2. When \(H\) is connected, clearly the values of \(\text{Ad}(H)\) are of the same sign.

3. The proof is the same as that of item1. In this case, all \(\Delta(g) = 1\), thus the existence of \(G\)-invariant volume form on \(X\) is equivalent to \(\text{Ad}(H) \subset SL(g/h)\).

**3 Lie Theory**

**Lie Algebras of Lie Groups**

**Def. (11.6.3.1)** [Invariant Vector Fields]. Let \(G\) be a Lie group, then a smooth vector field \(X\) on \(G\) is called left-invariant if \(d(L_g)_{g'}(X_{g'}) = X_{gg'}\) for any \(g, g' \in G\). The set of left-invariant vector fields on \(G\) is denoted by \(\text{Lie}(G)\).

**Prop. (11.6.3.2).** If \(X, Y\) are left-invariant vector fields over \(G\), then \([X, Y]\) is also left-invariant, by (11.1.2.13).
Prop. (11.6.3.3) [Invariant Vector Fields and Tangent Spaces]. Let $G$ be a Lie group, then the evaluation map $\text{Lie}(G) \to \mathfrak{g} : X \mapsto X_e$ is a vector space isomorphism.

Proof: The inverse map is given by $X \mapsto (L_X)_{e} = d(L_g)_{e}(X)$. This is clearly a left-invariant vector field. It suffices to show that this $\tilde{X}$ is smooth. By (11.1.2.10), it suffices to show $L_X(f)$ is smooth for any smooth function $f$.

$$L_X(f)(g) = d(L_g)_{e}(X)(f)(g) = X(L_g f)(0) = \frac{d}{dt}|_0 f(g \exp(tX))$$
which is a differential of a smooth map $\mathbb{R} \times G \to GL : (t, g) \mapsto f(g \exp(tX))$, so it is smooth in $g$. □

Cor. (11.6.3.4) [Lie Group is Parallelizable]. Every Lie group admits a left-invariant smooth global frame, thus any Lie group is parallelizable.

Prop. (11.6.3.5). If $X \in \mathfrak{g}$ corresponds to a left-invariant vector field $L_X$, then for any $g \in G$,

$$d(R_g)_p((L_X)_p) = (L_{\text{Ad}(g^{-1})X})_{pg}.$$

Proof: $d(R_g)_p((L_X)_p)(f)(pg) = (L_X)_p(R_g f) = d(L_p)_{e}(X)(R_g f)$

$$= X(L_p R_g f) = \frac{d}{dt}|_0 f(p \exp(tX)g)$$

$$= \frac{d}{dt}|_0 f(p \exp(t \text{Ad}(g^{-1})X)) = (\text{Ad}(g^{-1})X)(L_p f))$$

$$= (L_{\text{Ad}(g^{-1})X})_{pg}(f)(pg)$$

□

Def. (11.6.3.6) [Lie Algebra of a Lie Group]. If $G$ is a Lie group, $\text{Lie}(G)$ is a Lie algebra w.r.t. the Lie bracket (11.1.2.12). It is called the Lie algebra associated to $G$.

Proof: This is clear from the definition $[X, Y](f) = XY(f) - YX(f)$. □

Prop. (11.6.3.7) [Induced Map of Lie Algebras]. A homomorphism $F : G \to H$ of Lie groups induces a morphism of their Lie algebras via the tangent space.

Proof: For any $X \in \text{Lie}(G)$, define $F_*(X)_g = (dL_g)_e(dF_e(X_e))$, then this is a left-invariant vector field, and it clearly corresponds to the tangent map via isomorphism in (11.6.3.3). This map is a Lie algebra map by a variant of (11.1.2.13). □

Cor. (11.6.3.8). If $H \subset G$ is a Lie subgroup, then there is a natural isomorphism

$$\mathfrak{h} \cong \{ X \in \text{Lie}(G) | X_e \in T_eH \}.$$

In particular, the tangent space $\mathfrak{h}$ of $H$ is a Lie subalgebra of $\mathfrak{g}$.

$$\text{Lie}(H) \xrightarrow{X \mapsto X_e} \mathfrak{h} \xleftarrow{\iota_*} \text{Lie}(G) \xrightarrow{X \mapsto X_e} \mathfrak{g}$$

Proof: There is a commutative diagram □
Prop. (11.6.3.9) [Covering of Lie Groups]. Let $F : G \to H$ be a homomorphism of connected Lie groups, then the following are equivalent:

- $F$ is surjective with discrete kernel.
- $F$ is a smooth covering map.
- $F$ is a local diffeomorphism.
- The induced homomorphism $F_* : \mathfrak{g} \to \mathfrak{h}$ is an isomorphism.

Proof: 1 → 2: $F$ is surjective thus $H$ is a homogeneous $G$-space, so (11.6.2.6) shows $H \cong G/\ker(F)$. And $G \to G/\ker(F)$ is a smooth covering map by (11.6.2.8).

2 → 3 is trivial.

3 → 1: If $F$ is a local diffeomorphism, then $\ker(F)$ is discrete, and $F$ is open. Thus $F(G)$ is an open subgroup of $H$, thus all of $H$ because $H$ is connected (3.8.1.3).

3 → 4 is trivial. 4 → 3 is by inverse function theorem. □

Cor. (11.6.3.10) [Homomorphism with Discrete Kernel]. Let $G \to H$ be a homomorphism of Lie groups of the same dimension with discrete kernel and $H$ connected, then it is a covering space map, and the kernel is in the center of $G$, by (11.6.1.6).

Proof: This homomorphism is locally injective at 1, so it has rank $\dim G = \dim H$, so it is local diffeomorphism. In particular, the image contains a nbhd of 1 in $H$, thus it contains all $H$ by (3.8.1.3). □

Prop. (11.6.3.11) [Universal Covering Lie Group]. If $G$ is a connected Lie group, then its universal covering space $\tilde{G}$ can be given a Lie group structure that the covering map is a group homomorphism. Moreover, the group structure is unique up to isomorphism over $G$. Moreover, the kernel of $\tilde{G} \to G$ is a discrete central subgroup of $\tilde{G}$.

Proof: Because $\tilde{G}$ is simply connected, so does $\tilde{G} \times \tilde{G}$, let $\tilde{e}$ be an element over $e$, we can lift the map $\tilde{G} \times \tilde{G} \to \tilde{G} \times \tilde{G}$ to a map $\tilde{m} : \tilde{G} \times \tilde{G} \to \tilde{G}$ that $\tilde{m}(\tilde{e}, \tilde{e}) = \tilde{e}$. Similar we can lift an inverse map $\tilde{i}$ that $\tilde{i}(\tilde{e}) = \tilde{e}$. These maps are smooth because $\pi : \tilde{G} \to G$ is a local diffeomorphism.

It’s left to show that $(\tilde{m}, \tilde{i})$ makes $\tilde{G}$ into a Lie group: For example, the map $L_{\tilde{G}} : \tilde{G} \to \tilde{G}$ is a lift of $id_{\tilde{G}}$ and it coincides with $id_{\tilde{G}}$ on a point $\tilde{e}$, thus it is just $id_{\tilde{G}}$, which means $\tilde{e}$ is a left identity. The rest is easy.

For the uniqueness: By the universal property of covering, if there are two coverings, we can lift it to a map connecting them that maps identity to identity, then show it is a group homomorphism.

The last assertion follows from (11.6.3.10). □

Prop. (11.6.3.12) [Lie Subalgebras and Subgroups]. For a Lie group $G$, for any lie subalgebra $\mathfrak{h} \subset \mathfrak{g}$, there exists uniquely a connected Lie subgroup $H$ s.t. $\mathfrak{h}$ is the lie algebra of $H$.

Proof: By (11.1.3.1), there is a maximal connected manifold $H$ corresponding to $\mathfrak{h}$, we only need to show that it is a group. But the left invariance of $\mathfrak{h}$ shows that $HH \subset H$ because $H$ is maximal. Cf. [Lee13]P506. □

Cor. (11.6.3.13). If $G_1$ is a simply connected Lie group and $G_2$ is a connected Lie group, then any Lie algebra homomorphism $\tilde{h} : \mathfrak{g}_1 \to \mathfrak{g}_2$ can be lifted to a unique Lie group homomorphism.
Proof: Consider the image of $\tilde{h} : \Gamma(\tilde{h}) \subset \mathfrak{g}_1 \times \mathfrak{g}_2$, which is a Lie subalgebra. First notice a Lie group homomorphism $h$ is equivalent to a Lie subgroup $G_h$ of $G_1 \times G_2$ such that $\pi_1|G_h$ is a diffeomorphism onto $G_1$. And this Lie homomorphism induces the desired Lie algebra homomorphism iff the Lie algebra of $G_h$ is just $\tilde{h}$.

(11.6.3.12) shows that there exists a unique Lie group $G$ in $G_1 \times G_2$ with Lie subalgebra $\Gamma(\tilde{h})$.

The projection $\pi_1|G$ is a diffeomorphism onto $G_1$, because the tangent map at $e$ is an isomorphism, thus a local diffeomorphism and by (11.6.3.10) a covering map, so it must be an isomorphism because $G_1$ is simply connected and $G$ is connected. □

Cor.(11.6.3.14) [Representations of Simply-Connected Lie Groups]. The category of representations of s simply-connected Lie groups is equivalent to the category of representations of its Lie algebra.

Thm.(11.6.3.15) [The Lie Correspondence].

- The category of finite dimensional Lie algebras is equivalent to the category of simply connected Lie groups.
- For a f.d. Lie algebra $\mathfrak{g}$, the connected Lie groups with Lie algebras isomorphic to $\mathfrak{g}$ corresponds to $G/\Gamma$, where $G$ is a simply connected subgroup with Lie algebra $\mathfrak{g}$, and $\Gamma$ is a discrete central subgroup of $G$.

Proof: 1: By (11.6.3.12)(11.6.3.13) together with Ado’s theorem??.

2: (11.6.3.11) and (11.6.3.9) shows any Lie group is a quotient of its universal covering Lie group by a discrete central subgroup. Conversely, for any discrete central subgroup, $G/\Gamma$ is a Lie subgroup and $\pi : G \rightarrow G/\Gamma$ is a homomorphism with kernel $\Gamma$ by (11.6.1.4) and (11.6.1.28), thus $\text{Lie}(G) = \text{Lie}(G/\Gamma) \cong \mathfrak{g}(11.6.1.28)$. □

Prop.(11.6.3.16) [Ideals and Normal Subgroups]. Let $G$ be a connected Lie group and $H$ a connected Lie subgroup, then $H$ is a normal subgroup of $G$ iff $\mathfrak{h}$ is an ideal of $\mathfrak{g}$.

Proof: Because $G, H$ are both connected, (3.8.1.3) shows $H$ is normal in $G$ iff for any $X \in \mathfrak{g}, Y \in \mathfrak{h}$, $\exp(X) \exp(Y) \exp(X)^{-1} \in H$. Taking derivative w.r.t. $Y$, this is equivalent to $d(\text{Ad}(\exp(X)))(Y) = \text{ad}(X)Y \in \mathfrak{h}(11.6.1.12)$, by (11.6.1.25), which is equivalent to $\mathfrak{h}$ being an ideal of $\mathfrak{g}$. □

Prop.(11.6.3.17) [Center]. Let $G$ be a connected subgroup with Lie algebra $\mathfrak{g}$ and $Z$ the center of $G$, $\mathfrak{z}$ the center of $\mathfrak{g}$, then $Z$ is a closed Lie subgroup of $G$ with Lie algebra $\mathfrak{z}$.

Proof: Because $G$ is connected, $g \in Z$ iff $g$ commutes with all $\exp(tX), X \in \mathfrak{g}$. Thus $Z = \text{ker Ad}$. Now the assertion follows from (11.6.1.29). □

Prop.(11.6.3.18) [Chevalley’s Theorem]. Let $G$ be a complex connected Lie group and $\mathfrak{g}$ the Lie algebra of $G$, $\mathfrak{h}$ the Cartan subalgebra of $\mathfrak{g}$, and $W$ the Weyl group, then the restriction of functions induces a graded algebra isomorphism

$$\mathbb{C}[\mathfrak{g}]^G \cong \mathbb{C}[\mathfrak{h}]^W.$$

Proof: ? □
Classifications

Prop. (11.6.3.19) [Simply-Connected Compact Lie Groups]. Any simply connected compact Lie groups is a product of the following types:
- \( \text{Spin}(n) \) for \( n \geq 3 \).
- \( \text{SU}(2) \) for \( n \geq 2 \).
- \( \text{Sp}(n) \) for \( n \geq 1 \).
- \( E_6, E_7, E_8, F_4, G_2 \).

Proof: □

4 Classical Groups

In this subsection, Archimedean points of classical groups (7.3.5.1) are studied. For more classical groups, Cf. [Classical Groups Baker].

Def. (11.6.4.1) [Examples of Classical Groups]. Let \( K \) be either \( R, C, \)
- For any associative algebra \( K \) over a field, the general linear group \( GL(n, K) \) is the subgroup of \( M_n(K) \) consisting of invertible matrices.
- The unitary group \( U(n) \) is the subgroup of \( GL(n,C) \) consisting of matrices fixing a non-degenerate Hermitian form.
- The special unitary group \( SU(n) = U(n) \cap SL_n(C) \).
- The pseudo-unitary groups \( U(p,q,K) \): If \( K = R, \) it is the subgroup of \( GL(n,R) \) consisting of matrices preserving a bilinear form of signature \( (p,q) \). If \( K = C, \) it is the subgroup of \( GL(n,C) \) consisting of matrices preserving a Hermitian form of signature \( (p,q) \). If \( K = H, \) it is the subgroup of \( GL(n,H) \) consisting of matrices preserving a non-degenerate quaternionic Hermitian form of signature \( (p,q) \).
- The quaternionic orthogonal group \( O^*(2n) \) is the subgroup of \( GL(n,H) \) consisting of matrices preserving a non-degenerate quaternionic skew-Hermitian form \( (2.3.11.7) \). \( SO^*(2n) \) is the subgroup of \( O^*(2n) \) consisting of elements of determinant 1.
- \( PU(n) \) is the quotient group of \( SU(n) \) (or \( U(n) \)) by scalar matrices.

Proof: \( GL_n(K) \) has a natural smooth structure as an open subset of \( K^{n^2} \), and the multiplication map is clearly smooth, so it is a Lie group by (11.6.1.1). The other groups are closed subgroups of \( GL_n(K) \), so they have unique smooth manifold structure making them Lie subgroups of \( GL_n(K) \), by (11.6.1.22)(11.6.1.16). Finally the quotient group by normal closed subgroups have natural Lie group structure by (11.6.1.28). □

Prop. (11.6.4.2) [\( SU(2) \)].

\[
SU(2) = \{ A_{\alpha,\beta} = \begin{pmatrix} \alpha & \beta \\ -\beta & \alpha \end{pmatrix}, \alpha, \beta \in C, |\alpha|^2 + |\beta|^2 = 1 \}
\]

is isomorphic to the group of unit quaternions and diffeomorphic to \( S^3 \). The Lie algebra of \( SU(2) \) is isomorphic to \( \mathfrak{sl}_2(\mathbb{R}) \).
Proof: Let \( A = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in SU(2) \), then
\[
aa + b\bar{b} = 1, \quad ac + b\bar{d} = 0, \quad cc + d\bar{d} = 1, \quad ac - bd = 1.
\]

So \((c, d) = \lambda \cdot (-\bar{b}, \bar{a})\), and we can calculate \( \lambda = 1 \). So the first assertion follows.

By (2.3.3.11.4), \( SU(2) \) is isomorphic to the group of unit quaternions, which is clearly isomorphic to \( S^3 \).

\[ \Box \]

Prop. (11.6.4.3) [Action of \( SU(2) \)].

- There is a double covering of Lie groups \( SU(2) \to SO(3) \) with kernel \( \{ \pm 1 \} \).
- There is a double covering of Lie groups \( SU(2) \times SU(2) \to SO(4) \) with kernel \( \{ \pm 1 \} \).

Proof: 1: Regard \( SU(2) \) as the group of unit quaternions and \( SO(3) \) the transformation group of pure unit quaternions, then \( SU(2) \to SO(3) \) is given by
\[
u \mapsto \left( v \mapsto uv\bar{v} \right).
\]

Because \( u \cdot \bar{v} \) preserves orthogonality relations, it preserves the space of pure quaternions, so it has image in \( O(3) \). But it has image in \( SO(3) \) because \( SU(2) \cong S^3 \) is connected. Its kernel is in the center of \( \mathbb{H} \), so must be \( \pm 1 \). Now (11.6.3.10) shows this is a covering space map.

2: Consider the action \( SU(2) \times SU(2) \) on the section of unit vectors of \( \mathbb{H} \): \((u, v)(z) = uzv^{-1} \). If \((u, v)\) is in the kernel of this map, then \( uv^{-1} = 1 \), so \( u = v \) and \( u \) is in the center of \( \mathbb{H} \), so \( u = v = \pm 1 \). Because \( \dim SU(2) = 3 \) and \( \dim SO(4) = 6 \), (11.6.3.10) shows this is a double cover.

\[ \Box \]

Prop. (11.6.4.4).

- There is a double cover \( SU(4) \to SO(6, \mathbb{R}) \) with kernel \( \{ \pm 1 \} \).
- There is a double cover \( SL(4, \mathbb{C}) \to SO(6, \mathbb{C}) \) with kernel \( \{ \pm 1 \} \).
- There is a double cover \( Sp(4, \mathbb{C}) \to SO(5, \mathbb{C}) \) with kernel \( \{ \pm 1 \} \).

Proof: 1: \( SU(4) \) acts on a 4-dimensional Hermitian space \( V \). Then it acts on the Hermitian space \( \wedge^2 V \). Consider the Hodge star operator \( * : \wedge^2 V \to \wedge^2 V (11.1.3.9) \), it is an anti-linear operator, \( *^2 = \text{id} \) and \( * \) commutes with \( SU(4) \) action. Then \( W = \ker(* - \text{id}) \) is a real vector space of dimension 6 that \( SU(4) \) acts on. This kernel of this action is the same as the kernel of the action \( \wedge^2 V \), which is \( \{ \pm 1 \} \).

The Hermitian form induces a symmetric form on \( W \): Take a conjugation on \( V \), because \( V = W \oplus iW \), \( W = \text{Im}(* + \text{id})V \). So for \( a, b \in W \), let \( a = *c + c, b = *d + d \), then \((a, b)\omega = ((*a, *b) + (*a, b) + (a, *b) + (a, b))\omega = *a \wedge b + \bar{a} \wedge \bar{b} + a \wedge b + *a \wedge \bar{b} \) is a real form. Then this representation induces a map \( SU(4) \to SO(6) \)(because \( SU(4) \) is connected). Because \( \dim SU(4) = \dim SO(6) = 6 \), it is a double cover by (11.6.3.10).

2: \( SL(4, \mathbb{C}) \) acts on a 4-dimensional complex vector space \( V \), then it acts on the space \( W = \wedge^2 V^* \). We construct a non-degenerate bilinear form on \( W \) given by \( \wedge : W \times W \to \wedge^4 V^* \cong \mathbb{C} \). Then \( SL(4, \mathbb{C}) \) preserves this bilinear form, thus induces a map \( SL(4, \mathbb{C}) \to SO(6, \mathbb{C}) \). The kernel of this map is \( \{ \pm 1 \} \), because if \( A \) preserves all \( v_1 \wedge v_2 \), then \( Av_1 \wedge Av_2 = v_1 \wedge v_2 \), so \( Av_1 \wedge Av_2 \wedge v_3 = 0 \), so \( Av_1 \in \{ v_1 \wedge v_2 \} \), or \( Av_2 \in \{ v_1 \wedge v_3 \} \cap \{ Av_1 \wedge v_3 \} \cap \{ Av_1 \wedge v_2 \} = Av_1 \), then \( Av_1 \wedge Av_2 = 0 \), contradiction. So \( Av_1 \in \{ v_1 \wedge v_2 \} \). \( v_1, v_2 \) is arbitrary, thus \( A \) is diagonal, and it is clear \( A = \pm 1 \). Finally, \( SL(4, \mathbb{C}) \to SO(6, \mathbb{C}) \) is a double cover by (11.6.3.10).
3: The representation of $SL(4, \mathbb{C})$ on $W = \wedge^2 V^*$ restricts to a representation of $Sp(4, \mathbb{C})$, and it fixes the vector $\sigma = v_1^* \wedge v_2^* + v_1^* \wedge v_2^*$ by definition, so it also fixes the orthogonal $\{\sigma\}^\perp$, thus inducing a map $Sp(4, \mathbb{C}) \to SO(5, \mathbb{C})$ with kernel $\{\pm 1\}$, which is a double cover by $(11.6.3.10)$. 

**Prop. (11.6.4.5)** $[SU(1, 1) \text{ and } SL(2, \mathbb{R})]$. Let $SL(2, \mathbb{C})$ act on $\mathbb{P}^1(\mathbb{C})$ by linear transformations.

1. Prove that the stabilizer of the unit disk $D$ is

$$SU(1, 1) = \left\{ \begin{bmatrix} a & b \\ b & \bar{a} \end{bmatrix} \big\| |a|^2 - |b|^2 = 1 \right\}.$$ 

2. Prove that $SU(1, 1)$ is conjugate to $SL(2, \mathbb{R})$ in $SL(2, \mathbb{C})$.

3. Prove that the subgroup of $SU(1, 1)$ fixing $0 \in D$ is the subgroup of rotations $\{\text{diag}(e^{i\theta/2}, e^{-i\theta/2})\}$.

**Proof:** 3: By Schwartz lemma $(10.5.2.23)$, any element stabilizing $D$ and fixing $0$ acts as $z \mapsto e^{i\theta}z$ for some $\theta$. The only elements of $SL(2, \mathbb{C})$ that acts this way are of the form $\{\text{diag}(e^{i\theta/2}, e^{-i\theta/2})\}$.

1, 2: We first prove that $SU(1, 1)$ is of the form: If $\begin{bmatrix} a & b \\ c & d \end{bmatrix} \subset SU(1, 1)$, then

$$|a|^2 - |c|^2 = 1, \quad ad - bc = 1$$

which means $(b, d) = \lambda(\sigma, \bar{\sigma})$, and $\lambda = 1$.

Let $C = \frac{1}{\sqrt{2}e^{i\pi/4}} \begin{bmatrix} 1 & -i \\ 1 & i \end{bmatrix}$, then $C$ induces an isomorphism between $\mathcal{H}$ and $D$, because $\frac{z - i}{z + i} \in D$ iff $|z - i| < |z + i|$ iff $z$ is in the upper half plane. By this isomorphism and item 3, the element of $SL(2, \mathbb{C})$ stabilizing $D$ and fixing $i$ is of the group $SO(2, \mathbb{R}) \subset SL(2, \mathbb{R})$.

Notice that $SL(2, \mathbb{R})$ preserves $\mathcal{H}$ by $(10.5.1.8)$, and it acts transitively on it because $\sqrt{y} \begin{bmatrix} y & x \\ 1 & 1 \end{bmatrix}$ maps $i$ to $x + iy \in \mathcal{H}$. Now if $\gamma \in SL(2, \mathbb{C})$ stabilizes $\mathcal{H}$, then $\gamma g$ fixes $i$ for some $g \in SL(2, \mathbb{R})$, thus $\gamma g \in SL(2, \mathbb{R})$, thus $\gamma \in SL(2, \mathbb{R})$. Thus we have shown the stabilizer of $\mathcal{H}$ is $SL(2, \mathbb{R})$. Then the stabilizer of $D$ is

$$C \cdot SL(2, \mathbb{R})C^{-1} = \left\{ \frac{1}{2i} \begin{bmatrix} 1 & -i \\ 1 & i \end{bmatrix} \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} i & i \\ -1 & 1 \end{bmatrix} \big| a, b, c, d \in \mathbb{R}, ad - bc = 1 \right\}$$

which is exactly $SU(1, 1)$. So we get 1 and 2. 

**Prop. (11.6.4.6)** $[Sp(2, \mathbb{K}) \text{ and } SL(2, \mathbb{K})]$. For any field $\mathbb{K}$, $Sp(2, \mathbb{K}) \cong SL(2, \mathbb{K})$: They both consist of linear maps preserving the differential form $dx \wedge dy$.

**Prop. (11.6.4.7)** [Center of $SU(p, q)$], $Z_U(p, q)(SU(p, q))$ are all scalar matrices.

**Proof:** Firstly we consider $Z_U(2)(SU(2))$, if $A \in Z(SU(2))$, then it commutes with $\text{diag}(i, -i)$, so $A$ is a scalar. Similarly, if $A \in Z_U(1, 1)(SU(1, 1))$, then $A$ commutes with $\text{diag}(i, -i)$, thus $A$ is a scalar.

If $X \in Z(SU(p, q))$ is not a scalar matrix, then it has two eigenvectors $s, t$ with different eigenvalues. Consider the space $V$ generated by $s, t$ and its orthogonal complement, then $X$ restricted to this space is in the center of $U(V)$. Now $SU(V) \cong SU(1, 1)$ or $SU(2)$, both have the set of scalar matrices as center, so $X$ cannot have different eigenvalue, contradiction. Thus $X$ is a scalar matrix.
Prop. (11.6.4.8) \( PGL(2, \mathbb{C}) \cong SO(3, \mathbb{C}) \). \( V \cong \mathbb{C}^2 \) has a natural symmetric form \( (x, y) \mapsto x \wedge y \cong \mathbb{C} \), and this form is preserved by \( SL(2, \mathbb{C}) \) by definition. The kernel of this map is \( \{ \pm 1 \} \). Thus \( SL(2, \mathbb{C}) \) acts on \( \text{Sym}^2(V) \), thus induces a map \( PGL(2, \mathbb{C}) \to SO(3) \), which an isomorphism by (11.6.3.10).

Prop. (11.6.4.9) [Real and Complex Matrices]. \( GL_n(\mathbb{C}) \) can be embedded into \( GL_{2n}(\mathbb{R}) \), with determinant \( |\det|^2 \). And in this way, \( U(n) \) is mapped into \( O(2n, \mathbb{R}) \). Also, \( O(n, \mathbb{R}) \) embeds into \( U(n) \) diagonally.

Proof: \[
X + iy \mapsto \begin{bmatrix} X & -Y \\ Y & X \end{bmatrix} \sim \begin{bmatrix} X & -Y \\ iX + Y & X - iy \end{bmatrix} \sim \begin{bmatrix} X + iy & Y \\ 0 & X - iy \end{bmatrix}
\]

Prop. (11.6.4.10) [Symplectic Groups].
- \( U(p, q, \mathbb{H}) = Sp(2n, \mathbb{C}) \cap U(2p, 2q, \mathbb{C}) \). \( U(n, \mathbb{H}) = U(n, 0, \mathbb{H}) \) is also denoted by \( Sp(n) \), called the compact symplectic group.
- \( O^*(2n) = U(n, n) \cap O(2n, \mathbb{C}) \).
- \( Sp(2n, \mathbb{C}) = SL(n, \mathbb{H}) \).
- \( Sp(2n, \mathbb{R}) \cap O(2n, \mathbb{R}) = Sp(2n, \mathbb{R}) \cap GL(n, \mathbb{C}) = O(2n, \mathbb{R}) \cap GL(n, \mathbb{C}) = U(n) = \left\{ \begin{bmatrix} X & -Y \\ Y & X \end{bmatrix} : X + iy \in U(n) \right\} \).

Proof: 1: By (2.3.11.9), notice that any \( \mathbb{C} \)-linear automorphism preserving \( B_1 \) and \( B_2 \) is \( \mathbb{H} \)-linear.
2: By (2.3.11.9), notice that any \( \mathbb{C} \)-linear automorphism preserving \( B_1 \) and \( B_2 \) is \( \mathbb{H} \)-linear.
3: If \( A \in Sp(2n, \mathbb{R}) \cap O(2n, \mathbb{R}) \), then \( AA^t = A^tA = 1 \), \( A^tJA = 1 \), then \( AJ = JA \). The rest and the other identities are easy by (11.6.4.9). □

Spin Groups

Prop. (11.6.4.11). Let \( Cl_{r,s} \) denote the real Clifford algebra of signature \( r - s \), then
\[
Cl_{1,0} \cong \mathbb{C}, \quad Cl_{0,1} \cong \mathbb{R} \oplus \mathbb{R}, \quad Cl_{2,0} \cong \mathbb{H} \subset M(2, \mathbb{C}), \quad Cl_{0,2} \cong R(2) = M(2, \mathbb{R}),
\]
And we have
\[
Cl_{n+2,0} \cong Cl_{0,n} \otimes Cl_{2,0}, \quad Cl_{0,n+2} \cong Cl_{n,0} \otimes Cl_{0,2}.
\]
by the mapping \( e_i \rightarrow e_i \otimes e'_1 e'_2 \), \( e_{n+j} \rightarrow 1 \otimes e'_j \).
So we have
\[
Cl_{n+8,0} \cong Cl_n \otimes \mathbb{R}(16), \quad Cl_{n+2,0} = Cl_{n+2,0} \otimes \mathbb{C} = Cl_{n,0} \otimes \mathbb{C}(2).
\]
because \( \mathbb{H} \otimes \mathbb{C} = \mathbb{C}(2) \), and
\[
\begin{bmatrix}
\begin{array}{cccccccc}
1 & 2 & 3 & 4 & 5 & 6 & 7 \\
Cl_{0,0} & R & C & H & H \oplus H & R(2) & R(8) & R(8) \oplus R(8)
\end{array}
\end{bmatrix}
\]
The Clifford algebra is a \( Z_2 \)-graded algebra, \( Cl = Cl^0 \otimes Cl^1 \) and \( Cl_{n-1} \cong Cl_n^0 \) by the mapping \( e_i \rightarrow e_i \otimes e_{n+1} \). This is in fact the decomposition of the chirality operator \( \Gamma = (-1)^{i(n+1)/2}e_1 e_2 \cdots e_n, \Gamma^2 = 1 \).
Prop. (11.6.4.12). For $n$ even, $C(V)$ is naturally isomorphic to $\text{End}_C(\Lambda^*W)$, where $W = \{ \frac{1}{\sqrt{2}} (e_{2i-1} - ie_{2i}) \}$. This isomorphism is not obvious and restrict to a Spinor representation of $\text{Spin}(n)$ and $\rho(\Gamma)^2 = 1$ induce two representations of $Cl(n)^0$, in particular $\text{Spin}(n)$, called the (half Spinor representations). This has a unique extension to representation of $\text{Pin}^\circ$. $\Lambda^*W$ comes with a Hermitian metric which is preserved by the action of $\text{Pin}(n)$ (check). So the image is $SO(n)$ is in $SO(\Lambda^*W)$. Cf.[Jost Geometric analysis P72].

Def. (11.6.4.13) $[\text{Spin}(n)]$, denote $\text{Pin}(n)$ as the group in $Cl_n$ generated by $v_i$ of norm 1. Because $v_i \cdot v_i = -1$, it is a group. And denote $\text{Spin}(n)$ as the subgroup of $\text{Pin}(n)$ generated by even number of $v_i$s.

Prop. (11.6.4.14) [Action of $\text{Spin}(n)$]. The conjugation action $Ad(v) = v(\cdot)v = \text{reflection w.r.t} v$, maps $\text{Pin}(n)$ to $O(n)$ and $\text{Spin}(n)$ to $SO(n)$. The kernel of this mapping is $\{ \pm 1 \}$ when $n$ is even. This is a double covering of $SO(n)$ and $O(n)$, it is nontrivial because $1, -1$ is connected by $(\cos te_1 + \sin te_2)(\cos te_1 - \sin te_2)$.

In particular, $\text{Spin}(n)$ is a universal covering of $SO(n)$ and thus simply-connected for $n \geq 3$.

Proof: Let $\alpha = e_i \beta + \gamma$, then $\beta, \gamma \in Cl^0$ and so $\alpha = ce_1 \ldots e_n + d$, and $c$ can happen only when $n$ is odd. □

Prop. (11.6.4.15) [Center of $\text{Spin}(n)$]. $Z(\text{Spin}(n)) = \begin{cases} S^1 & n = 2 \\ Z/2Z & n = 2k + 1, \\ Z/2Z \oplus Z/2Z & n = 4k, \\ Z/4Z & n = 4k + 2, \end{cases}$

Proof: □

Prop. (11.6.4.16) [Low Dimensional Accidental Isomorphisms].

- $\text{Spin}(2) \cong SO(2) \cong U(1)$.
- $\text{Spin}(3) \cong SU(2) \cong Sp(1)$
- $\text{Spin}(4) \cong SU(2) \times SU(2)$ because they are both universal coverings of $SO(4)$, by (11.6.4.17) and (11.6.4.14).
- $\text{Spin}(5) \cong Sp(2)$.
- $\text{Spin}(6) \cong SU(4)$.

Proof: 2: because $\text{Spin}(3), SU(2)$ are both universal covering of $SO(3)$, by (11.6.4.17) and (11.6.4.14), and $Sp(1)$ acts transitively on the set of unit vectors in $H$ with trivial kernel. □

Fundamental Groups

Prop. (11.6.4.17).

- $SU(n-1) \rightarrow SU(n) \rightarrow S^{2n-1}$ shows $SU(n)$ are connected and simply connected. Also $\pi_2(SU(n)) \cong \pi_2(SU(2)) \cong \pi_2(S^3) = 0$.
- $SO(n-1) \rightarrow SO(n) \rightarrow S^{n-1}$ shows $SO(n)$ are connected and $\pi_1(SO(n)) \cong \pi_1(SO(3)) = Z/2Z$ for $n \geq 3$ by (11.6.4.3) and (11.6.4.2). And $\pi_1(SO(2)) = Z$. 
11.6. LIE GROUPS

- \( U(n-1) \to U(n) \to S^{2n-1} \) shows \( U(n) \) are connected and \( \pi_1(U(n)) \cong \mathbb{Z} \).
- \( SO(n, \mathbb{R}) \) is a deformation retraction of \( SL(n, \mathbb{R}) \), and \( SU(n) \) is a deformation retraction of \( SL(n, \mathbb{C}) \).
- \( \pi_1(PSO(n)) = \begin{cases} 
\mathbb{Z} & n = 2 \\
\mathbb{Z}/2\mathbb{Z} & n = 2k + 1, \\
\mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z} & n = 4k, \\
\mathbb{Z}/4\mathbb{Z} & n = 4k + 2, 
\end{cases} \)

Because for \( n \geq 3 \), its universal covering is \( Spin(n) \), so \( \pi_1(PS(n)) = Z(Spin(n)) \).

- \( \pi_1(PSU(n)) = Z/nZ \).
- \( Sp(n-1) \to Sp(n) \to S^{4n-1} \) shows \( Sp(n) \) are connected and simply connected.
- \( \pi_1(Sp(2n, \mathbb{R})) = \pi_1(U(n)) = \mathbb{Z} \) and the determinant induces an isomorphism onto \( \pi_1(S^1) \). In fact, this is used to define the Maslov index.

Generals

Prop. (11.6.4.18) [Finite Subgroups of \( SO(3, \mathbb{R}) \)]. Every finite subgroup of \( SO(3, \mathbb{R}) \) is conjugate to one of the following:

- the cyclic group \( C_n \) generated by rotation.
- the dihedral group \( D_{2n} \) generated by adjoining a reflection to the rotation.
- the group \( A_4 \) of rotation of the tetrahedron.
- the group \( S_4 \) of rotations of the octahedron.
- the group \( A_5 \) of rotations of the icosahedron.

Proof: Cf.[Dornhoff, Group Representation Theory, 1971 Part A, Chap26]. □

Prop. (11.6.4.19) [Image of Exponential Maps].

- The exponential map for \( GL_n(\mathbb{C}) \) is surjective.
- The image of the exponential map for \( GL_n(\mathbb{R}) \) is \( GL_n(\mathbb{R})^2 \).
- The image of exponential map for \( B_+ \) which is the subgroup of \( GL(n, \mathbb{R}) \) consisting of upper-triangular matrices with positive entries, is surjective.
- The exponential defines a diffeomorphism from the space of Hermitian(symmetric) matrices to positive definite Hermitian(symmetric) matrices in \( GL(n, \mathbb{C})(GL(n, \mathbb{R})) \).
- The exponential for a compact Lie group is surjective, by (11.6.8.6) and (11.6.8.2).

Proof: 1: Use Jordan forms. Notice the logarithm of \( (cI + N) \), \( c \neq 0 \) is definable for \( N \) nilpotent, and it is a polynomial function of the matrix itself.

2: It is clear the image is contained in \( GL(n, \mathbb{R})^2 \), conversely, we see from the complex case that any \( B \in GL(n, \mathbb{R}) \) is of the form \( \exp(P(B)) \) for some polynomial \( P \in \mathbb{C}[X] \), then \( T = B^2 = \exp(P(B) + \overline{P}(B)) \in \exp(GL(n, \mathbb{R})) \).

3: Use Jordan forms. Notice the logarithm of \( (cI + N) \), \( c \neq 0 \) is definable for \( N \) nilpotent and \( c > 0 \), and it is a polynomial function of the matrix itself, so it is also upper-triangular.
4: By (2.3.8.3) it is clearly surjective. For injectivity, consider $\exp(X) = \exp(Y)$, then at least $X, Y$ are both unitarily conjugate to the same diagonal matrix $\text{diag}(d_1, \ldots, d_n)$, and we may assume $Y = \text{diag}(d_1, \ldots, d_n)$, then

$$X = \tau^{-1}Y\tau, \quad \text{diag}(D_1, \ldots, D_n) = \tau^{-1}\text{diag}(D_1, \ldots, D_n)\tau$$

where $D_i = e^{d_i}$. Consequently, $\text{diag}(D_1^k, \ldots, D_n^k) = \tau^{-1}\text{diag}(D_1^k, \ldots, D_n^k)\tau$, and we can choose $c_i$ that $\sum c_i D_i^j = d_j$ for any $j$, because the Vandermonde matrix is nonsingular. Hence $\text{diag}(d_1, \ldots, d_n) = \tau^{-1}\text{diag}(d_1, \ldots, d_n)\tau$, so $X = Y$. □

5 Compact Lie Groups and Representations

Prop. (11.6.5.1). Any compact connected complex Lie group is Abelian. And it is a complex tori. So we only consider only compact real Lie groups.

Proof: Mimic the proof that Abelian variety is commutative (13.5.1.5), using a similar rigidity lemma. □

Cor. (11.6.5.2). $U(n)$ is not a complex Lie group, in particular not a complex algebraic variety.

Prop. (11.6.5.3). Let $G$ be a compact connected Lie group with Lie algebra $\mathfrak{g}$ and center $Z$. Let $G_{ss}$ be the connected subgroup of $G$ corresponding to the Lie subalgebra $[\mathfrak{g}, \mathfrak{g}] (11.6.3.12)$, then $G_{ss}$ has finite center, and $Z^0, G_{ss}$ are closed in $G$, and $G = Z^0G_{ss}$.


Prop. (11.6.5.4) [Compact Lie Group and Representations]. A compact topological group $G$ is a real Lie group iff it has a faithful real f.d. representation. And in this case, it is a closed subgroup of $U(n)$ for some $n$.

Proof: If it has a faithful f.d. representation, then $G \subset GL(n, \mathbb{R})$ compact hence closed, thus a Lie subgroup by (11.6.1.22).

Conversely, if $G$ is a Lie group, then we can choose a small nbhd $U$ of $e \in G$ that contains no non-trivial subgroup of $G$ (choose $\exp\left(\frac{1}{2}V\right)$ where $\exp$ is an diffeomorphism on $V$). Consider kernel $K_\pi$ for irreducible representations $\pi$ of $G$, then $\cap_\pi K_\pi = \emptyset$ by Gelfand-Raikov (10.9.2.22), in particular $\cap_\pi (K_\pi - U) = \emptyset$. But $G - U$ is compact, hence there are f.m. $\pi_i$ that $\cap_\pi K_{\pi_i} \subset U$, but by definition of $U$, $\cap_\pi K_{\pi_i} = \{e\}$, which gives a f.d. faithful representation of $G$, by (10.9.4.4). □

Prop. (11.6.5.5) [Reduction to Faithful Representations]. Let $V$ be a faithful f.d. representation of a compact Lie group $G$ and $Y$ is an irreducible f.d. representation of $G$, then $Y$ is a direct summand of $V^\otimes n \otimes V^* \otimes m$ for some $m, n \geq 0$. Moreover, if $G$ is unimodular, we can take $m = 0$.

Proof: Cf. [Etingof, P175]. □

Remark (11.6.5.6). Theory of Representations of compact Lie groups are a special case of abstract harmonic analysis 10.9.
Maximal Tori

Prop.(11.6.5.7)[Tori]. Any connected compact Abelian real Lie group is a torus.

Proof: By(11.6.4.19), the exponential map realizes \( \mathfrak{g} \) as the universal cover of \( G \), and the kernel is then a complete lattice \( \Lambda \) in \( \mathbb{R}^n \), so \( G \cong \mathbb{R}^n/\Lambda \cong (S^1)^n \). □

Prop.(11.6.5.8). The maximal tori in a compact Lie group \( G \) corresponds to the maximal Abelian subalgebras of \( \mathfrak{g} \).

Proof: Let \( T \) be a maximal tori, then \( t \) is maximal Abelian by fundamental theorem of Lie(11.6.3.12). Conversely, if \( t \) is a maximal tori, then the corresponding Lie subgroup \( T \) is Abelian, and \( T \) is also Abelian. The Lie algebra of \( T, T' \) are the same by maximality of \( t \), so \( T = T' \), and it is a torus by(11.6.5.7), and it is clearly maximal. □

Prop.(11.6.5.9). Let \( G \) be a compact connected Lie group with Lie algebra \( \mathfrak{g} \), then any two maximal Abelian subalgebra of \( \mathfrak{g} \) are conjugate via \( \text{Ad}(G) \).

Proof: Let \( t, t' \) be two maximal Abelian subalgebra of \( \mathfrak{g} \). As \( \mathfrak{g} \) is reductive(2.5.5.3), if we choose \( X \in t, X' \in t' \) that are not zero for any roots, then \( Z_{\mathfrak{g}}(X) = T, Z_{\mathfrak{g}}(X') = T' \). Let \( \langle \cdot, \cdot \rangle \) be an invariant inner product on \( \mathfrak{g} \) defined in(11.6.8.2), choose a \( g_0 \in G \) that \( (\text{Ad}(g_0)X, X') \) is maximal, then \( 0 = ([Z, \text{Ad}(g_0)X, X']) = (Z, [\text{Ad}(g_0)X, X']) \) for any \( Z \in \mathfrak{g} \), so \( \text{Ad}(g_0)X \in Z_{\mathfrak{g}}(X') = t' \). Thus \( t' \subset Z_{\mathfrak{g}}(\text{Ad}(g_0)X) = \text{Ad}(g_0)Z_{\mathfrak{g}}(X) = \text{Ad}(g_0)t \), and the equality holds as \( t' \) is maximal. □

Cor.(11.6.5.10)[Maximal Tori are Conjugate]. Let \( G \) be a compact connected Lie group, then any two maximal tori of \( G \) are conjugate via \( \text{Ad}(G) \).

Prop.(11.6.5.11). Let \( G \) be a compact connected Lie group, then any element of \( G \) is connected in a maximal torus.

Proof: By(11.6.4.19), this element is contained in a 1-parameter subgroup \( T \) of \( G \), and \( T \) is also Abelian, so is a torus by(11.6.5.7). Then choose a maximal torus containing \( T \). □

Cor.(11.6.5.12). The center of \( G \) is contained in any maximal torus, by(11.6.5.10).

Prop.(11.6.5.13). Let \( S \) be a torus in a compact Lie group \( G \) and \( g \in G \) that commutes with elements in \( S \), then there is a torus containing both \( S \) and \( g \).

Proof: Let \( A \) be the closure of \( \cup_{i \in \mathbb{Z}} g^i S \), and \( A_0 \) the identity component of \( A \), then as \( A \) is compact, \( A_0 \) is open in \( A \) and compact, so \( \cup_{i \in \mathbb{Z}} g^i A_0 = A \), and also \( A/A_0 \) is a cyclic group. As \( A_0 \) is a torus, we can find \( a \in A \) that the closure of \( \{a^n | n \in \mathbb{Z} \} \) is \( A \). By(11.6.4.19), let \( a = \exp_G(X) \), then the closure of the 1-parameter group generated by \( X \) is a torus containing both \( S \) and \( g \). □

Cor.(11.6.5.14). In a compact connected Lie group \( G \), then centralizer of a torus \( T \) is connected. In fact, it is the union of maximal tori containing \( T \). In particular, a maximal torus is self-centralizing.

Highest Weight Theory

Cf.[Compact Lie Groups, Sepanski].Chap7.
Examples of Representations

Prop.(11.6.5.15) [Representations of SU(2)]. SU(2) \cong S^3 is simply connected with Lie algebra sl(2, \mathbb{R})(11.6.4.2), thus we can use (11.6.3.14) and (15.15.1.14) to see that the representations of SU(2) are all of the form \( W_n \), where \( W_n \) is the representation of SU(2) on the space of homogenous polynomials of degree \( n \) in two variables \( x, y \) induced by \[
\begin{bmatrix}
a & b \\
c & d
\end{bmatrix}
\begin{bmatrix}
x \\
y
\end{bmatrix}
= \begin{bmatrix}
ax + by \\
ax + dy
\end{bmatrix}.
\]

Proof: Check the central character of the induced representations of Lie algebra. \( \square \)

Prop.(11.6.5.16). Let \( G = SO(n) \) for \( n \neq 2 \mod 4 \). Show that:

1. For any element \( g \in G \), \( g \) and \( g^{-1} \) are conjugate in \( SO(n) \).

2. Any irreducible finite-dimensional \( \mathbb{C} \)-representation \( V \) of \( G \) is isomorphic to its dual.

Proof: 1: By (2.3.8.16), if \( n = 2m + 1 \), \( g \) is orthogonally diagonal to a matrix of the form \( \text{diag}\{SO(2, \mathbb{R}), \ldots, SO(2, \mathbb{R}), 1\} \). Notice \( SO(2, \mathbb{R}) = \{k_\theta, \theta \in (0, 2\pi)\} \), where \( k_\theta = \begin{bmatrix}
\cos \theta & \sin \theta \\
-\sin \theta & \cos \theta
\end{bmatrix} \), and \( k_\theta^{-1} = k_{-\theta} = k^t_\theta \). If we take \( W = \text{diag}\{\begin{bmatrix}1 & 0 \\ 0 & 1\end{bmatrix}, \ldots, \begin{bmatrix}1 & 0 \\ 0 & 1\end{bmatrix}\} \), then \( W \in SO(n, \mathbb{R}) \) and \( WgW^{-1} = g^{-1} \).

If \( n = 4k \), then \( g \) is orthogonally diagonal to a matrix of the form \( \text{diag}\{SO(2, \mathbb{R}), \ldots, SO(2, \mathbb{R})\} \).

If we take \( W = \text{diag}\{\begin{bmatrix}1 & 0 \\ 1 & 1\end{bmatrix}, \ldots, \begin{bmatrix}1 & 0 \\ 1 & 1\end{bmatrix}\} \), then \( W \in SO(n, \mathbb{R}) \) and \( WgW^{-1} = g^{-1} \).

2: Because \( \chi_V(g) = \chi_V(g^{-1}) = \chi_V(g) \) as \( g, g' \) are in the same conjugacy class, \( V \) and \( V^* \) are isomorphic, because f.d. representations are determined by characters (2.4.1.13) (applied to the group algebra \( \mathbb{C}[G] \)). \( \square \)

Maximal Compact Subgroup

For maximal compact subgroup of general locally compact subgroups, Cf.1.

Prop.(11.6.5.17) [Uniqueness for Semisimple Lie group]. Maximal compact subgroup exists by (10.9.1.47), and for a semisimple Lie group \( G \), the maximal compact subgroup is unique up to conjugation.

Proof: Cf.[Wiki]. \( \square \)

Prop.(11.6.5.18) [Examples of Maximal Subgroups].

- \( O(n) \) is the maximal compact subgroup of \( GL(n, \mathbb{R}) \).
- \( SO(n) \) is the maximal compact subgroup of \( SL(n, \mathbb{R}) \).
- \( SO(m, n) \) is the maximal compact subgroup of \( S(O(m) \times O(n)) \).
- \( SO(n) \) is the maximal compact subgroup of \( SL(n, \mathbb{R}) \).
- \( SU(n) \) is the maximal compact subgroup of \( SL(n, \mathbb{C}) \).
- \( SU(m, n) \) is the maximal compact subgroup of \( S(U(m) \times U(n)) \).
- \( SO(n) \) is the maximal compact subgroup of \( SO(n, \mathbb{C}) \).
- \( U(n) \) is the maximal compact subgroup of \( GL(n, \mathbb{C}) \).
11.6. LIE GROUPS

- $SU(n)$ is the maximal compact subgroup of $SL(n, \mathbb{C})$.
- $Sp(n)$ is the maximal compact subgroup of $Sp(n, \mathbb{C})$, by (11.6.4.10).
- $Sp(m, n)$ is the maximal compact subgroup of $Sp(m) \times Sp(n)$.
- $Sp(n)$ is the maximal compact subgroup of $SL(n, \mathbb{H})$, by (11.6.4.10).
- $U(n)$ is the maximal compact subgroup of $O^*(n)$, by (11.6.4.10).

And the above maximal compact subgroups are also deformation retracts.

Proof: This follows from polar decomposition (11.6.6.2), notice that the projection of a compact group is a compact group in $\mathbb{R}^n$, so it is trivial.

6 Decompositions

Prop. (11.6.6.1) [Cartan Decomposition]. Let $G = GL(n, \mathbb{R}), K = O(n)$ or $G = GL(n, \mathbb{R})^+, K = SO(n)$, then every double coset $K \backslash G / K$ has a unique representation of diagonal matrix $D$ with decreasing positive entries.

Proof: For the existence, given $g$, consider $S = g^t g = k^{-1}_1 \text{diag}(\lambda_1, \ldots, \lambda_n)k_1$, where $k_1 \in SO(n)$ (2.3.8.3). Then consider

$$k_2 = g k^{-1}_1 \text{diag}(\lambda^{-1/2}_1, \ldots, \lambda^{-1/2}_n)$$

it is orthogonal and $g = k_2 \text{diag}(\lambda^{1/2}_1, \ldots, \lambda^{1/2}_n)k_1$.

For the uniqueness, consider $g k^{-1}_1 \text{diag}(\lambda^{-1/2}_1, \ldots, \lambda^{-1/2}_n)$ is orthogonal, thus $k_1 S k^{-1}_1$ is diagonal with decreasing positive entries, thus uniquely defined.

Prop. (11.6.6.2) [Polar Decomposition for Linear Groups]. Let $G \subset GL(n, \mathbb{C})$ be a closed linear group that is defined by the a family of real valued polynomials in the real and imaginary parts of entries of $G$, and $G$ is closed under conjugation. Let $K = G \cap U(n)$, and let $\mathfrak{p}$ be the subspace of Hermitian matrices in $\mathfrak{g}$, then the map $K \times \mathfrak{p} \rightarrow G : (k, X) \mapsto k \exp(X)$ is a homeomorphism. In particular, $G$ has $K$ as deformation retracts.

Proof: The $GL(n, \mathbb{C})$ case follows from (10.8.4.20) and (11.6.4.19), and for the general case, it suffices to show if $g \in G$ and $g = k \exp(X)$, then $X \in \mathfrak{g}$: By hypothesis, $g^t g = e^{2X} \in G$. Take a basis that $2X = \text{diag}(a_1, \ldots, a_n)$ with $a_i$ real, then $e^{2kX} = \text{diag}(e^{ka_1}, \ldots, e^{ka_n})$ are all in $G$. Then it can be easily shown any polynomial that vanishes at all such $e^{2kX}$ vanishes on all $e^{2tX}$, thus $X \in \mathfrak{g}$.

Cor. (11.6.6.3). $GL(n, \mathbb{R}) \cong P \cdot O(n)$, where $P$ is the set of positive symmetric matrix, by (11.6.4.19).

Prop. (11.6.6.4) [QR-Decomposition].
- Any real matrix $A$ has the form $A = QR$ where $Q$ is orthogonal and $R$ is upper triangular with positive diagonal entries. Moreover, if $A$ is invertible, then the decomposition is unique.
- Any complex matrix $A$ has the form $A = QR$ where $Q$ is unitary and $R$ is upper triangular with positive diagonal entries. Moreover, if $A$ is invertible, then the decomposition is unique.
- Any Quaternion matrix $A$ has the form $A = QR$ where $Q \in U(n, \mathbb{H})$ (11.6.4.10) and $R$ is upper triangular with positive diagonal entries. Moreover, if $A$ is invertible, then the decomposition is unique.
Proof: We only prove for $GL(n, \mathbb{R})$, the rest is similar. Use Gram-Schmidt orthogonalization: choose a basis $v = \{v_1, \ldots, v_n\}$ of $V$ and $A$ acts on $V$, then $A$ maps $\{v_1, \ldots, v_n\}$ to a set $\{w_1, \ldots, w_n\}$. Then we can define an orthonormal basis $\{e_1, \ldots, e_n\}$ that $v_k \in \text{span}\{e_1, \ldots, e_k\}$. Now let $\{w_1, \ldots, w_n\} = \{e_1, \ldots, e_n\}R$, then $R$ is upper triangular, and $Q = [e_1, \ldots, e_n]_v$ is orthogonal, and $A = QR$.

To make diagonal entries of $R$ positive by left multiplying a diagonal orthogonal matrix.

To show the uniqueness when $A$ is invertible, let $A = Q_1R_1 = Q_2R_2$, then $A^tA = R_1^tR_1 = R_2^tR_2$. Then $(R_2)^{-1}R_1^t = R_2R_1^{-1}$, where the LHS is lower-triangular and the RHS is upper-triangular, which means both of them are diagonal. Then if $\alpha_i$ are the diagonal entries of $R_1$ and $\beta_i$ are the diagonal entries of $R_2$, then $\alpha_i/\beta_i = \beta_i = \alpha_i$, which means $\alpha_i = \beta_i$, and $R_2R_1^{-1} = 1$. \hfill \Box

Prop. (11.6.6.5) [Bruhat Decomposition]. Let $K$ be a field, $B$ be the set of upper-triangular matrices, $N$ be the set of unipotent upper-triangular matrices, then

$$GL(n, K) = BWB = BWN$$

where $W$ is the set of permutation matrices, $B$ is the invertible upper triangular matrices, and the decomposition is a disjoint union w.r.t. $W$.

Moreover, if $K$ is a topological field, there is a lexicographical stratification $0 = W_0 \subset W_1 \subset \ldots \subset W_n$ of $GL(n, K)$ that $W_k$ is closed in $W_{k+1}$ and each $W_{k+1}\backslash W_k$ is a double coset $BwB$.

Proof: For any matrix $M \in GL(n, K)$, consider the first column, then there is a lowest term $a_{i_11}$ that are not zero, then we can left multiply an upper triangular matrix $b_1$ s.t. the first column of $b_1M$ has only one nonzero entry $a_{i_11} = 1$, then consider the second column but ignore the $k$-th row, we can find a lowest term $a_{i_22}$ that is non-zero, then left multiply an upper triangular matrix $b_2$ that the second column of $b_2b_1M$ has only one non-zero entry $a_{2i_2} = 1$. Now continuing this way, we find a permutation $\sigma$ that only the entries $a_{ij}$ that $j \geq \sigma^{-1}(i)$ are non-zero. Then we can find an upper triangular matrix $c$ that $b_nb_{n-1} \ldots b_1Mc$ is a permutation matrix $M_{\sigma^{-1}}$.

So we proved $BWB = GL(n, K)$. Now it suffices to show if $M_{\sigma_1}^{-1}bM_{\sigma_2} \in B$ for some $b \in B$, then $\sigma_1 = \sigma_2$. Because $M_{\sigma} = \sum_i e_{\sigma(i)i} = \sum_i e_{i\sigma^{-1}(i)}$,

$$M_{\sigma_1}^{-1}bM_{\sigma_2} = \sum_{ij} b_{\sigma_1(i)\sigma_2(j)}e_{ij}.$$ 

This is an element in $B$, both its $(\sigma_1^{-1}(k), \sigma_2^{-1}(k))$-entry is $b_{kk} \neq 0$, thus $\sigma_1^{-1}(k) \leq \sigma_2^{-1}(k)$, which implies $\sigma_1 = \sigma_2$. \hfill \Box

Cor. (11.6.6.6). If $N$ is the group of unipotent upper triangular matrices, then $GL(n, L) = BWN$.

Prop. (11.6.6.7) [Smith Normal Form]. Let $R$ be a PID, and $K$ its fraction field. Choose a representative $\mathcal{P}$ for associativity classes of any prime in $R$(to eliminate the distraction of units), then there is complete set of representatives for the double cosets of $GL(n, R) \backslash GL(n, K)/GL(n, R)$ consisting of diagonal matrices $\text{diag}(f_1, \ldots, f_n)$, where $f_i \in K$ are products of elements in $\mathcal{P}$, and $f_k$ divides $f_{k+1}$. Notice $GL(n, R)$ is the matrices with unit determinants in $R$.

Proof: For the uniqueness, clearly the row operators doesn’t change the greatest common divisor of $k \times k$ minors of $M$ for any $k$(change by a scalar but the diagonal entries are monic), thus the entries are determined by the minors of $M$.

For the existence, for any $g \in GL(n, K)$ there is an $r \in R$, that $rg$ has coefficients in $R$, and also $r$ is a product of elements in $\mathcal{P}$. let $M$ be the submodule of $R^n$ generated by the rows of $rg$, then
by the elementary divisor theorem (2.2.4.24), there exists a basis \( \xi_i \) for \( R^n \) and \( d_i \in R \) that \( d_i | d_{i+1} \), and \( \{d_i \xi_i\} \) form a basis of \( M \). We may assume \( d_i \) are products of elements in \( P \). Then the matrix \( \xi \) with rows \( \xi_i \) are in \( GL(n, R) \), and the rows of the matrix \( \text{diag}(d_1, \ldots, d_n) \xi \) span the same module as \( rg \). Then

\[
K_1 rg = \text{diag}(d_1, \ldots, d_n) \xi
\]

for some \( K_1 \in GL(n, R) \), so \( g \) are in the same double coset as \( \text{diag}(r^{-1}d_1, \ldots, r^{-1}d_n) \). □

Prop. (11.6.6.8) [Iwasawa Decomposition].

7 Semisimple Lie Groups

Def. (11.6.7.1) [Semisimple Lie Group]. A semisimple/solvable/nilpotent/simple Lie group is a Lie group with a semisimple/solvable/nilpotent/simple Lie algebra.

Def. (11.6.7.2) [Adjoint Lie Group]. An adjoint Lie group is a semisimple real Lie group (11.6.7.1) with trivial center.

Prop. (11.6.7.3). Let \( G \) be a semisimple complex Lie group, then the center \( Z \) of \( G \) is contained in \( G^c \), thus the restriction of f.d. representations of \( G \) to \( G^c \) is an equivalence of categories.

Proof: Cf. [Etingof, P209] □

Maximal Tori

Prop. (11.6.7.4). Let \( G \) be a complex semisimple Lie group with Lie algebra \( \mathfrak{g} \), compact form \( \mathfrak{g}^c \) and compact part \( G^c \), then

8 Analysis

Lemma (11.6.8.1). Let \( H \) be a Lie subgroup of \( G \) and \( g \notin H \), then there is a smooth function \( \Phi \) on \( G \) that \( \Phi(xh) = \Phi(x) \) for any \( x \in G, h \in H \), and \( \Phi(H) = 0 \), yet \( \Phi(g) \neq 0 \).

Proof: Because \( H \) is closed, there is a nbhd \( U \) of \( g \) disjoint from \( H \) and a function \( \varphi \) supported in \( U \). Then \( \Phi(x) = \int_H \varphi(xh)dh \) satisfies the desired condition. □

Bi-Invariant Metric

Lemma (11.6.8.2). Bi-invariant metric exists in a compact Lie group.

Proof: Because the Haar measure on a compact metric is bi-invariant. Choose a Riemann metric and set

\[
\langle V, W \rangle = \int_{G \times G} \langle L_{\sigma*} R_{\tau*} (V), L_{\sigma*} R_{\tau*} (W) \rangle d\mu(\sigma) d\mu(\tau).
\]

Note that \( L_\ast \) and \( R_\ast \) commute. □

Prop. (11.6.8.3). For a left-invariant metric on a connected Lie group \( G \), if it is bi-invariant, then the inner product at the origin \( e \) is invariant under \( \mathfrak{g} \) (2.5.1.13), and the converse is also true if \( G \) is connected.
Proof: If the metric is invariant, then for any $X,Y,Z \in \mathfrak{g}$, $\langle \text{Ad}(\exp(tX))Y, \text{Ad}(\exp(tX))Z \rangle = \langle X,Y \rangle$, so we take derivation w.r.t. $t$ to get

$$\langle \text{ad}(X)Y, Z \rangle + \langle Y, \text{ad}(X)Z \rangle = 0$$

by (11.6.1.12).

Conversely, if this is invariant, then using $\exp(tX) = \exp((t - t_0)X) \exp(t_0X)$, we get $\partial(\langle \text{Ad}(\exp(tX))Y, \text{Ad}(\exp(tX))Z \rangle)/\partial t = 0$ for all $t$, thus $\langle \text{Ad}(\exp(tX))Y, \text{Ad}(\exp(tX))Z \rangle = \langle X,Y \rangle$, and it is invariant under right actions by $\exp(tX)$ also. As $G$ is generated by the elements $\exp(X)(3.8.1.3)$, it is right-invariant under $G$. \[\square\]

Prop.(11.6.8.4). If $G$ is a Lie group with a bi-invariant metric, then

$$\nabla_X Y = 1/2[X,Y], \quad R(X,Y)Z = 1/4[[X,Y],Z], \quad K(\sigma) = 1/4||[X,Y]||^2.$$ 

So it has non-positive sectional curvature, and its curvature is non-negative, and all 1-parameter subgroups are geodesics from $e$.

Proof: It suffices to show that $\langle Z, \nabla_X Y \rangle = 1/2\langle Z, [X,Y] \rangle$ for any $Z$, and this follows from (11.2.3.16). The second follows from the first and the definition (11.2.3.11). \[\square\]

Cor.(11.6.8.5). A bi-invariant Lie group with $\mathfrak{g}$ having trivial center is compact and $\pi_1(G)$ finite.

Proof: The Ricci curvature has a positive lower bound, otherwise for some $X, [X,Y] = 0$ for all $Y$, thus $X$ is in the center. Hence we use Myer theorem (11.2.5.20). \[\square\]

Cor.(11.6.8.6). If $G$ has a bi-invariant metric, then the exp map $\mathfrak{g} \to G$ is surjective.

Proof: Because exp is defined for any $X \in \mathfrak{g}$, and for any $g \in G$ and $v \in T_g(G)$, $\exp_p(v) = L_g(\exp(dL_{g^{-1}})g(v))$ because $L_g$ is an isomorphism of Riemann manifolds. So by Hopf-Rinow (11.2.3.46), $G$ is complete. Thus for any $q$, there is a geodesic connecting $e,q$, which is a 1-parameter subgroup, thus $q = \exp(X)$ for some $X \in \mathfrak{g}$. \[\square\]

Prop.(11.6.8.7) [Structure of bi-invariant Lie groups]. A simply-connected Lie group with a bi-invariant metric is equal to $G' \times \mathbb{R}^k$, $G'$ compact.

Proof: Because the orthogonal complement of the center of $\mathfrak{g}$ is a Lie algebra, $G$ is like $G' \times \mathbb{R}^k$, and a simply connected abelian Lie group is $\mathbb{R}^k$? \[\square\]
11.7 Complex Geometry

Basic References are [Voi02], [Principle of Algebraic Geometry Griffith/Harris], more advanced stuffs to add from [Kähler Geometry] and [Complex Geometry Daniel]. Even more advanced is [Demailly Complex Analytic and Differential Geometry].

1 Complex Manifolds

Def.(11.7.1.1) [Complex Manifold]. A complex manifold is an even dimensional manifold that the transformation matrices are holomorphic.

Prop.(11.7.1.2) [Andreotti-Francl]. Let \( M^n \subset C^n \) be a complex submanifold of dimension \( n \), then \( M \) is homotopic to a CW complex of real dimension \( \leq n \).

\[ \text{Proof: } \]

Prop.(11.7.1.3) [Adjunction Formula]. The normal sheaf of a submanifold \( Y \subset X \) is defined the same as the case of nonsingular varieties(5.10.1.17), then the same is true of the adjunction formula:

\[ K_Y \cong K_X \otimes \det N_{Y/X} \]

In case \( Y \) is of codimension 1, \( N_{Y/X} \cong \mathcal{L}(Y)|_Y = \mathcal{O}_Y(Y) \).

Prop.(11.7.1.4)[Remmert]. A non-compact manifold admits a proper holomorphic embedding into \( C^N \) for some \( N \) iff it is a Stein manifold.

\[ \text{Proof: } \]

Prop.(11.7.1.5)[Siegel]. Let \( X \) be a compact complex manifold of dimension \( n \), then the field \( K(X) \) of meromorphic functions on \( X \) has transcendence degree \( \leq n \) over \( C \). And in case \( \text{tr.deg} K(X) = \dim X \), it is a f.g. field extension of \( C \). Then we define the algebraic dimension of a compact connected complex manifold \( X \) to be \( \text{dim}^{\text{alg}}(X) = \text{tr.deg} R(X) \).

\[ \text{Proof: } \]

It suffices to show that given any meromorphic functions \( f_1, \ldots, f_{n+1} \), there is an algebraic relation between them.

Now for each \( x \), there is a nbhd \( U_x \) that any \( f_i \) writes as the quotient of two holomorphic functions \( \frac{g_i}{h_i} \). And assume \( W_x \subset V_x \subset \overline{V_x} \subset U_x \) are the metric balls \( B(x, \frac{1}{2}) \subset B(x, 1) \). As \( X \) is compact, there are \( N x_k \) that \( X = \bigcup W_{x_k} \).

As on the intersections, \( \frac{g_{i,k}}{h_{i,k}} = \frac{g_i}{h_i} \), any we can assume they are all prime, so \( \frac{g_{i,k}}{g_i} = \varphi_{i,kl} \) is a unit. Let \( \varphi_{kl} = \prod \varphi_{i,kl} \), as \( X \) is compact, let \( C = \max_{k,l} \varphi_{kl} \geq 1 \).

For any homogenous polynomial \( F \in C[X_1, \ldots, X_{n+1}] \) of deg \( m \), let \( G_k = F(\frac{g_{i,k}}{h_i}, \ldots, \frac{g_{n,k}}{h_{n,k}})(\prod h_{i,k})^m \). Then \( G_k \) are holomorphic and \( G_k = \varphi_{ik} G_l \) on the intersection. Now I claim for any \( M > 0 \), there is a \( F \) that \( G_k \) vanishes vanishes up to at least order \( M \) at \( x_k \).

For this, just consider the dimension of all homogenous polynomials of degree \( m \) is \( C_{m+n+1}^m \), and the number of desired equations of elements needs to be vanish is \( N \cdot C_{m-1+n}^{m-1} \), so this always can be achieved when \( m \) is sufficiently large.

By Schwartz lemma(10.5.9.4), \( |G_k(x)| \leq (\frac{1}{2})^{m'} C' \), where \( C' = \max\{|G_k(x)||k = 1, \ldots, n, x \in \overline{V_k}|\} \).

If \( C' = |G_k(x)| \), and \( x \in W_l \), then \( C' = |G_l(x)||\varphi_{ik}^{m'}(x)| \leq \frac{C'}{2^{m'}} C^m \). If for some \( m, m', C^m < 2^{m'} \), then this shows \( C' = 0 \) which will finish the proof.
Look back at the condition of \( m, m', \; C_{m+n+1}^m > N \cdot C_{m'-1+n}^{m'} \), can be achieved together with \( m < \lambda m' \) for any \( \lambda \), because the left hand is degree \( n + 1 \) in \( m \) and the right hand is degree \( n \) in \( m' \). □

**Almost Complex Structure**

**Def. (11.7.1.6) [Almost Complex Structures].** For \( M \) a real orientable manifold of dimension \( 2n \), an **almost complex structure** is a real bundle map \( J : T_C M \to T_C M \) satisfying \( J^2 = -1 \). A manifold with an almost complex structure is called an **almost complex manifold**.

A complex manifold has an almost complex structure, just define \( J(\partial/\partial x_i) = \partial/\partial y_i \) and \( J(\partial/\partial y_i) = -\partial/\partial x_i \).

**Def. (11.7.1.7).** \( J \) will define a bundle map on \( T^* M \to T^* M \), and it has two eigenvalues \( \pm i \), denoted by \( T^* M \). The **formal differential forms** \( \Lambda^k T^* M \cong \sum \Lambda^{p,k-p} T^* M \). \( \partial \) is defined to be \( \pi_{p+1,q} \circ d \) on \( \Lambda^p T^* M \), and \( \overline{\partial} \) is defined to be \( \pi_{p,q+1} \circ d \).

**Def. (11.7.1.8) [Integrability].** An almost complex structure is called **integrable** iff it satisfies the following equivalent conditions:

- \( da = \partial a + \overline{\partial} a \).
- \( da = \partial a + \overline{\partial} a \) is true for \( a \in \mathcal{A}^{1,0}(X) \).
- \( [T^{0,1} X, T^{0,1} X] \subset T^{0,1} X \).
- \( \overline{\partial}^2 f = 0 \) for functions \( f \).

**Proof:** \( 1 \iff 3 \) is because by (11.1.3.6), if \( u, v \in T^{0,1} X \),

\[
da(u, v) = u(\alpha(v)) - v(\alpha(u)) - \alpha([u, v]) = -\alpha([u, v]).\]

\( 3 \iff 4 \) is because by (11.1.3.6), if \( \alpha = \overline{\partial} f \) and \( u, v \in T^{0,1} X \), then

\[
\overline{\partial}^2 f(u, v) = u(\overline{\partial} f(v)) - v(\overline{\partial} f(u)) - \overline{\partial} f([u, v]) = u(df(v)) - v(df(u)) - \overline{\partial} f([u, v]) = \partial f([u, v])
\]

□

**Prop. (11.7.1.9) [Nirenberg-Newlander].** Given an almost complex manifold \((M, J)\), it is integrable iff it comes from a complex structure.

**Proof:** Cf. [Foundation of Differential Geometry Kobayashi Chap9.2]. □

2 **Deformation of Complex Structures**

Cf. [Kähler Geometry] and [Complex Geometry Chap6], should be completed as soon as possible.

3 **Analytic Spaces and Coherence Sheaves**

Cf. [Demailly] and [GAGA Serre].
11.7. COMPLEX GEOMETRY

**Analytic Subvarieties**

**Def.(11.7.3.1)** [Analytic subvariety]. An analytic subvariety is a closed subset of a complex manifold that is locally defined by f.m. holomorphic functions. The regular points of an analytic subvariety locally defined by $k$ functions is the points that rank $\left( \frac{\partial (f_1, \ldots, f_k)}{\partial (z_1, \ldots, z_n)} \right) = k$.

**Prop.(11.7.3.2)** [Proper Mapping Theorem]. If $U, M$ are complex manifolds and $M \subset U$ is an analytic subvariety, then if $f : U \to N$ is a holomorphic mapping whose restriction on $M$ is proper, then $f(M)$ is an analytic subvariety of $N$.

*Proof:* Cf.[Griffith/harris P395]. □

**Def.(11.7.3.3).** An analytic space of $\mathbb{C}^n$ is an analytic subvariety of $\mathbb{C}^n$. On an analytic space, there is a sheaf of holomorphic functions $\mathcal{H}_U$. So we can define holomorphic map $\varphi$ as continuous functions that map holomorphic germs to holomorphic germs, which is equivalent to the coordinates of $\varphi$ are all holomorphic.

**Def.(11.7.3.4)** [Analytic Spaces]. An analytic space is a Hausdorff space $X$ with a structure sheaf $\mathcal{H}_X$ that is locally isomorphic to an analytic set. Morphisms are continuous maps that are locally holomorphic. Sub-analytic spaces are defined as usual.

The products of analytic spaces can be defined, and it has the product topology, unlike the case of schemes.

**Prop.(11.7.3.5)** [Analytic Modules]. An analytic module is just a module over the sheaf $\mathcal{H}_X$. For a sub-analytic space $Y$, we have a sheaf of ideals $\mathcal{A}_Y$ which is the sheaf of germs vanishing at $Y$, and $\mathcal{H}_X/\mathcal{A}_Y$ is a sheaf of $X$ that is zero outside $Y$, and we identify it with $\mathcal{H}_Y$.

**Def.(11.7.3.6)** [Coherent Analytic Sheaves].

**Prop.(11.7.3.7)** [Coherence of Structure Sheaf]. The structure sheaf of an analytic space is coherent, and the sheaf of ideals of a sub analytic space is coherent.

*Proof:* First prove for $X$ is an open subset of $\mathbb{C}^n$, Cf.[GAGA Serre P4]. And by definition $\mathcal{A}_X$ is a $\mathcal{O}_X$-module of f.t., and it is also coherent?, so $\mathcal{H}_X$ is coherent. $\mathcal{A}_Y$ is coherent because it is a kernel of $\mathcal{H}_X \to \mathcal{H}_Y$. □

4 Positive Current

5 Hermitian Vector Bundles

**Def.(11.7.5.1).** A holomorphic vector bundle is a vector bundle on a complex manifold that the transition functions are holomorphic. A Hermitian vector bundle is a holomorphic vector bundle endowed with a Hermitian metric. Any holomorphic vector bundle has a Hermitian structure, by partition of unity method.

**Prop.(11.7.5.2)** [Hodge Star for Hermitian bundles]. If $E$ is a Hermitian vector bundle over a compact complex manifold of complex dimension $n$, we define a conjugate-linear operator $\tilde{\eta} : A^{p,q}(X) \to A^{n-p,n-q}(X) : \eta \mapsto *\eta$, and a conjugate-linear functor $\tau E \to E^*$ induced by the Hermitian metric on $E$.

Then we can define $\tilde{\eta}_E : A^{p,q}(E) \to A^{n-p,n-q}E : \eta \otimes s \mapsto \tilde{\eta}(\eta) \otimes \tau(s)$. It can be checked that $(\alpha, \beta) * 1 = \alpha \land *E \beta$,

$$\overline{\partial}_E = -\overline{\tilde{\eta}_E \partial \tilde{\eta}_E} \overline{\tilde{\eta}_E} \overline{\tilde{\eta}_E}, \quad \overline{\tilde{\eta}_E \Delta \overline{\partial}_E} = \Delta_{\overline{\partial}_E \overline{\tilde{\eta}_E}}, \quad \overline{\tilde{\eta}_E \Delta \overline{\partial}_E} = (-1)^{p+1} \text{ on } \Omega^{p,q}(E).$$
Hermitian Manifold

Def. (11.7.5.3) [Holomorphic Tangent Bundle]. Let $M$ be a complex manifold, the complexified tangent bundle $T_C M$ is defined as $T M \otimes \mathbb{R} \mathbb{C}$, the holomorphic tangent bundle $T^{1,0} M$ and anti-holomorphic bundle $T^{0,1} M$ are defined to be the vectors generated resp. by $\partial/\partial z_i$ and $\partial/\partial \bar{z}_i$. The holomorphic cotangent bundle and anti-holomorphic cotangent bundle is defined to be the covectors generated by $dz_i$ and $d\bar{z}_i$. 

Def. (11.7.5.4) [Hermitian Metric]. Let $M$ be an almost complex manifold, a Hermitian metric on $T_C M$ is a metric that is $J$-invariant, that is $g(Ju, Jv) = g(u, v)$. Notice (2.3.8.1) shows a Hermitian metric is equivalent to a non-degenerate Hermitian form on $T_C M$, where $g$ appears as the real part of the Hermitian form. 

Def. (11.7.5.5) [Hermitian Manifolds]. A complex manifold with a Hermitian metric is called a Hermitian manifold. 

Def. (11.7.5.6). Given a Hermitian manifold $M$, define the Kahler form $\omega_g$ as $\omega_g(u, v) = g(Ju, v)$. Then it is a real 2-form on $M$. Notice $g(u, v) = \omega_g(u, Jv)$, so $g$ can be constructed by $\omega_g$, iff $\omega_g$ is positive (11.8.7.1).

Analytic Picard Groups

Def. (11.7.5.7) [Analytic Picard Groups]. The group of isomorphisms of holomorphic line bundles on a complex manifold $X$ is denoted by $Pic_C(X)$, called the analytic Picard group of $X$. 

Prop. (11.7.5.8) [First Chern Class]. For a connected space $X$, there is an exact sequence $0 \to \mathbb{Z} \to \mathcal{O}_X \xrightarrow{f \mapsto e^{2\pi i f}} \mathcal{O}_X^* \to 0$, and it induces a map $Pic_C(X) = H^1(X, \mathcal{O}_X^*) \to H^2(X, \mathbb{Z})$, which is just the first Chern class (same proof as in (3.11.4.19)). 

WARNING: in this case it is not necessarily isomorphism, not as in the case of topological line bundles. 

in particular, The image of the first Chern class is trivial in $H^2(X, \mathcal{O}_X)$. 

Def. (11.7.5.9). The dual of the universal line bundle on $\mathbb{CP}^n$ is called the hyperplane line bundle, denoted by $H$ or $\mathcal{O}(1)$. 

Prop. (11.7.5.10). $Pic_C(\mathbb{CP}^n) \cong \mathbb{Z}$, with $\mathcal{O}(1)$ as a generator. 

Proof: As $\mathbb{CP}^n$ is Kähler, use (11.8.6.1), then $H^{0,k}(X, \mathcal{C}) \cong H^k(X, \mathcal{O}_X) = H^k(X, \mathcal{K}_X \otimes \mathcal{O}(2)) = 0$ for $k \geq 1$ by Kodaira vanishing (11.8.8.3), and then $\text{NS}(X) = H^{1,1}(X) = H^2(X, \mathbb{Z}) = \mathbb{Z}$ by Lefschetz (1,1)-form theorem (11.8.6.2). It remains to prove $c_1(\mathcal{O}(1))$ is the generator, for this, Cf. [Demailly P280]. 

Prop. (11.7.5.11). Let $S_d$ be the set of homogenous polynomials of degree $d$, then 

$$H^0(\mathbb{CP}^n, \mathcal{O}(d)) = \begin{cases} S_d & d \geq 0 \\ 0 & d < 0 \end{cases}$$

Proof: This is because it is sections that satisfy $f_\alpha([z]) = (\frac{z_n}{z_0})^k f_\beta([z])$, which says $f_\alpha$ glue together to give a holomorphic function homogenous of degree $k$ on $\mathbb{C}^n - \{0\}$, which extends to a function on $\mathbb{C}^n$ by (10.5.9.3), then it is easy to see it is a homogenous polynomial using the power series expansion. 

□
Def. (11.7.5.12) [Néron-Severi Group]. For a compact complex manifold $X$, the Néron-Severi group $\text{NS}(X)$ is the image of $\text{Pic}_C(X) \to H^2(X, \mathbb{Z})$. \text{rank}(\text{NS}(X))$ is called the Picard number of $X$.

There is a good description of $\text{NS}(X)$ in case $X$ is Kähler, see Lefschetz theorem (11.8.6.2).

This is compatible with the the algebraic Néron-Severi group (7.7.3.38). Cf. [G-H78] P457, [Vak17] P484.

**Chern Connection**

Prop. (11.7.5.13) [Chern Connection]. Given a Hermitian holomorphic bundle $E \to M$ on a complex manifold, there is a unique Chern connection $\nabla$ on $E$, that $\nabla$ is holomorphic (i.e. the connection matrix is holomorphic w.r.t a homomorphic frame), and it is compatible with the Hermitian metric.

*Proof:* Write out the requirement: if $H = h_{ij}$ is the matrix of the Hermitian metric, so $H$ is Hermitian, and we need $dh_{ij} = (\nabla e_i, e_j) + (e_i, \nabla e_j) = \sum_k \omega_{ik}h_{kj} + \sum \overline{\omega}_{jk}h_{ik}.\omega$ is holomorphic, so $\partial H = \theta H$, $\bar{\partial}H = \bar{H}\theta t$. □

Cor. (11.7.5.14). The curvature of the Chern connection is $\Omega = \partial(\partial(h^{-1})h)$. In particular, it is a skew-symmetric matrix of $(1, 1)$-forms. If it is of dimension 1, then $\Omega = \partial\bar{\partial}\log h$.

*Proof:* $\Omega$ is locally $d\omega + \omega \wedge \omega$, so if we choose a unitary basis, then $\omega$ is skew-symmetric by definition and $\omega \wedge \omega$ is also skew-symmetric, so $\Omega$ is skew-symmetric. The calculation is direct calculation. □

Prop. (11.7.5.15). The transformation matrix of a complex manifold is holomorphic, so it is possible to define globally $\bar{\partial}$ operator. And locally on a nbhd, $\bar{\partial}$ is defined as $d - \partial$.

Prop. (11.7.5.16) [Normal Coordinate]. For a Hermitian vector bundle $E$ over a complex manifold $X$, given any coordinate frame $(z_j)$, there exists a holomorphic frame $(e_\lambda)$ that

$$\langle e_\lambda, e_\mu \rangle = \delta_{\lambda,\mu} - \sum c_{jk\lambda\mu}z_j\bar{z}_k + O(|z|^3)$$

where $c_{ij\lambda\mu}$ is the coefficient of the Chern connection $\Omega$. Such a coordinate is called the normal coordinate frame of $E$ at $x$.

*Proof:* Cf. [Demailly P270]. □

Def. (11.7.5.17) [Dolbeault Cohomology]. The Dolbeault cohomology group $H^{p,q}_\bar{\partial}(X, \mathcal{E})$ of a holomorphic vector bundle $\mathcal{E}$ over a complex manifold $X$ is defined to be the $q$-th cohomology group of the complex

$$0 \to \Omega^{p,0} \overset{\bar{\partial}}{\to} \Omega^{p,1} \overset{\bar{\partial}}{\to} \ldots \overset{\bar{\partial}}{\to} \Omega^{p,n-p} \to 0$$

and $H^{p,q}_\bar{\partial}$ is defined to be $H^q_c(X, \mathcal{E})$. By (5.3.5.16), $H^{p,q}_\bar{\partial}(X, \mathcal{E}) \cong H^q(M, \Omega^p_{\text{hol}} \otimes \mathcal{O}_X \mathcal{E})$.

6 GAGA

Main references are [Ser55].
Analytification of Algebraic Varieties and Sheaves

Prop. (11.7.6.1) [Analytification]. For any variety over $\mathbb{C}$, any open affine subset is isomorphic to an analytic space of $\mathbb{C}^n$, hence can be given an analytic structure $X^\text{an} \to X$, called the analytification of $X$. It is a locally ringed space. This is because algebraic isomorphisms are analytic isomorphism. Moreover, for any morphism of algebraic variety over $\mathbb{C}$, the corresponding morphism is analytic, thus giving a functor from the category of algebraic varieties over $\mathbb{C}$ to the category of analytic spaces. An algebraic analytic space is an analytic space that is in the essential

$X^\text{an}$ is Hausdorff because analytification preserves products and morphisms, and separability of $X$ shows that $\Delta(X)$ is closed in $X \times X$, hence it is also closed in the analytification.

Notice $X^\text{an}$ and $X$ have in fact the same underlying sets.

Remark (11.7.6.2). There is in fact a more general analytification for any scheme locally of finite type over $\mathbb{C}$. That is, we define it as the right adjoint to the forgetful functor from analytic spaces to local ringed spaces. Where an analytic space is a local ringed space that locally has immersions into $\mathbb{C}^n$. Should consult [Grothendieck EGA1-7].

Proof: Notice the schemes that have an analytification is stable under open subscheme, closed subscheme and products, and we can make a glue a large space from open subschemes by the unicity. So we only need to consider Spec $\mathbb{C}[T]$, whose analytification is $\mathbb{C}$. □

Def. (11.7.6.3) [Betti Cohomology]. For any variety defined over $\mathbb{C}$, and $R$ a ring, let $H^i_{\text{Betti}}(X, R) = H^i(X^\text{an}, R)$ be the Betti cohomology of $X$ with coefficients in $R$.

Prop. (11.7.6.4) [Transfer of Properties].
- $X^\text{an}$ is locally compact and $\sigma$-compact.
- $X$ is smooth over $\mathbb{C}$ iff $X^\text{an}$ is a complex manifold.
- A morphism $f : X \to Y$ is proper iff $X^\text{an} \to Y^\text{an}$ is proper. In particular, $X$ is complete(proper) iff $X^\text{an}$ is compact.
- If $X$ is projective and connected, then $X^\text{an}$ is connected iff $X$ is connected.

Proof: The first is because $X$ is qc hence covered by f.m. affine subsets hence second-countable and use(3.6.2.23). $X^\text{an}/X$ is flat because completion of Noetherian rings are flat(4.2.3.14).

For proper, Cf.[GAGA Serre P8]. If $S$ is smooth, then by Jacobian criterion(4.4.5.24), the Jacobian of local defining function is not zero every where, so its analytification is clearly smooth.

The last assertion in fact follows from(11.7.6.16), as $H^0(X, O_X) = H^0(X^\text{an}, O_X)$. □

Prop. (11.7.6.5). There is a natural map from $O_x$ to $H_x$ that maps $m_x$ to $m_xH_x$, thus inducing a map $\theta : \hat{O}_x \to \hat{H}_x$. This is an isomorphism. In particular, $\theta : \Omega_x \to H_x$ is injective.

Moreover, if $Y$ is a locally closed subscheme of $X$, then the local ideal of functions vanishing at $Y$ maps to $A_x(Y)$, and $A_x(Y)$ is generated by $\theta(\mathcal{I}_x(Y))$. Moreover, $H_{x,Y} = H_x/\mathcal{I}_x(Y)$.

Proof: [GAGA Serre P6]. □

Cor. (11.7.6.6). The inclusion $O_x \subset H_x$ is flat ring extension, by(4.4.1.20) and the fact $\hat{A}/A$ is flat. And dim $O_x = \dim H_x$ because dim $A = \dim \hat{A}(4.2.4.16)$.

Cor. (11.7.6.7). Given an open and dense subscheme $U$ of an algebraic variety $X$ over $\mathbb{C}$, $U^\text{an}$ is dense in $X^\text{an}$. 
Proof: Consider the complement $Y$, if $U^\text{an}$ is not dense in $X^\text{an}$, then there exists a $x$ that $A_x(Y) = 0$, so by (11.7.6.5), $I_x(Y) = 0$, so $Y$ is not dense near $x$, contradiction. □

Cor. (11.7.6.8). For a morphism $f$ of algebraic varieties over $C$, $f(X)^\text{an} = f(X)^\text{an}$.

Proof: By Chevalley theorem (5.6.1.6), there is a open dense subscheme $U$ of $f(X)$ that is contained in $f(X)$, then (11.7.6.7) shows $U^\text{an}$ is dense in $(f(X))^{\text{ab}}$, so $f(X)^\text{an} \subset f(X)^\text{an}$. The converse is obvious. □

Def. (11.7.6.9) [Analytification of Sheaves]. Denote for a sheaf $F$ over $X$ $F'$ the inverse image sheaf over $X^\text{an}$ pulled back along $X^\text{an} \to X$. Define $F^\text{an}$ the analytic sheaf of $F$ as the sheaf $F' \otimes_{O_X} O_X$.

Prop. (11.7.6.10). $F \to F^\text{an}$ is exact from the category of sheaves on $X$ to the category of analytic sheaves on $X^\text{an}$, $F' \to F^\text{an}$ is injective, and it maps coherent sheaves to coherent analytic sheaves.

Proof: The first two follows from the fact that $H_X$ is flat over $X^\text{an} \to X$ (11.7.6.6). For the last assertion, notice if $O_X \to O_X^\text{an} \to F \to 0$, then $H_X^p \to H_X^p \to F^\text{an} \to 0$, so it is coherent because $H_X$ is coherent (11.7.3.7) (5.2.2.28).

Prop. (11.7.6.11). Let $i : Y \to X$ be a closed subscheme, then for a coherent sheaf $F$ on $Y$, $(i^\text{an})_*F^\text{an} \cong (i_*F)^\text{an}$.

Proof: These two sheaves are both 0 outside $Y^\text{an}$, consider a point of $Y$, their stalks are respectively $F_x \otimes_{O_{x,Y}} H_{x,Y}$ and $F_x \otimes_{O_{x,Y}} H_{x,Y}$. By (11.7.6.5) we notice

$$H_{x,y} = H_{x,x}/I_x(Y)H_{x,x} = H_{x,x} \otimes_{O_{x,x}} O_{x,y}.$$ 

So this two are equal by associativity of tensor product. □

Prop. (11.7.6.12). By Leray Spectral sequence (5.3.1.10), for an analytic sheaf $G$, there is a boundary map $H^k(X, G)H^k(X^\text{an}, G)$. So for a sheaf $F$ on $X$, there is a map

$$\varepsilon : H^k(X, F) \to H^k(X, \text{an}_*F^\text{an}) \to H^k(X^\text{an}, F^\text{an})$$

Equivalence between Algebraic Variety and Analytic Spaces

Remark (11.7.6.13) [GAGA Principle]. In principal, any complete analytic object in $\mathbb{CP}^n$ is algebraic.

Prop. (11.7.6.14). Let $X,Y$ be algebraic varieties over $C$ and $f : X \to Y$ is morphism that is bijective, if $f^\text{an}$ is an analytic isomorphism, then $f$ is an isomorphism.

Proof: Cf. [GAGA Serre P9]. □

Cor. (11.7.6.15). Let $X,Y$ be algebraic varieties over $C$, iff $f : X^\text{an} \to Y^\text{an}$ is holomorphic map and the image of $f$ in $X^\text{an} \times Y^\text{an} = (X \times Y)^\text{an}$ comes from an algebraic subscheme, then $f$ comes from an algebraic morphism. (Because $X^\text{an} \to \Gamma(X)$ is an analytic isomorphism).

Prop. (11.7.6.16) [GAGA on Coh(X)]. Let $X$ be a proper scheme over $C$, then $F \to F^\text{an}$ defines an equivalence of categories between $\text{Coh}(X)$ and $\text{Coh}^\text{an}(X^\text{an})$. 
Proof: Cf.[GAGA Serre P13], [SGA1,Chap12].

Prop. (11.7.6.17) [GAGA on Projective Varieties].

- (Chow) Any analytic subvariety of $\mathbb{CP}^n$ is algebraic.
- Any meromorphic function on an algebraic variety $V \subset \mathbb{CP}^n$ is rational.
- Any meromorphic differential form on a smooth variety is algebraic.
- Any holomorphic map between smooth varieties can be given by rational maps.
- Any holomorphic vector bundle on a smooth variety is algebraic, i.e. transition function can be made rational.

Cf.[Griffith/Harris P168,170].

Cor. (11.7.6.18). If the analytification of a variety $X$ is a compact complex manifold, i.e. $X$ is smooth (11.7.6.4), then $K(X) = K(X^{an})$, as they are both morphism to $\mathbb{P}^1$.

Applications

Prop. (11.7.6.19) [Generalized Riemann Existence Theorem]. Let $X$ be a normal scheme of finite type over $\mathbb{C}$. Given any finite morphism of analytic spaces(i.e. proper and has finite fibers) form a normal complex analytic space $f : X' \to X^{an}$, then there is a unique normal scheme $X'$ and a finite morphism $g : X' \to X$ that $g^{an} = f$.

Proof: Cf.[SGA1, Chap12], using resolution of singularities.

Cor. (11.7.6.20) [Algebraic Fundamental Group].

7 Algebraic Compact Complex Manifolds

Def. (11.7.7.1) [Moishezon Manifolds]. A compact complex manifold is called a Moishezon manifold iff $\text{tr.deg.} K(X) = \dim X$, by (11.7.1.5) this is the highest degree it can have. When $X$ is an analytification of an algebraic variety $X^{an}$, $K(X^{an}) = K(X)$ by (11.7.6.18), so Moishezon is a necessary condition for a compact complex manifold to be algebraic.

Prop. (11.7.7.2) [Chow-Kodaira]. Any Moishezon manifold of dimension 2 is algebraic and projective.

Proof: 

Prop. (11.7.7.3) [Moishezon]. Any Moishezon manifold becomes algebraic and projective after a finite number of monoidal transformations with non-singular centers.

Proof: 

Prop. (11.7.7.4) [Artin]. The category of smooth proper algebraic spaces over $\mathbb{C}$ is equivalent to the category of Moishezon manifolds.

In particular, there are non-algebraic Moishezon manifolds in dimension $\geq 3$. Examples are given in [Har77]P444.

Proof: 

Prop. (11.7.7.5) [Moishezon]. Every Moishezon manifold that is Kähler is projective algebraic.

Proof: Cf.[Moishezon On n-dimensional compact varieties with n algebraically independent meromorphic functions].
11.8 Kähler Geometry

Basic References are [Voisin], [Principle of Algebraic Geometry Griffith/Harris], more advanced stuffs to add from [Kähler Geometry] and [Huy05]. Even more advanced is [Demailly Complex Analytic and Differential Geometry].

Notations (11.8.0.1).
- Use notations as in Complex Geometry.

1 Kähler Metric

Def. (11.8.1.1) [Kähler Manifolds]. A metric $g$ on a manifold is called a Kähler metric if the metric form $\omega_g$ is closed. In which case, it is called the Kähler class of $g$ in $H^2_{dR}(M)$. A complex manifold with a Kähler metric is called a Kähler manifold.

If $g_{ij} = g(\frac{\partial}{\partial z_i}, \frac{\partial}{\partial \bar{z}_j})$, then $\omega_g = \sum_{ij} g_{ij} dz_i \wedge d\bar{z}_j$. Then the condition of $\omega_g$ being closed can in fact be written in derivatives of $g$.

Prop. (11.8.1.2). If $g$ is Hermitian, then $\omega_g$ is real, non-degenerate and $\frac{1}{m!} \omega^n$ is a volume form on $M$.

In particular, if $\omega$ is Kähler, then it is a symplectic form.

Proof: If $g = \sum \varphi_i \otimes \bar{\varphi}_i$, then $\omega = i \sum \varphi_i \wedge \bar{\varphi}_i$, so it is clear that $\omega = \omega$. $\omega$ is non-degenerate as $g$ is. The last assertion follows from (2.3.8.7).

Cor. (11.8.1.3). If $M$ is a compact Kähler manifold, then its even dimensional cohomology group doesn’t vanish (11.5.1.6).

Remark (11.8.1.4). Notice there are notions like almost Hermitian and almost Kähler, similar to the definition of Hermitian and Kähler, but they are just defined using an almost complex structure on $M$. And an almost Kähler structure is Kähler iff $\nabla J = 0$, Cf.[Foundation of Differential Geometry Kobayashi].

Example (11.8.1.5) [Kähler Manifolds].
- If $M = \mathbb{R}^{2n}$, $g = \sum dx_i \wedge dz_i + \sum dy_i \wedge d\bar{z}_i$, then $\omega_g = \frac{1}{2} \sum dz_i \wedge d\bar{z}_i$ is Kähler.
- The metric $\omega_g = \sum dz_i \wedge d\bar{z}_i$ on a complex tori $\mathbb{C}^n/\Lambda$ is Kähler.
- Any Riemann surface is Kähler, because $d\omega$ is a 3-form so vanish.
- if $M = B(0, 1) \subset \mathbb{C}^n$ and $\omega_g = i \partial \bar{\partial} \log \frac{1}{1-|z|^2}$, then it is Kähler.
- The product metric on the product space $M \times N$ of two Kähler manifold is Kähler.
- A submanifold of a Kähler manifold is Kähler, as the Kähler form is the pullback of the Kähler form of the large manifold.

Prop. (11.8.1.6) [Fubini-Study Metric]. The Fubini-Study metric form on $\mathbb{CP}^n$ is defined locally to be $i \partial \bar{\partial} |s|^2$, for any local lifting $s$ of the projection $\mathbb{C}^n \setminus \{0\} \to \mathbb{CP}^n$. This doesn’t depend on the lifting, as $\partial \bar{\partial} (\log f + \log \bar{f}) = 0$, so they glue together to be a global form on $\mathbb{CP}^n$. It can be checked, $\omega$ is translation invariant and on the coordinate $(1, w_1, \ldots, w_n) \to (w_1, \ldots, w_n)$, $\omega|_{(0, \ldots, 0)} = \sum dw_i \wedge dw_i$, so it is positive definite.

Cor. (11.8.1.7). Any projective manifold is Kähler.
Prop. (11.8.1.8). the Fubini-Study metric on $\mathbb{CP}^n$ has sectional curvature $1 \leq K \leq 4$.

Proof: Cf.[Do Carmo P188]. □

Prop. (11.8.1.9)[Kähler Normal Coordinate]. For a Hermitian metric $g$ on $M$, $g$ is Kähler iff for any point $p$ of $M$, there is a holomorphic coordinate centered at $p$, $\omega_g = \sum g_{ij} dz_i \wedge d\bar{z}_j$ satisfying $g_{ij}(p) = 0$ and $dg_{ij}(p) = 0$. This coordinate is called Kähler normal coordinate. (Notice this is different from Darboux theorem, because this coordinate should be holomorphic).

Proof: Cf.[Complex Geometry P210]. □

2 Geometry of Kähler Manifolds

Prop. (11.8.2.1). Let $(M,J,g)$ be a Kähler manifold, then the complexification of the Levi-Civita connection of $g$ restricts to the Chern connection on $T^{1,0}M$.

Proof: Cf.[Complex Geometry note 石亚龙 48] and [Complex geometry Daniel Chap4.A]. □

Prop. (11.8.2.2). For a Kähler manifold, $\nabla J = 0$.

Proof: The problem depends only on first derivative, so choosing a Kähler normal nbhd (11.8.1.9), we may choose $J$ to be constant, so obviously $\nabla J(p) = 0$, $P$ is arbitrary, so $\nabla J = 0$. □

Cor. (11.8.2.3). $\nabla (JX) = J \nabla X$, so $R(X,Y)JZ = JR(X,Y)Z$, thus

$$\langle R(JX,JY)Z,W \rangle = \langle R(Z,W)JX,JY \rangle = \langle R(Z,W)X,Y \rangle = \langle R(X,Y)Z,W \rangle,$$

so $R(JX,JY)Z = R(X,Y)Z$.

Prop. (11.8.2.4). The curvature tensor of the complexified Levi-Civita connection on a Kähler manifold can be calculated in terms of $\partial_i$, $\partial_j$, Cf.[Complex Geometry note 石亚龙 50].

3 Kähler Identities

Let $X$ be a compact complex Kähler manifold.

Def. (11.8.3.1). Introduce some operators:

- $d^c = i(\partial - \bar{\partial})$, then $dd^c = 2i\partial \bar{\partial}$.

- The Lefschetz operator $L(\eta) = \omega \wedge \eta$. $\Lambda$ is defined as the formal adjoint of $L$ as $A^{p,q}$ is an inner space. In fact, $\Lambda = \pm \ast L \ast$.

- $h = (k - n)$ on $A^k(X)$.

Prop. (11.8.3.2). $[L, \Lambda] = p + q - n$ on $(p,q)$-forms.

Proof: The problem doesn’t depend on the derivatives, so using the Kähler normal coordinate (11.8.1.9), it suffice to prove for $\mathbb{C}^n$, for this, Cf.[Griffith/Harris P120] or [Complex Geometry P34]. □

Prop. (11.8.3.3)[Kähler Identities].

$$[\Lambda, \partial] = i\partial^*, \quad [\Lambda, \partial] = -i\partial^*.$$
Proof: The second one follows from the first because $\omega$ is a real form. For the first, notice only first derivation are involved, so by using the Kähler normal coordinate, it suffice to prove for $\mathbb{C}^n$, and this is by [Complex Geometry 石亚龙 P61].

Cor. (11.8.3.4).

$[\Lambda, d^*] = d^*$, $[\Lambda, d] = -d^{*c}$.

Prop. (11.8.3.5). $\Delta_d$ commutes with both $L$ and $\Lambda$.

Proof: $L$ commutes with $d$ because $\omega$ is closed, so taking adjoints, $\Lambda$ commutes with $d^*$. Now by Kähler identities,

$$\Lambda \Delta_d = \Lambda (dd^* + d^*d) = -d^{*c} d^* + dd^* \Lambda = \Delta_d \Lambda.$$

So taking adjoints, $\Delta_d$ also commutes with $L$. □

 Prop. (11.8.3.6). In the Kähler case, $\Delta_\partial = \Delta_\bar{\partial} = \frac{1}{2} \Delta_d$.

Proof: $\Delta_d = \partial(\partial + \bar{\partial})(\partial + \bar{\partial}^*) + (\partial^* + \bar{\partial}^*)(\partial + \bar{\partial}) = \Delta_\partial + \Delta_\bar{\partial} + (\partial \bar{\partial}^* + \bar{\partial}^* \partial) + (\bar{\partial} \partial^* + \partial^* \bar{\partial})$

So it suffice to prove $\partial \bar{\partial}^* + \bar{\partial}^* \partial = 0$ (so $\partial \partial^* + \partial^* \partial = 0$ by conjugation), and $\Delta_\partial = \Delta_\bar{\partial}$. For the first, use Kähler identities, then

$$i(\partial \bar{\partial}^* + \bar{\partial}^* \partial) = \partial [\Lambda, \partial] + [\Lambda, \partial] \partial = 0$$

For the second, using Kähler identities,

$$i \Delta_\bar{\partial} = \bar{\partial} [\Lambda, \partial] + [\Lambda, \partial] \bar{\partial} = \bar{\partial} \Lambda \partial + \partial \bar{\partial} - \Lambda \bar{\partial} \partial - \partial \Lambda \bar{\partial}$$

and the same is miraculous true for $\Delta_\partial$, so the result is true. □

4 Hodge Theory

Prop. (11.8.4.1)[Hodge Decomposition of compact Kähler Manifolds]. For a compact Kähler manifold $X$,

$$H^*_d(X, \mathbb{C}) = \bigoplus_{p+q=r} H^{p,q}_d(X) \simeq \bigoplus_{p+q=r} H^q(X, \Omega^p)$$

and $H^*_d(X) \simeq H^*_{\bar{\partial}}(X)$. Moreover, this decomposition doesn’t depends on the Kähler metric.

Proof: (11.8.3.6) shows that $\Delta_d$ maps $A^{p,q}$ to $A^{p,q}$, so $H^{p,q}_d \cap A^{p,q} = H^{p,q}_d(X)$. The last assertion is seen using the $\Delta_d$ definition.

If chosen two different Kähler metric $g, g'$, there $H^{p,q}(X, g) \cong H^{p,q}(X) \cong H^{p,q}(X, g')$. If $\alpha, \alpha'$ be $g, g'$ $\bar{\partial}$-harmonic respectively, so by definition $\alpha - \alpha' = \bar{\partial} \gamma$ for some $\gamma$, and they are both $d$-harmonic, so $d \bar{\partial} \gamma = 0$, and $\bar{\partial} \gamma$ is $g$-orthogonal to $H^k(X, g)$ by Hodge decomposition for $\bar{\partial}$ with metric $g$, so by Hodge theorem for $d$ with metric $g$, $\partial \gamma$ is $d$-exact, so $[\alpha] = [\alpha']$.

Cor. (11.8.4.2). Betti number $b_r = \sum_{p+q=r} h^{p,q}$, $h^{p,q} = h^{q,p}$. In particular, $b_{2k+1}$ is always even.
Cor. (11.8.4.3) [Holomorphic Form on Kähler Manifold is Closed]. \( \mathcal{H}^{p,0}(X) = H^0(X,\Omega^p) \).

Now a \((p,0)\)-form is automatically \(\bar{\partial}\)-closed, so it is \(\bar{\partial}\)-harmonic iff it is holomorphic. So we conclude any holomorphic \(p\)-form on a Kähler manifold is \(d\)-closed, even \(d\)-harmonic.

Lemma (11.8.4.4) \([\partial\bar{\partial}\text{-lemma}]\). A closed differential form \(\eta\) on a compact Kähler manifold \(M\) is \(d\)-exact iff it is \(\partial\)-exact iff it is \(\partial\)-exact iff it is \(\partial\bar{\partial}\)-exact.

Proof: Now \(\Delta_d, \Delta_{\bar{\partial}}, \Delta_{\partial}\) are all the same, By Hodge theorem, it suffice to prove, if a form is orthogonal to \(H^{p,q}(X)\), then it is \(\partial\bar{\partial}\)-exact (this implies other exactness).

Now \(\eta\) is \(d\)-closed hence \(\partial\) and \(\bar{\partial}\)-closed, then \(\eta = \partial \gamma\) for some \(\gamma\), and then \(\gamma = \bar{\partial} \beta + \bar{\partial}\beta' + \beta''\) for \(\beta''\) harmonic. So \(\bar{\partial} \eta = \bar{\partial} \bar{\partial} \beta = 0\), but then inner product with \(\partial \beta\) shows \(\partial \bar{\partial} \beta = 0\), so \(\eta = \partial \bar{\partial} \beta\).

Cor. (11.8.4.5) [Kodaira-Serre Duality]. By \((11.1.10.15)\), For a Hermitian line bundle over a compact Hermitian complex manifold \(X\), from Hodge theorem and \((11.7.5.2)\), we get

\[
H^p(X,\Omega^q(E)) \cong H^{n-p}(X,\Omega^{n-q}(E^*))
\]

induced by \(\bar{\pi}_E\) and \(\pi_{E^*}\). Moreover, there is a perfect pairing

\[
H^p(X,\Omega^q(E)) \times H^{n-p}(X,\Omega^{n-q}(E^*)) \to \mathbb{C}
\]

induced by

\[
H^{p,q}(X,E) \times H^{n-p,n-q}(X,E^*) \to \mathbb{C} : \alpha, \beta \mapsto \int_X \alpha \wedge \bar{\pi}_E \beta
\]

In fact, \(\int_X \alpha \wedge \bar{\pi}_E \alpha = ||\alpha||^2 \neq 0\).

Prop. (11.8.4.6). Holomorphic 1-forms on a compact complex surface is closed.

Prop. (11.8.4.7) [Hard Lefschetz Theorem]. For a compact Kähler manifold \(M\), the map

\[
L^k : H^{n-k}(M) \to H^{n+k}(M)
\]

is an isomorphism, (notice it is defined because \(L\) commutes with \(d\)).

Define the \textbf{primitive cohomology class} \(P^{n-k}(M) = \ker L^{k+1}\) on \(H^{n-k}\), then

\[
H^m(M) = \oplus_k L^k P^{m-2k}(M).
\]

Proof: Cf.[Griffith/Harris P122], using representation theory of \(\mathfrak{sl}_2\).

Prop. (11.8.4.8) [Hodge-Riemann Bilinear Relation]. Let \((X,\omega)\) be a Kähler manifold, if \(\alpha \neq 0 \in H^{p,q}(X)\) is a primitive cohomology class, then

\[
i^{p-q}(-1)^{(p+q)(p+q-1)} \int_X \alpha \wedge \bar{\alpha} \wedge \omega^{n-p-q} > 0
\]

Proof: Cf.[Griffith/Harris] or [Complex Geometry Daniel P138].

Cor. (11.8.4.9). For a compact Kähler manifold of complex dimension \(2m\),

\[
\text{sgn}(X) = \sum_{p,q=0}^m (-1)^p h^{p,q}(m)
\]
11.8. KÄHLER GEOMETRY 1121

Proof: Cf.[Complex Geometry Daniel P140]. □

Prop.(11.8.4.10) [Hirzebruch-Riemann-Roch]. By (11.1.10.8), for a n-dimensional complex line bundle $L$ over a compact Kähler manifold $M$,
\[ \chi(M, L) = \int_M [\text{ch}(E) \text{td}(T^{1,0}M)]_n. \]
Where $\chi(M, L) = \sum_{q=0}^n (-1)^q \dim H^q(M, E)$, ch is the Chern character (11.1.9.5) and $\text{td}(T^{1,0}M)$ is the Todd polynomial, i.e. Taylor expansion of $\prod_{i=1}^n \frac{t_i}{1 - e^{-t_i}}$ in terms of the symmetric polynomial, applied to $c_i(T^{1,0}M)$.

Cor.(11.8.4.11) [Riemann-Roch]. By (11.1.10.9), for a complex vector bundle $E$ over a Riemann surface $M$, let $\deg E = \int_M c_1(E)$, then
\[ \chi(M, E) = H^0(M, E) - \dim H^1(M, E) = \deg E + \text{rk}(E)(1 - g). \]

Cor.(11.8.4.12). For other examples of corollaries of Hirzebruch-Riemann-Roch theorem, Cf.[Complex Geometry P232].

Formality of Complex Kähler Geometry

Cf.[Complex Geometry Daniel Chap3.A].

5 Complex Tori

Def.(11.8.5.1) [Complex Tori]. A complex torus is a pointed complex manifold isomorphic to the complex manifold $V/\Lambda$, where $V$ is a f.d. vector space over $\mathbb{C}$ and $\Lambda$ is a complete lattice in $V$.

Prop.(11.8.5.2). Let $X = V/\Lambda, X' = V'/\Lambda'$ be complex tori, then any $\mathbb{C}$-linear map $\alpha: V \to V'$ s.t. $\alpha(\Lambda) \subset \Lambda'$ defines a holomorphic map $X \to X'$ sending 0 to 0. And any holomorphic map $X \to X'$ sending 0 to 0 is of this form.

Proof: Any $\varphi: X \to X'$ lifts to a continuous map $\psi: V \to V'$, and it is holomorphic because the morphisms $V \to X, V' \to X'$ are locally biholomorphic, $\psi$ is also holomorphic. For any $\omega \in \Lambda$, $\psi(z + \omega) - \psi(z)$ has value in $\Lambda'$ for any $z$, so $\psi(z + \omega) = \psi(z) + a(\omega)$. From here it is easy to see that $\psi$ is linear. □

Def.(11.8.5.3) [Riemann Pairs]. A Riemann pair is a pair $(\Lambda, J)$ where $\Lambda$ is a finite $\mathbb{Z}$-module of finite rank, and $J$ is a complex structure on $\Lambda \otimes \mathbb{R}$. A homomorphism of Riemann pairs is a group homomorphism $\Lambda \to \Lambda'$ that preserves the complex structure.

Prop.(11.8.5.4) [Riemann Pairs and Abelian Varieties]. There is an equivalence of the category of Riemann pairs with $\text{AbVar}/\mathbb{C}$ by
\[ (\Lambda, J) \mapsto (\Lambda \otimes \mathbb{R})/\Lambda. \]

Proof: It is fully faithful by (11.8.5.2), and it is clearly essentially surjective. □
Prop. (11.8.5.5) [Cohomology of Complex Tori]. For any complex torus $X = V/\Lambda$, $H_1(X, \mathbb{Z}) \cong \Lambda$, so $H^1(X, \mathbb{Z}) \cong \text{Hom}(\Lambda, \mathbb{Z})$, and by K"unneth formula,

$$H^n(X, \mathbb{Z}) \cong \wedge^n H^1(X, \mathbb{Z}) \cong \wedge^n \text{Hom}(\Lambda, \mathbb{Z}).$$

Then

$$H^n(X, \mathbb{C}) \cong \wedge^n \text{Hom}_\mathbb{R}(V, \mathbb{C}) \cong \wedge^n (\text{Hom}_\mathbb{C}(V, \mathbb{C}) \oplus \text{Hom}_\mathbb{C}(\overline{V}, \mathbb{C})) = \bigoplus_{p+q=n} \wedge^p V^* \otimes \wedge^q \overline{V}^*$$

and

$$H_1(X, \mathbb{C}) \cong \Lambda \otimes_\mathbb{Z} \mathbb{C} \cong V \otimes_\mathbb{R} \mathbb{C} \cong V \otimes V^* = \text{Tgt}_0(X) \oplus \overline{\text{Tgt}_0(X)}.$$

Cor. (11.8.5.6) [Complex Tori are K"ahler]. A complex torus (11.8.5.1) $X = V/\Gamma$ is a K"ahler manifold. And $H^2(X, \mathbb{R}) \cong \wedge^2 \text{Hom}_\mathbb{R}(V, \mathbb{R})$, by (11.8.5.5).

Prop. (11.8.5.7) [Hodge Theory of Complex Tori]. Let $X = V/\Lambda$ be a complex torus, as $X$ is K"ahler (11.8.5.6), there is a decomposition

$$H^n_{\text{dR}}(X, \mathbb{C}) \cong \bigoplus_{p+q=n} H^q(X, \Omega^p)$$

by (11.8.4.1). Then this decomposition corresponds to the decomposition in (11.8.5.5) via the isomorphism $H^n_{\text{dR}}(X, \mathbb{C}) \cong H^n(X, \mathbb{C})$. In particular, there is a canonical isomorphism

$$H^q(X, \Omega^p) \cong \wedge^p V^* \otimes \wedge^q \overline{V}^*.$$

Proof: \hfill \Box

Def. (11.8.5.8) [Dual Complex Tori]. Let $X = V/\Lambda$ be a complex torus with a Riemann form, then we can define the dual complex torus as

$$X^\vee = V^*/\Lambda^*$$

where $V^* = \text{Hom}_\mathbb{C}(V, \mathbb{C})$ and $\Lambda^* = \{ f \in V^* | f(\Lambda) \subset \mathbb{Z} \}$.

Riemann Forms

Prop. (11.8.5.9) [Riemann Forms]. For a complex torus $V/\Lambda$, it is projective iff there is a Riemann form on $V$, which is an alternating bilinear form $\omega : V \times V \to \mathbb{R}$ that:

- $\omega(iu, iv) = \omega(u, v)$.
- $\omega(v, iv) > 0$ for $v \neq 0$.
- $\omega(u, v) \in \mathbb{Z}$ for $u, v \in \Gamma$.

Notice $\omega$ is clearly non-degenerate.

Proof: Use (11.8.5.6). The conditions are just equivalent to $\omega$ being an integral positive K"ahler form (11.8.9.6). \hfill \Box

Prop. (11.8.5.10) [Dual Riemann Forms]. If $X = V/\Lambda$ is a complex torus with a Riemann form, then the dual complex torus (11.8.5.8) $X^\vee$ also has a Riemann form defined as follows: any $f \in V^*$ corresponds to an element $v_f$ s.t. $f(u) = \omega(u, v_f)$. Thus we can define $\omega'(f, g) = \omega(v_f, v_g)$. And there is an isogeny (i.e. surjective isomorphism with finite kernel)

$$A \to A^\vee : \pi \mapsto [x \mapsto \omega(x, \pi)]$$

which is compatible with the Riemann forms.
6 Jacobian and Albanese

Lemma (11.8.6.1). If \( X \) is compact Kähler, then the natural map \( H^k(X, \mathbb{C}) \to H^k(X, \mathcal{O}_X) \) is just the projection onto the \((0, k)\)-part. In particular, the image is in \( H^{0,k}(X) \).

Proof: By Hodge decomposition, the definition of Dolbeault cohomology and the commutative diagram

\[
\begin{array}{ccc}
\mathbb{C} & \longrightarrow & \mathcal{A}^0(X) \\
\downarrow & & \downarrow d \\
\mathcal{O}_X & \longrightarrow & \mathcal{A}^1(X)
\end{array}
\]

Proof: Because by the long exact sequence of (11.7.5.8) and (11.8.6.1) again, an \( \alpha \in H^2(X, \mathbb{C}) \) is in \( H^1(X, \mathbb{Z}) \) if and only if \( \alpha \) is in the image of \( \text{Pic}_c(X) \to H^{1,1}(X, \mathbb{Z}) \).

Cor. (11.8.6.3). The image of \( H^1(X, \mathbb{Z}) \to H^1(X, \mathcal{O}_X) \) is a lattice. In particular, it is isomorphic to \( \mathbb{Z}^{b_1(X)} \).

Proof: \( H^1(X, \mathbb{Z}) \) is a lattice in \( H^1(X, \mathbb{R}) \), and \( H^1(X, \mathbb{R}) \to H^1(X, \mathcal{O}_X) = H^{0,1}(X, \mathbb{C}) \) is an isomorphism, because \( H^{0,1}(X, \mathbb{C}) \) are conjugate to \( H^{1,0}(X, \mathbb{C}) \) and \( H^1(X, \mathbb{R}) \) is real.

Def. (11.8.6.4) [Jacobian]. The Jacobian \( \text{Jac}(X) \) of a compact Kähler manifold \( X \) is defined to be \( H^1(X, \mathcal{O}_X)/H^1(X, \mathbb{Z}) \), so it is a complex torus of dimension \( b_1(X) \) by (11.8.6.3), it is also the kernel of the first Chern class map by the long exact sequence (11.7.5.8), i.e.

\[
0 \to \text{Jac}(X) \to \text{Pic}(X) \xrightarrow{\gamma} NS(X) \to 0
\]

Def. (11.8.6.5) [Albanese]. The Albanese variety \( \text{Alb}(X) \) of a compact Kähler manifold \( X \) is defined to be the complex torus \( H^0(X, \Omega_X^1)^*/H_1(X, \mathbb{Z}) \), where

\[
H^1(X, \mathbb{Z}) \to H^0(X, \Omega_X^1) : [\gamma] \mapsto \left( u \mapsto \int_{\gamma} u \right)
\]

(Notice this is well-defined because by (11.8.4.3) any \( u \in H^0(X, \Omega_X^1) \) is closed).

Fix a base point \( x_0 \) of \( X \), the Albanese map \( \text{Alb} : X \to \text{Alb}(X) \) is defined to be

\[
x \mapsto \left( u \mapsto \int_{x_0}^{x} u \right)
\]

It is holomorphic and functorial in \((X, x_0)\). It is just the so called Abel-Jacobi map in case when \( X \) is a Riemann surface.
7 Positivity

**Def. (11.8.7.1) [Positive Line Bundle]**. A 2-form $\omega$ on a Hermitian complex manifold $M$ is called **positive** iff $\omega(u, J u) \geq 0$ for $u \neq 0 \in TM$, which is equivalent to $-i \omega(v, \overline{v}) > 0$ for all $v \in T^{1,0} X$.

A holomorphic vector bundle is called **(Griffith-)positive** iff there exists a Hermitian metric on it that the curvature form $\Omega$ for the Chern connection ($11.7.5.13$) satisfies $h(\Omega(s), s)(v, \overline{v}) > 0$ for all $s \in E$ and $v \in T^{1,0} X$.

The pullback of a positive line bundle along an immersion is positive.

**Prop. (11.8.7.2) [Positivity on Kähler Manifolds]**. On a compact Kähler manifold, being positive is a topological property for line bundles. It is equivalent to the first Chern class of $L$ can be represented by a positive form in $H^2_{dR}(M)$.

**Proof**: $c_1(L) = \frac{1}{2\pi} \Omega$, so one direction is trivial, and if $c_1(L) = \frac{i}{2\pi} \theta$, choose an arbitrary Hermitian metric $h$ on $L$, then by $\partial \overline{\partial}$-lemma ($11.8.4.4$), $\theta = \Omega + \partial \overline{\partial} \rho$ for some smooth function $\rho$. Then $e^{\rho} h$ has $\Omega = \theta$ by formula ($11.7.5.14$).

**Cor. (11.8.7.3)**. On a compact Kähler manifold, if $L$ is positive, then for any other Hermitian line bundle $L'$, $kL + L'$ is positive.

**Prop. (11.8.7.4)**. The hyperplane line bundle $\mathcal{O}(1)$ ($11.7.5.9$) is positive.

**Proof**: The hyperplane line bundle is dual to the tautological line bundle. The metric on the tautological line bundle is given by locally $g_i = \frac{1}{|z_i|^2} \sum |z_i|^2$. It is compatible with the transition map, and then by ($11.7.5.14$), the Chern curvature is

$$\overline{\partial} \partial (\frac{1}{|z_i|^2} \sum |z_i|^2) = \overline{\partial} \partial (\sum |z_i|^2).$$

So by ($11.2.3.6$) the curvature of the hyperplane line bundle times $i$ is just the Fubini-Study metric form ($11.8.1.6$), so it is positive.

**Prop. (11.8.7.5)**. For $\widetilde{X} \to X$ the blowing-up of $X$ at a point $x$, If $L$ is a positive line bundle on $X$, then for any integer $n$, there exists a $k > 0$ that $\pi^* L^k - nE$ is a positive line bundle on $\widetilde{X}$, where $E$ is the exceptional divisor.

**Proof**: Involves explicit metric calculation, Cf.[Kodaira Embedding Theorem P11] and [Complex Geometry P249].

8 Kodaira Vanishing Theorem

**Prop. (11.8.8.1) [Nakano Identities]**. For a holomorphic vector bundle over a compact Kähler manifold $(M, \omega)$ with Hermitian metric $h$, introduce operators $D$ and $\Lambda$ as before. If we denote the $(1, 0)$ and $(0, 1)$-part of the Chern connection on $E$ by $D^\prime$ and $D'^\prime = \overline{\partial}$, then

$$[\Lambda, \overline{\partial}] = -i D'^\prime, \quad [\Lambda, D'] = i D^\prime.$$

**Proof**: The question is local, choose normal coordinate frame at $x$ ($11.7.5.16$), then by the formula of Chern connection ($11.7.5.14$), $\nabla_E = d + A$, $A(x) = 0$, and $\nabla_{E^*} = d + B$, $B(x) = 0$. so

$$[\Lambda, \overline{\partial}_E] + i D'^\prime = [\Lambda, \overline{\partial}] + i \partial^\prime + [\Lambda, A^{0,1}] + i B^{0,1}$$

where the usual Kähler identities ($11.8.3.3$) are used. Then it is zero when evaluated at $x$, Cf.[Demailly Complex Analytic and Differential Geometry P329].
Cor. (11.8.8.2) [Bochner-Kodaira-Nakano Identity].
\[ \Delta_{\partial,E} - \Delta_{D',E} = i[\Omega, \Lambda] \]

Proof:
\[ -i\Delta_{D',E} = D'[\Lambda, \partial] + [\Lambda, \partial]D' = D'\Lambda\partial - D'\partial\Lambda + \Lambda \partial D' - \partial \Lambda D' \]
and similar calculation for \( i\Delta_{\partial,E} \), so
\[ i\Delta_{\partial,E} - i\Delta_{D',E} = \Lambda(\partial D' + D'\partial) - (\partial D' + D'\partial)\Lambda = -[\Omega, \Lambda]. \]

Prop. (11.8.8.3) [Kodaira-Akizuki-Nakano Vanishing Theorem]. If \( L \) is a positive line bundle on a compact Kähler manifold \( M \), then
\[ H^p(M, \Omega^q(L)) = 0 \]
for \( p + q > n \). In particular, \( H^p(M, K_M \otimes L) = 0 \) for \( p > 0 \).

Proof: By Hodge theorem (11.1.10.13), it suffice to prove there are no harmonic \((p, q)\)-forms \( \in H^{p,q}(X, L) \).

As \( i\Omega = \omega \) is positive, we may endow \( M \) with the metric \( \omega \), then by (11.8.8.2) and (11.8.3.2),
\[ \Delta_{\partial} - \Delta_{D'} = [\Lambda, \partial] = p + q - n \] on \( A^{p,q} \).

So if \( s \in H^{p,q}(X, L) \), then \( (\Delta_{\partial}s - \Delta_{D'}s, s) = (p + q - n)||s||^2 \geq 0 \), but \( (\Delta_{\partial}s - \Delta_{D'}s, s) = -||D's||^2 - ||D'^s||^2 \leq 0 \), so \( s = 0 \).

Cor. (11.8.8.4) [Serre's Theorem]. Let \( L \) be a positive line bundle on a compact complex Kähler manifold \( X \), then for any holomorphic vector bundle \( E \), for \( m \) large, \( H^q(X, L^m \otimes E) = 0 \).

Proof: Same notation as in the proof of (11.8.8.3), choose Hermitian structure on \( E \) and \( L \) and their Chern connections by \( \nabla_E, \nabla_L \), the corresponding Chern connection on \( E \otimes L^m \) is denoted by \( \nabla \), and make sure \( \frac{i}{2\pi} F_{\nabla_E} \) is the Kähler form \( \omega \), then for any harmonic form \( \alpha \in H^{p,q}(X, E \otimes L^m) \), by (11.8.8.2), \( \frac{i}{2\pi} ([\Lambda, F_{\nabla_E}], \alpha) \geq 0 \), but \( \frac{i}{2\pi} F_{\nabla} = \frac{i}{2\pi} F_{\nabla_E} + m\omega \), so
\[ 0 \leq \frac{i}{2\pi} ([\Lambda, F_{\nabla_E}], \alpha) + m(n - p - q)||\alpha||^2 \]
Notice \( ||[\Lambda, F_{\nabla_E}], \alpha|| \) has a bound by Schwartz inequality, then if \( p + q > n \) and \( m \) sufficiently large, \( \alpha \) must by 0. In this case \( H^{p,q}(X, E \otimes L^m) = 0 \), but \( H^{0,q}(X, K_X \otimes E \otimes L^m) \subset H^{p,q}(X, E \otimes L^m) \), so it is 0. Now we’ve proved \( H^q(X, K_X \otimes E \otimes L^m) = 0 \) for any \( E \) if \( m \) is large. But \( E \) is arbitrary, so the conclusion is true. 

Cor. (11.8.8.5) [Grothendieck’s Lemma]. Every holomorphic line bundle \( E \) over \( \mathbb{CP}^1 \) is uniquely isomorphic to a finite direct sum of \( \mathcal{O}(a_i) \).

Proof: If \( E \) has rank 1, this is the content of (11.7.5.10), so use induction on rank of \( E \). Choose a maximal \( a \) that \( \text{Hom}(\mathcal{O}(a), E) = H^0(\mathbb{CP}^1, E(-a)) \neq 0 \). This \( a \) exists because Serre’s Theorem (11.8.8.4) shows that \( H^1(\mathbb{CP}^1, E(-a)) = 0 \) for \( a \) sufficiently small, and Riemann-Roch (11.1.10.9) shows that \( \chi(\mathbb{CP}^1, E(-a)) = \deg E + \text{rk}(E)(1 - a) \) is positive for \( a \) sufficiently small, so \( H^0(\mathbb{CP}^1, E(-a)) \neq 0 \). Conversely, if \( a \) is sufficiently large, then \( H^0(\mathbb{CP}^1, E(-a)) \cong H^1(\mathbb{CP}^1, E^*(a - 2)) = 0 \) (Notice \( K_{\mathbb{CP}^n} = \mathcal{O}(-n - 1) \)).
So now there is an exact sequence of sheaves

\[ 0 \to \mathcal{O}(a) \xrightarrow{\cdot s} E \to E_1 \to 0 \]

I claim \( E_1 \) is also a vector bundle, because \( s \) never vanishes, otherwise if it vanish at some \( x \), then we can divide by a linear factor \( s_x \in H^0(\mathbb{CP}^1, \mathcal{O}(1)) \) to get a map \( \mathcal{O}(a + 1) \to E \), contradicting the maximality. So by induction \( E_1 = \oplus \mathcal{O}(a_i) \), then I claim \( a_i \leq a \), because otherwise \( H^0(\mathbb{CP}^1, E_1(-a-1)) \neq 0 \), and by the exact sequence \( 0 \to \mathcal{O}(-1) \to E(-a-1) \to E_1(-a-1) \to 0 \), \( H^0(\mathbb{CP}^1, E(-a-1)) \neq 0 \), contradiction.

Then we want to show the above sequence splits, this is equivalent to

\[ 0 \to E_1^*(a) \to E^*(a) \to \mathcal{O} \to 0 \]

splits, and his follows from the fact \( H^1(\mathbb{CP}^1, E_1^*(a)) = H^1(\mathbb{CP}^1, \oplus \mathcal{O}(a-a_i)) = 0 \), by Serre duality. So there is a section lifting \( \mathcal{O} \to E^*(a) \), which splits the sequence. \( \square \)

Prop.(11.8.8.6) [Weak Lefschetz Theorem]. Let \( X \) be a compact Kähler manifold and \( Y \) be a submanifold that the line bundle \( L(Y) \) is positive, then the canonical restriction map \( H^k(X, \mathbb{C}) \to H^k(Y, \mathbb{C}) \) is isomorphism for \( k \leq n-2 \) and injective for \( k = n-1 \).

Proof: In fact, using Hodge decomposition, it suffices to prove on the level of \( H^q(X, \Omega^p_X) \). Tensoring the exact sequence

\[ 0 \to \Omega_X(-Y) \to \Omega_X \to \iota_* i_Y^* \Omega_X \to 0 \]

with \( \Omega^p_X \) and taking the cohomology. By Serre duality and Kodaira vanishing(11.8.8.3), the map \( H^q(X, \Omega^p_X) \to H^q(X, \Omega^p i_* i_Y^* \Omega_X) \) is isomorphism for \( p + q < n-1 \) and injection for \( p + q = n-1 \).

Next consider the exact sequence \( 0 \to TY \to TX \to \mathcal{N}_{Y/X} \to 0 \). By(5.5.1.26) there is an exact sequence

\[ 0 \to \wedge^p TY \to \wedge^p TX |_Y \to \wedge^{q-1} TY \mathcal{N}_{Y/X} \to 0 \]

Taking dual and applying adjunction formula(11.7.1.3), it becomes:

\[ 0 \to \Omega^q_Y \to \Omega^{q-1} \Omega(-N) \to \Omega^q_X |_Y \to \Omega^q_Y \to 0 \]

Taking cohomology and use Serre duality and Kodaira vanishing as before, the result follows, and the composition is also true. \( \square \)

Remark(11.8.8.7). There is a topological proof of weak Lefschetz theorem in [Bott, On a Theorem of Lefschetz].

9 Kodaira Embedding

Prop.(11.8.9.1) [Kodaira map]. For a holomorphic line bundle \( L \) on a compact complex manifold \( M \), if \( s_0, \ldots, s_n \) be a basis of \( H^0(X, L) \), we try to define a map from \( M \) to \( \mathbb{CP}^n : x \to [s_0(x), \ldots, s_n(x)] \). This is independent of the change of coordinates because \( g_{\alpha\beta} \) is invertible, and it is definable iff \( L \) is basepoint-free. This map is holomorphic where it is definable.

Def.(11.8.9.2) [Ample Holomorphic Line Bundles]. For a holomorphic line bundle \( L \) on a compact complex manifold \( X \), \( L \) is called

- semi-ample holomorphic line bundle iff for \( m \) large, \( L^m \) is basepoint-free.
• **very ample holomorphic line bundle** iff \( L \) is basepoint-free and the Kodaira map \( \iota_L : X \to \mathbb{CP}^N \) is a holomorphic embedding.

• **ample holomorphism line bundle** iff for \( m \) large, \( L^m \) is very ample.

**Lemma (11.8.9.3) [Cohomological Method for Very Ampleness]**. For the above Kodaira map to be a holomorphic embedding, it suffice to show that the map is definable, injective and surjective on cotangent space. For these, it is equivalent to \( H^0(X, L) \to L_x \) surjective, \( H^0(X, L) \to L_x \oplus L_y \) surjective, and \( L \otimes I_x \to L_x \otimes T^{1,0*}(X)_x \) surjective. And they are true if

\[
H^1(X, L \otimes I_x) = 0, \quad H^1(X, L \otimes I_{x,y}) = 0, \quad H^1(X, L \otimes I_x^2) = 0.
\]

respectively.

**Proof**: Basepoint-free at \( x \) is easily seen to be equivalent to \( H^0(X, L) \to L_x \) surjective. And there is an exact sequence of sheaves:

\[
0 \to L \otimes I_x \to L \to L_x \to 0
\]

where \( L_x \) means the skyscraper sheaf. So \( H^1(X, L \otimes I_x^2) = 0 \) induces the result.

Injective is easily seen to be equivalent to \( H^0(X, L) \to L_x \oplus L_y \) surjective. And there is an exact sequence of sheaves:

\[
0 \to L \otimes I_{x,y} \to L \to L_x \oplus L_y \to 0
\]

where \( I_{x,y} \) is the sheaf of functions vanishing at \( x \) and \( y \), and \( L_x \oplus L_y \) means the skyscraper sheaf. So \( H^1(X, L \otimes I_{x,y}) = 0 \) induces the result.

For the surjection on cotangent spaces, given any point \( x \), choose a basis \( s_1, \ldots, s_n \) of sections in \( H^0(X, L) \) vanishing at \( x \), and by basepoint-free, there is a \( s_0 \) not vanishing at \( x \), then on a coordinate, the Kodaira map is given by \( x \to (s_1/s_0, \ldots, s_n/s_0) \), then it need to be checked \( d_x(s_i/s_0) = d_x(x_i)/s_0 \) span \( T^{1,0*}(X)_x \). But there are exact sequences of sheaves:

\[
0 \to L \otimes I_x^2 \to L \otimes I_x \xrightarrow{d_x} L_x \otimes T^{1,0*}_x \to 0
\]

where \( d_x \) is given by \( d_x(s \otimes f) = s(x) \otimes d_x(f) \) (by the universal property of skyscraper sheaf), it suffice to give a map \( (L \otimes I_x \to L_x \otimes T^{1,0*}_x) \), notice this is independent of the coordinate because \( d_x(s) = d_x(g_{\alpha\beta}s_{\beta}) = g_{\alpha\beta}d_x(s_{\beta}) \), as \( s_{\alpha} \) vanishes at \( x \), so this is truly a sheaf map, and its kernel is \( L \otimes I_x^2 \). So \( H^1(X, L \otimes I_x^2) = 0 \) induces the result. \( \square \)

**Prop. (11.8.9.4)**. A holomorphic line bundle \( L \) on a compact Kähler manifold is ample iff it is positive.

**Proof**: If \( L \) is ample, then \( L^m \) is the pullback of the hyperplane bundle by the Kodaira map. The hyperplane line bundle is positive by (11.8.7.4), so \( L^m \) is positive with the induced metric, so \( L \) is also positive given the \( m \)-th roots of the induced metric (notice the metric of line bundle is just locally a number compatible with transition map).

Conversely, using (11.8.9.3), we want to find a \( L^k \) that \( H^1(X, L^k \otimes I_x) = 0, H^1(X, L^k \otimes I_{x,y}) = 0, H^1(X, L^k \otimes I_x^2) = 0 \). First notice it suffice to prove for single points when \( k \) is sufficiently large, because the holomorphic embedding is an open property and \( X \) is compact so a sufficiently large \( k \) will suffice.
Consider the blowing-up $\tilde{X}$ at a point $x$, there is a commutative diagram

\[
\begin{array}{ccc}
H^0(X, L^k) & \longrightarrow & L^k_x \\
\downarrow \pi^* & & \downarrow \cong \\
H^0(\tilde{X}, \pi^* L^k \otimes L^k_x) & \longrightarrow & H^0(E, \mathcal{O}_E) \otimes L^k_x
\end{array}
\]

The right vertical map is isomorphism as $E \cong \mathbb{C}P^n$, so $H^0(E, \mathcal{O}_E) = \mathbb{C}$. The left exact sequence is also isomorphism: it is injective because $\pi$ is surjective, and it is surjective because: if $\dim X = 1$, then $\pi = \text{id}$ so trivially true, and if $\dim X \geq 2$, then because $\pi : \tilde{X} - E \cong X - \{x\}$, any holomorphic function on $\tilde{X}$ induces a holomorphic function on $X - \{x\}$ and by Hartog’s theorem (10.5.9.3), it comes from a holomorphic function on $X$.

Now the second horizontal line is part of the cohomology exact sequence of (5.5.3.15)

\[
0 \rightarrow \pi^* L^k \otimes \mathcal{O}_{\tilde{X}}(-E) \rightarrow \pi^* L^k \rightarrow \pi^* L^k|_E \rightarrow 0
\]

So it is reduced to prove $H^1(\tilde{X}, \pi^* L^k \otimes \mathcal{O}(-E)) = 0$, but by (5.8.2.8), $\pi^* L^k - E = \pi^* L^k - E + \mathcal{K}_{\tilde{X}} - \pi^* \mathcal{K}_X - (n - 1)E = \mathcal{K}_{\tilde{X}} + (\pi^* L^k - E) + \pi^* (L^k - \mathcal{K}_X)$, and by (11.8.7.5)(11.8.7.3) the last two are positive when $k$ is large, so the conclusion follows from Kodaira vanishing (11.8.8.3).

The proof of $H^1(X, L^k \otimes \mathcal{I}_{x,y}) = 0$ is verbatim, just use blowing-up at two different points.

To prove $H^1(X, L^k \otimes \mathcal{I}^n_x) = 0$, consider the blowing-up $\tilde{X}$ at a point $x$, notice there is a commutative diagram

\[
\begin{array}{ccc}
H^0(X, L^k \otimes \mathcal{I}_x) & \xrightarrow{d_x} & L^k_x \otimes T^{1,0}X_x \\
\downarrow \pi^* & & \downarrow \cong \\
H^0(\tilde{X}, \pi^* L^k - E) & \longrightarrow & L^k_x \otimes H^0(E, -E)
\end{array}
\]

In fact this comes from the two commuting exact sequences twisted with $\pi^* L^k$:

\[
\begin{array}{ccc}
0 & \longrightarrow & \pi^* \mathcal{I}^2_x \\
\downarrow & & \downarrow \\
0 & \longrightarrow & \mathcal{O}(-2E) \longrightarrow \mathcal{O}(-E) \longrightarrow \mathcal{O}_E(-E) \longrightarrow 0
\end{array}
\]

The second line is (5.5.3.15) and the fact a section vanishing at $x$ lifts to a section vanishing at $E$ thus equivalent to a section in the twisted sheaf $- \otimes \mathcal{O}(-E)$. These two exact sequences commutes because

Back to the commutative diagram, the above argument also shows that the first vertical map is isomorphism. To show the second vertical map is isomorphism, notice by (5.8.2.7) $\mathcal{O}(-E)$ is just the hyperplane line bundle on $E$, so $H^0(E, -E) = T^{1,0}X_x$, we need to know the vertical map is the natural map $V^* \rightarrow H^0(\mathbb{P}(V), \mathcal{O}(1))$. This in fact need some careful calculation using coordinates in (5.8.2.7)?

Now the map $d_x$ is surjective iff the second horizontal map is surjective, with is part of the cohomology exact sequence of

\[
0 \rightarrow \pi^* L^k \otimes \mathcal{O}_{\tilde{X}}(-2E) \rightarrow \pi^* L^k \mathcal{O}_{\tilde{X}}(-E) \rightarrow \pi^* L^k|_E \rightarrow 0
\]

So it is reduced to prove $H^1(\tilde{X}, \pi^* L^k \otimes \mathcal{O}(-wE)) = 0$, which is by Kodaira vanishing theorem the same reason as before. \qed
Cor. (11.8.9.5) [Kodaira Embedding Theorem]. If a compact complex manifold $M$ has a positive line bundle, then it is projective.

Def. (11.8.9.6) [Hodge Manifold]. A compact Kähler manifold $X$ is projective iff it has a closed positive $(1,1)$-form $\omega$ whose cohomology class $[\omega]$ is rational/integral (i.e. in $H^2(X, \mathbb{Q})$). In fact, a compact Kähler manifold with a Hodge metric is called a Hodge manifold. So compact Hodge manifolds are just those compact Kähler manifolds that are projective.

Proof: if $\omega$ is rational, then a multiple of it is integral, then there is a $L$ that $c_1(L) = k[\omega]$ by Lefschetz theorem on $(1,1)$-forms (11.8.6.2), so $L$ is positive by (11.8.7.2), so $X$ is projective. Conversely, the Chern class of the pullback of the hyperplane line bundle is positive rational (11.8.7.4) (11.8.6.2). □

Cor. (11.8.9.7) [Compact Riemann Surfaces are Hodge Manifolds]. A Riemann surface is a complex variety of dimension 1. Any compact Riemann surface is a compact Hodge manifold.

Proof: This is because $H^2(X, \mathbb{C}) = H^2(X, \mathbb{Q}) \otimes \mathbb{Q} \cong \mathbb{C}$ is generated by the metric form $\omega$, so there must be a multiple of $\omega$ that is integral. □

Cor. (11.8.9.8). if $\tilde{X}$ is the blowing-up of a Kähler manifold $X$ at a point $x$, then if $X$ is projective, then $\tilde{X}$ is also projective, because by (11.8.7.5) $\pi^*L^k \setminus E$ is positive for $k$ large.

Cor. (11.8.9.9). For a finite unbranched cover of compact Kähler manifolds $\tilde{X} \to X$, $\tilde{X}$ is projective iff $X$ is projective.

Proof: A positive rational closed $(1,1)$-form on $X$ pull backs to a positive rational closed $(1,1)$-form on $\tilde{X}$, and it can even be pulled forward: $\omega' = \sum_{y \in \pi^{-1}(x)} (\pi^{-1})^* \omega(y)$, then it is also positive closed. It is rational because $\int_X \omega' \wedge \eta = \frac{1}{d} \int_{\tilde{X}'} \omega \wedge \pi^* \eta$, where $\tilde{X} \to X$ is branched of degree $d$. □

Def. (11.8.9.10) [Kähler Cone]. For a Kähler manifold $X$, the Kähler cone $K_X$ is defined to be the set of closed real positive $(1,1)$-forms. Then $K_X$ is an open convex cone in $H^{1,1}(X) \cap H^2(X, \mathbb{R})$. Then (11.8.9.6) says $X$ is projective iff $K_X \cap H^2(X, \mathbb{Z}) \neq 0$.

10 Fujiki Manifolds
11.9 Locally Symmetric Spaces

1 Symmetric Spaces

Main references are [Hel78], [Mil17b] and [Lan20].

Def. (11.9.1.1) [Symmetric Spaces]. A Riemannian manifold is called \textbf{locally symmetric} at \( p \) if \( \nabla R(p) = 0 \). Locally symmetric is equivalent to the fact that every local reversing map is an isometry.

A \textbf{symmetric space} is a Riemannian manifold that \( \nabla R = 0 \) everywhere.

A symmetric space is complete because two folding is an extension of geodesics. In particular, a symmetric space is homogenous, and to check symmetrically, it suffices to show it is homogenous and locally symmetric at a point.

\textit{Proof:}

Prop. (11.9.1.2). A Lie group with a bi-invariant metric is a symmetric space.

\textit{Proof:}

Prop. (11.9.1.3). The conjugate points in a symmetric space is easy to calculate, they are \( \exp(\frac{\pi k}{\sqrt{e_i}} V) \), counting multiplicity, where \( e_i \) is the eigenvalue of the self-adjoint operator \( K_V(W) = R(V,W)V \) at \( p \).

Prop. (11.9.1.4) [Group of Isometries]. Let \( M \) be a symmetric space, then the group of isometries \( \text{Isom}(M^\infty, g) \) of \( M \) has a natural structure of a Lie group.

\textit{Proof:} \text{Cf.[Helgason, homogenous Spaces, 4.3.2].}

\textit{Proof:}

Prop. (11.9.1.5) [Symmetric Space is a Homogenous Space]. Let \( (M, g) \) be a symmetric space, and \( p \in M \), then the subgroup \( K_p \subset \text{Isom}(M^\infty, g) \) fixing \( p \) is compact, and the natural map

\[ \text{Isom}(M, g)^0/K_p \to M^\infty \]

is an isomorphism of smooth manifolds, where \( \text{Isom}(M, g)^0/K_p \) is given the homogenous space structure\( (11.9.1.4) \). In particular, \( \text{Isom}(M, g)^0 \) acts transitively on \( M \).

\textit{Proof:} \text{Cf.[Mil17c]P12.}

2 Decompositions of Symmetric Spaces

3 Non-Compact Type

4 Compact Type

5 Hermitian Symmetric Spaces

Def. (11.9.5.1) [Hermitian Symmetric Spaces]. A \textbf{Hermitian symmetric space} is a Hermitian manifold that is a symmetric space\( (11.9.1.1) \) and that the local symmetries are all holomorphic.

Prop. (11.9.5.2) [Group of Isometries]. For a Hermitian symmetric space, the group of holomorphic symmetries \( \text{Isom}(M, g) \) is closed in the group of isometries \( \text{Isom}(M^\infty, g) \), which is a Lie group by\( (11.9.1.4) \), so it is also a Lie group.
Prop. (11.9.5.3) [Basic Hermitian Symmetric Spaces]. There are three different families of Hermitian symmetric spaces (but not complete):

- (Non-compact Type): These spaces are non-compact and simply connected, with negative curvatures, and $\text{Isom}(M, g)^0$ is adjoint and non-compact.
- (Compact Type): These spaces are compact and simply connected, with positive curvatures, and $\text{Isom}(M, g)^0$ is adjoint and compact.
- (Euclidean Type): These spaces have constant curvature $0$.


Prop. (11.9.5.4) [Decomposition]. Any Hermitian symmetric space $M$ decomposes into a product $M^0 \times M^+ \times M^-$ of Hermitian symmetric spaces with $M^0$ Euclidean, $M^-$ of non-compact type and $M^+$ of compact type.

Proof:

Prop. (11.9.5.5). Any Hermitian symmetric space of Euclidean type is a quotient of $\mathbb{C}^g$ by a discrete subgroup of translations.

Proof:

Example (11.9.5.6). The upper half plane $\mathcal{H}$ is a Hermitian symmetric space with the metric $\frac{dxdy}{y^2}$, because $GL(2, \mathbb{R})$ acts transitively on $\mathcal{H}$ and preserves the metric, and the diffeomorphism $z \mapsto -1/z$ is a geodesic isomorphism at $i$.

Proof: See (11.9.6.6).

Example (11.9.5.7). The projective space $\mathbb{P}^n(\mathbb{C})$ with the Fubini-Study metric is a Hermitian symmetric space. For any $p$, the (descent of) the rotation through $\pi$ about the axis through $p$ and its polar opposite is the geodesic isomorphism at $p$.

Proof: See (11.8.1.6).

6 Hermitian Symmetric Domains

Def. (11.9.6.1) [Hermitian Symmetric Domain]. A Hermitian symmetric space of non-compact type is called a Hermitian symmetric domain. A bounded symmetric domain is an open connected symmetric subset of $\mathbb{C}^n$.

Prop. (11.9.6.2). Every Hermitian symmetric domain can be embedded into $\mathbb{C}^n$ for some $n$.

Proof:

Prop. (11.9.6.3) [Bergman Metric]. Every bounded symmetric domain has a canonical Hermitian metric called the Bergman metric, it is invariant under holomorphic automorphisms, and it has negative curvatures.

Proof: Cf. [Mil17] P11 and [Hel78] 8.3.3.

Cor. (11.9.6.4). Every Hermitian symmetric domain $D$ has a unique Hermitian metric that maps to the Bergman metric under any isomorphism of $D$ onto a bounded symmetric domain.
**Def. (11.9.6.5) [Siegal Upper Half Plane \( \mathcal{H}_g \)].** The **Siegal upper half plane** \( \mathcal{H}_g \) consists of symmetric complex \( g \times g \) matrices \( Z = X + iY \) with \( Y \) positive definite. It is identified with an open subset of \( \mathbb{C}^{g(g+1)/2} \). The symplectic group \( \text{Sp}_{2g}(\mathbb{R})(11.6.1) \) acts transitively on \( \mathcal{H}_g \) via

\[
\begin{bmatrix} A & B \\ C & D \end{bmatrix} Z = (AZ + B)(CZ + D)^{-1}
\]

The matrix \( \begin{bmatrix} 0 & -I \\ I & 0 \end{bmatrix} \) acts as an involution on \( \mathcal{H}_g \), and has \( iI_g \) has its fixed point, so \( \mathcal{H}_g \) is homogenous and symmetric.

The injection into \( \mathbb{C}^g \) is not holomorphic, so we cannot see from this that \( \mathcal{H}_g \) is holomorphic, but we can see from ?

**Proof:** ?

**Cor. (11.9.6.6) [\( H_1 \)].** The group \( \text{GL}(2, \mathbb{R}) \) acts on \( \mathbb{C}^g \) by \( \gamma(z) = az + b \) where \( \gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \). It can be checked that this is a continuous group action.

Also in the same way the group \( \text{GL}(2, \mathbb{R}) \) or \( \text{SL}(2, \mathbb{R}) \) acts on the upper plane, by(10.5.1.8). This action is transitive and the stabilizer of \( i \) is \( \text{SO}(2, \mathbb{R}) \), thus we have \( \mathcal{H} \cong \text{SL}(2, \mathbb{R})/\text{SO}(2, \mathbb{R}) \), and \( \text{SL}(2, \mathbb{R}) \) is the group of holomorphic automorphisms of \( \mathcal{H} \).

Also, the Riemannian metric \( \frac{dx dy}{y^2} \) on \( \mathcal{H} \) is fixed by this action.

**Proof:**

**Def. (11.9.6.7) [Siegal Unit Circle \( D_g \)].** Let \( D_g \) be the set of symmetric complex matrixes that \( I - Z^*Z \) is positive definite, then it is identified with an open subset of \( \mathbb{C}^{g(g+1)/2} \), this is a holomorphic embedding.

There is an isomorphism from \( \mathcal{H}_g(11.9.6.5) \) to \( D_g \):

\[
Z \mapsto (Z - iI_g)(Z + iI_g)^{-1}.
\]

This is an isomorphic, so \( D_g \) is symmetric, and \( \mathcal{H}_g \) has an invariant metric, so they are both Hermitian symmetric domains ?.

**Proof:** ?

**Prop. (11.9.6.8).** Let \( (M, g) \) be a Hermitian symmetric domain, then the inclusions

\[
\text{Isom}(M^\infty, g) \supset \text{Isom}(M, g) \subset \text{Hol}(M)
\]

induce equalities

\[
\text{Isom}(M^\infty, g)^0 = \text{Isom}(M, g)^0 = \text{Hol}(M)^0
\]

Then \( \text{Hol}(M)^0 \) acts transitively on \( M \), the stabilizer \( K_p \) of \( p \) in \( \text{Hol}(M)^0 \) is compact, and

\[
\text{Hol}(M)^0/K_p \cong M^\infty.
\]

**Proof:** Cf.[Mil17b]P12.
**Prop. (11.9.6.9) [Rotation at a Point]**. Let $D$ be a Hermitian symmetric domain and $p \in D$, then there is a unique homomorphism $u_p : U_1 \to \text{Hol}(D)$ that $u_p(z)$ fixes $p$ and acts on $T_p(D)$ as multiplication by $z$.

**Prop. (11.9.6.10) [Classification of Hermitian Symmetric Domains]**. The isomorphism classes of irreducible Hermitian symmetric domains are classified by the special nodes on connected Dynkin diagrams.


## 7 Quotients of Hermitian Symmetric Domains

**Prop. (11.9.7.1) [D(Γ)]**. Let $D$ be a Hermitian symmetric domain, and let $Γ$ be a discrete subgroup of $\text{Hol}(D)^0$. If $Γ$ is torsion-free, then $Γ$ acts freely on $D$, and there is a unique complex manifold structure on $Γ\setminus D$ that the quotient map $π : D \to Γ\setminus D$ is a local isomorphism.

In this case, denote $D(Γ) = Γ\setminus D$, and $D$ is a universal covering of $D(Γ)$, by (11.9.5.3) and (11.9.6.1).

**Proof**: Cf. [Mil17b]P32.

**Prop. (11.9.7.2)**. Let $D$ be a Hermitian symmetric domain and $Γ \subset \text{Hol}(D)^0$ is a discrete subgroup, then by (11.9.6.8), $Γ$ has finite covolume in $\text{Hol}(D)^0$ iff $Γ\setminus D$ has finite covolume.

**Proof**: 

**Prop. (11.9.7.3)**. $D(Γ)$ has only f.m. automorphisms, as a complex manifold.

**Proof**: Cf. [Mil17b]P41.

**Thm. (11.9.7.4) [Baily-Borel Compactifications]**. Let $D$ be a locally symmetric Hermitian space and $Γ \subset \text{Hol}(D)^0$ an arithmetic subgroup, then $D(Γ)$ can be realized as an open subset of a projective variety $\overline{D(Γ)}$ over $C$, and it is a normal algebraic variety. If moreover $Γ$ is torsion-free, then it is smooth, by (11.9.7.1).

Such a projective variety $\overline{D(Γ)}$ is called a **locally symmetric variety**.


Cf. [Mil17b]P38 for a history.

**Thm. (11.9.7.5) [Borel]**. Let $D(Γ)$ be a quotient of a Hermitian symmetric domain by a torsion-free arithmetic subgroup in $\text{Hol}(D)^0$, then for any other smooth quasi-projective variety $V$ over $C$, any holomorphism map $V^\text{an} \to D(Γ)^\text{an}$ comes from a morphism.

**Proof**: 

**Cor. (11.9.7.6) [Algebraic Structure is Unique]**. The algebraic variety structure on $D(Γ)$ is unique.

**Proof**: If there is another structure, then by GAGA it is a smooth variety, then the holomorphic map extends to a bijective morphism, which must be an isomorphism, by [Milne, Algebraic Geometry, P188].
Cor. (11.9.7.7). The Baily-Borel compactification is minimal in the sense that it factors through any compatification $D(\Gamma) \subset D(\Gamma)^\dagger$ s.t. $D(\Gamma)^\dagger \setminus D(\Gamma)$ is a divisor with normal crossing.

Proof: ? □
11.10 Compactifications of Locally Symmetric Spaces


[Smooth compactifications of locally symmetric varieties] contains a lot of references.

Def. (11.10.0.1) [Toroidal Compactifications]. Cf. [BOREL, A. AND JI, L. 2006. Compactifications of symmetric and locally symmetric spaces].

For Siegel modular varieties, there is a short note in [Conrad, Mordell conjecture seminar].
11.11 Calabi-Yau Manifolds
12 Algebraic Number Theory

12.1 $p$-adic Analysis

This section should only contain theorems that are only applicable to non-Archimedean valuations. Theorems that are applicable to both Archimedean and non-Archimedean valuations should be put into 10.6.

As far as I know, all properties proved in Functional Analysis independent of complex analysis is applicable to the non-Archimedean case, and in fact, the goal of this section is to build an analytic theory parallel to complex analysis.

References are [Non-Archimedean Analysis Part A].

1 (Ultranormed) Valuation Theory

Ultranormed Rings

Def.(12.1.1.1) [Normed Groups]. A semi-normed group is a group with a non-Archimedean valuation, it is called a normed group iff the valuation has kernel 0, which is equivalent to Hausdorff.

A normed group is totally connected, because open balls at 0 are subgroups hence closed.

Def.(12.1.1.2) [Normed Ring]. A (semi-)normed ring is a (semi-)normed additive group that
- $|1| = 1$, or the valuation is trivial.
- $|ab| \leq |a||b|$.

A valued ring is a normed ring with $|ab| = |a||b|$. It is called degenerate if all non-zero valuation value $\geq 1$.

Prop.(12.1.1.3). A valuation on a ring is non-Archimedean iff $\{|n|\}$ is bounded. Thus any valuation on a field with finite characteristic is non-Archimedean.

Prop.(12.1.1.4). In a normed ring, every triangle is an acute isosceles triangle. (This is because the biggest is smaller than the maximal of the other two, thus the biggest two are equal). Hence we have, for a circle $B(O,r)$, any interior point $P$ is a center of circle, because $OP < r$.

Def.(12.1.1.5). A normed ring $R$ is call a $B$-ring if elements of valuation 1 is invertible, it is called bald if there is a $\varepsilon$ that no elements has valuation in $(1 - \varepsilon, 1)$.

Def.(12.1.1.6) [Uniform Rings]. A non-Archimedean ring $A$ is called uniform if the set of topologically nilpotent elements are bounded in $A$.

Prop.(12.1.1.7). If $K$ is a normed field with valuation ring $R$, the smallest subring containing a zero sequence $a_0, a_1, \ldots$ is bald.
Proof: Cf. [Formal and Rigid Geometry P25]. □

Def. (12.1.1.8). An element \( a \) in a normed ring \( A \) is called topologically nilpotent iff \( \lim a^n = 0 \). The set of all topological nilpotent elements in \( A \) are denoted by \( \tilde{A} \) or \( A^0 \).

Prop. (12.1.1.9). \( \tilde{A} \) is a subgroup of \( A^+ \), which is multiplicatively closed. And \( \tilde{A} \) is Clopen in \( A \). In particular, \( \tilde{A} \) is complete if \( A \) is complete.

Proof: Cf. [Non-Archimedean analysis P27]. □

Prop. (12.1.1.10) [Nakayama’s Lemma]. If \( A \) is complete normed ring and \( M \) is a \( A \)-module, if there are f.m. elements \( x_i \) of \( M \) that \( M = N + \sum x_iM \), then \( M = N \).

Proof: The proof is verbatim as the proof of the usual Nakayama lemma. □

Normed Modules

Def. (12.1.1.11) [Ultranormed Module]. A module \( M \) over a normed ring \( A \) is called normed module iff it is a normed additive group and \( |ax| \leq |a||x| \) for \( a \in A, x \in M \). If \( A \) is valued and the equality always holds, we call it faithfully normed or valued module.

If \( A \) is a valued field, any normed module is valued.

Prop. (12.1.1.12) [Ultranormed Algebra]. A normed algebra is an \( A \) algebra \( B \) with \( A \to B \) bounded of norm 1.

Prop. (12.1.1.13). For two valued module over \( A \), if \( A \) is non-degenerate, a morphisms is bounded iff it is continuous. This is because we can multiply by elements of \( A \) to reduce to a nbhd of 0.

This applies to the case when \( A \) contains a field where the valuation is non-trivial, because we can use (12.1.1.11).

Def. (12.1.1.14) [Completed Tensor Product]. For two normed modules over a normed ring \( R \), there is a complete normed \( R \)-module \( M \hat{\otimes} N \) called the completed tensor product, satisfying the following universal properties: \( M \times N \to M \hat{\otimes} N \) is bounded by 1, and for any complete normed \( R \)-module \( T \) and a \( R \)-map \( M \times N \to T \) bounded by \( a \), then it factor through a \( R \)-map \( M \hat{\otimes} N \to T \) bounded by \( a \).

It satisfies many universal properties as you can imagine.

Proof: Cf. [Formal and Rigid Geometry P238]. □

Cor. (12.1.1.15). By (12.1.1.13), when \( A \) is non-degenerate, then the amalgamated sum is just the fibered pushout when restricted to the category of complete valued module over \( A \) with continuous maps as morphisms, because it satisfies the universal property.

Prop. (12.1.1.16) [Amalgamated Sum]. For two normed \( R \)-algebras there is an operation of amalgamated sum which satisfies universal properties similar to (12.1.1.14). In fact, it is just the completed tensor product when seen as modules.

Proof: Cf. [Formal and Rigid Geometry P242]. □
Weakly Cartesian Space

Def. (12.1.1.17). A normed $K$-vector space over a valued field $K$ is called **weakly Cartesian** iff

Prop. (12.1.1.18). If $K$ is a complete valued field, then each normed $K$-vector space $V$ is weakly Cartesian.

Proof: Cf. [Non-Archimedean Analysis P92]. □

Extensions of Norms and Valuations

Def. (12.1.1.19). If $L/K$ is a finite extension of valued field of degree $n$, then $v$ extends uniquely to $w(\alpha) = \frac{1}{n}v(N_{L/K}(\alpha))$, now we define the **ramification degree** as $(w(L^*) : v(K^*))$, and the **inertia degree** as the degree of the residue field extension.

Completeness

Prop. (12.1.1.20) [Cauchy Sequence of Non-Archimedean field]. For a sequence $\sum a_i$ in a non-Archimedean field, it is a Cauchy sequence iff $\lim |a_i| = 0$.

In particular, convergent sequence are all absolutely convergent and for a Cauchy sequence not converging to 0, the valuations of the terms stabilize.

Proof: One way is easy, the other way, notice $|\sum_{v=1}^j a_i| \leq \max_{i,j+1,...,j} |a_v| < \varepsilon$. □

Prop. (12.1.1.21) [Completion of a Field]. The completion of a non-Archimedean field is preferred to choose the definition of Cauchy sequence, so we see by (12.1.1.20) that $v(\hat{K}) = v(K)$.

Prop. (12.1.1.22). For a complete field $K$ and any finite vector space $L$, $L$ has only one norm up to equivalence and it is complete.

Proof: Cf. [Formal and Rigid Geometry P230]. □

Prop. (12.1.1.23). A complete valuation on a field can extend uniquely to a valuation on its alg.closure. And in the finite case, it is $|\alpha| = |N(\alpha)|^{\frac{1}{n}}$. This is an immediate consequence of (12.1.1.31) and (12.1.1.28), and $|\alpha| \leq 1$ iff it is integral over valuation ring $R$ of $K$.

Prop. (12.1.1.24). Any infinite separable algebraic extension of a complete field is never complete.

Proof: We use Krasner’s lemma (12.1.1.32). By Ostrowski theorem (10.3.3.18), we can assume it is non-Archimedean, otherwise it cannot by infinite dimensional. Choose an infinite linearly independent basis of decreasing value rapidly enough, then we can see the field generated by the limit contains all the partial sums, contradiction. □

Prop. (12.1.1.25). If $K$ is alg.closed valued field, then its completion is also alg.closed.

Proof: Let $L = \overline{K}$, then we can extend to a valuation on $L$, now let $f$ be a monic polynomial with coefficients in $\hat{K}$, we show its root $\alpha \in L$ can be approximated by elements in $K$, now let $g$ monic in $K[X]$ be an approximation of $f$ that $|g(\alpha)| \leq \varepsilon^n$, then there is a root $\beta$ of $g$ that $|\alpha - \beta| < \varepsilon$, and $\beta \in K$ by alg.closedness. □

Prop. (12.1.1.26). If $K$ is a complete valued field, then $K^{sep}$ is dense in $\overline{K}$.

Proof: Assume $F$ is non-Archimedean, then for $y \in F^{alg}$, there is a $n$ that $y^n = \alpha \in F^{sep}$. We may assume $|\alpha| \leq 1$, then let $\pi$ be an element that $|\pi| < 1$, then if $y_i$ is a root of the separable polynomial $Y^n - \pi^iY - \alpha = 0$, then $(y - y_i)^n = \pi^iy_i$. So $|y - y_i| \to 0$. □
**Henselian Valued Field**

**Def. (12.1.1.27)**[Henselian Valued Field]. A Henselian valued field is a valued field $K$ that the valuation ring $O_K$ is a Henselian local ring (4.3.10.1).

**Prop. (12.1.1.28).** $K$ is Henselian iff the valuation of $K$ has a unique extension to any finite extension $L/K$.

**Proof:** Cf. [Algebraic Number Theory Neukirch P144].

**Cor. (12.1.1.29).** Thus for a normal extension, $x$ and $\sigma(x)$ has the same valuation. Hence any polynomial in $K[X]$ has a decomposition into polynomials where all their roots has the same valuation.

**Prop. (12.1.1.30)**[Hensel’s Lemma Generalized]. Let $K$ be a complete valued non-Archimedean field and $O_K$ be the valuation ring. If $P, Q, R \in O_K[X]$ and $0 \leq \lambda < 1$ that $\deg P = m + n$, $\deg Q = n$, $\deg R = m$, and

$$\deg(P - QR) \leq m + n - 1, \quad |P - QR|_G \leq \lambda |\text{res}(Q, R)|^2$$

Where $| - |_G$ is the induced Gauss norm on $K[X]$. Then there exist polynomials $U, V$ that

$$|U|_G, |V|_G \leq \lambda |\text{res}(Q, R)|^2, \quad \deg U \leq n - 1, \quad \deg V \leq m - 1$$

and $P = (Q + U)(R + V)$.

**Proof:** If $\rho = |\text{res}(Q, R)| = 0$, then $P = QR$. Otherwise, the map $\theta_{Q, R} : W_m \oplus W_n \to W_{m+n}$ is invertible (2.2.2.11). Then we let $\varphi(U, V) = \theta_{Q, R}^{-1}(P - QR - UV)$, then If $U, V \in B(0, \lambda \rho)$, then $|\varphi(U, V)|_G \leq \lambda \rho$. And it can be proved $\varphi$ is a contraction map from $B(0, \lambda \rho)^2$ to itself with contraction factor $\lambda$, so it has a fixed point $(U, V)$ by (3.6.8.8). So $QU + RV = P - QR - UV$. □

**Cor. (12.1.1.31)**[Hensel’s Lemma]. Let $K$ be a complete valued non-Archimedean field and $A$ be the valuation ring. If $P(X) \in A[X]$ and $\alpha_0$ is an element of $A$ s.t. $|P(\alpha_0)/P'(\alpha_0)|^2 = \varepsilon < 1$, then there exists a $\alpha \in A$ that $P(\alpha) = 0$ and $|\alpha - \alpha_0| \leq |P(\alpha_0)/P'(\alpha_0)|$.

The usual form is when $|P'(\alpha_0)| = 1$, in which case we can pass to the residue field. Equivalently, a complete valued field is Henselian (12.1.1.27).

**Proof:** Let $\lambda = |P(\alpha_0)/P'(\alpha_0)|$ and $\text{res} = |P'(\alpha_0)|$. Notice If $P(X) = Q(X)(X - \alpha_0) + P(\alpha)$, then $\text{res}(Q(X), X - \alpha_0) = Q(\alpha_0) = P'(\alpha_0)$ (2.2.2.13). □

**Prop. (12.1.1.32)**[Krasner’s Lemma]. For a Henselian non-Archimedean field $K$, the if $\alpha, \beta \in \overline{K}$ that $|\alpha - \beta| < |\alpha - \sigma(\alpha)|$ for all $\sigma$, then $K(\alpha, \beta)/K(\beta)$ is purely inseparable. So when $\alpha$ is separable over $K$, $K(\alpha) \in K(\beta)$.

**Proof:** It suffice to prove that for all field morphism $\tau : K(\alpha, \beta) \to \overline{K}$ fixing $K(\beta), \tau(\alpha) = \alpha$. This is because $|\tau(\alpha) - \beta| = |\alpha - \beta| < |\alpha - \sigma(\alpha)|, \text{thus } |\tau(\alpha) - \alpha| \leq \max\{|\tau(\alpha) - \beta|, |\beta - \alpha|\} < |\alpha - \sigma(\alpha)|$. □

**Cor. (12.1.1.33).** If $f$ is a separable irreducible polynomial and $\alpha$ is a root, then for $g$ closed enough to $f$, there is a root $\beta$ of $g$ that $K(\beta) = K(\alpha)$. (Immediate consequence of (10.3.3.19)).

**Cor. (12.1.1.34).** Let $K$ be a non-Archimedean valued field with completion $\hat{K}$, then any finite separable extension $L/\hat{K}$ is of the form $\hat{L}\hat{K}$. (Because of Primitive element theorem).

**Cor. (12.1.1.35).** If a Henselian field is dense in its alg closure, then it is alg closed.

**Prop. (12.1.1.36)**[Kaplansky-Schilling]. A field which is Henselian w.r.t two inequivalent valuation is separably closed, and separably closed field is Henselian w.r.t any valuation.

**Proof:** □
2 Ultranormed Banach Spaces

In this section, denote $K$ a complete non-Archimedean field (of rank 1), $K^0 = \{ x \in K \mid |x| < 1 \}$, and $|t| < 1$ a uniformizer.

Ultranormed $K$-modules

Prop. (12.1.2.1). If $K$ is complete, then each normed $K$-module is weakly-Cartesian.

Proof: Cf. [Non-Archimedean Analysis P92].

Cor. (12.1.2.2). If $K$ is complete, any two valuation on a finite $K$-vector space are equivalent.

Proof: Cf. [Non-Archimedean Analysis P93].

Prop. (12.1.2.3). If $V$ is a normed $\mathbb{Q}_p$ vector space and $V_0 = \{ x \in V \mid |x| \leq 1 \}$, then $V^\wedge \cong (V_0)^\wedge [p^{-1}]$.

Ultranormed Banach Spaces

Def. (12.1.2.4) [Ultranormed Banach Spaces]. In the non-Archimedean case, an ultranormed Banach algebra is defined as in (10.6.4.2), but additionally $|a + b| \leq \max\{|a|, |b|\}$.

Def. (12.1.2.5) [Uniform Banach Space]. For a complete non-Archimedean field $K$ and a Banach algebra $R$, define $R^0$ to be the ring of power bounded elements. Then it is a subring, and it is open, as it contains the closed ball $B(0, 1)$.

Recall $R$ is called uniform if $R^0$ is itself bounded in $R$ (12.1.1.6). Notice a uniform Banach space must be reduced, because a nilpotent element is clearly power bounded, and any scalar multiple of it is nilpotent.

Lemma (12.1.2.6). Fix a uniformizer $t$ in a non-Archimedean complete field $K$, if $|K^*|$ is discrete, then if $A$ is a $t$-adically complete and $t$-torsion-free $K^0$-algebra, let $R = A[t^{-1}]$, then the norm

$$ |f| = \inf\{|t|^n |f| \in t^n A\}, $$

then this makes $R$ into a $K$-Banach space that the $t$-adic topology of $A$ is the same as the metric topology of $A$, so $A \subset R_{\leq 1} \subset R^0$.

Notice if $|K^*|$ is not discrete but there is a pseudo-uniformizer $t$ that has a compatible system of $p^n$-th roots, if $A$ is a $t$-adically complete and $t$-torsion-free $K^0$-algebra, let $R = A[t^{-1}]$, then the norm

$$ |f| = \inf\{|t|^n |f| \in t^n A\}, $$

then this makes $R$ into a $K$-Banach space that the $t$-adic topology of $A$ is the same as the metric topology of $A$, so $A \subset R_{\leq 1} \subset R^0$, and in this case $R^0 = A_\ast = \text{Hom}((t^{\frac{1}{p^n}}), A)$ (4.8.2.2).

Prop. (12.1.2.7) [Uniform $K$-Banach Space and $K^0$-Algebra]. Fix a pseudo uniformizer $t$ in a non-Archimedean complete field $K$, the following category are equivalent:

- The category $\mathcal{C}$ of uniform Banach $K$-algebras $R$.
- The category $\mathcal{D}_{\text{bic}}$ of $t$-adically complete and $t$-torsionfree $K^0$-algebras $A$ with $A$ totally integrally closed (4.2.1.1) in $A[t^{-1}]$. 

Proof: The functor $F : C \to \mathcal{D}_{\text{tie}}$ : if $R$ is uniform Banach space, then $F(R) = R^0$: $R^0$ is open subring by (12.1.2.5), and $R^0 \in B(0,r)$ for some $r > 0$ by uniformity. As $R$ is $K$-Banach, $\cap t^n B(0,r) = 0$, so $R^0$ is $t$-adically separated, and also it is complete. If $f^R \in t^{-k} R^0 \subset t^{-k} B(0,r)$, then clearly $f$ is power bounded thus $f \in R^0$, so $R^0$ is totally integrally closed in $R$. $R \to R^0$ is preserved by continuous mappings, so $F$ is truly a functor.

Conversely, lemma above (12.1.2.6) shows $R = A[t^{-1}]$ is a $K$-Banach algebra, this is a functor $G : \mathcal{D}_{\text{tie}} \to C$, and $A \subset R^0$. We show $A = R^0$, as this is equivalent to $FG \cong \text{id}$: as the $t$-adic topology and metric topology are the same (12.1.2.6), if $t^n f^R \subset A$ for some $c$, thus $f$ is totally integral over $A$, thus $f \in A$ by tic.

Finally, we need to show $GF \cong \text{id}$, which in fact that the given Banach algebra norm on $R$ is equivalent to the norm $| \cdot |$ given in (12.1.2.6) w.r.t $R^0$. $R_{<1}^c \subset R^0 \subset R_{\leq c}$ by uniformity, and conversely, $R_{<1}^c \subset R^0 \subset R_{\leq c}$, thus this two norms are equivalent. □

Prop. (12.1.2.8). Let $\varphi : A \to B$ be a $k$-homomorphism between $k$-Banach algebras that there is a family $\mathfrak{B}$ of ideals of $B$ that for each $b \in \mathfrak{B}$:

- $B$ is closed and $\varphi^{-1}(b)$ is closed in $A$.
- $\dim_k B/b < \infty$.
- $\cap_{b \in \mathfrak{B}} b = (0)$.

Then $\varphi$ is continuous.

Proof: Consider the map $A/\varphi^{-1}(b) \to B/b$ with the residue norms, Cf.[non-Archimedean analysis P167]. □

Cor. (12.1.2.9). Let $\varphi : A \to B$ be a $k$-homomorphism between Noetherian $k$-Banach algebras that there is a family $\mathfrak{B}$ of ideals of $B$ that for each $b \in \mathfrak{B}$, $\dim_k B/b < \infty$ and $\cap_{b \in \mathfrak{B}} b = (0)$, then $\varphi$ is continuous. (Because the closedness condition is automatic by (12.1.2.12)).

Cor. (12.1.2.10). All complete $k$-algebra norms on a Noetherian $k$-algebra $B$ satisfying the condition of (12.1.2.9) are equivalent.

Modules over $K$-Banach Spaces

Prop. (12.1.2.11). If $M$ is a normed module over a $k$-Banach algebra $A$, if the completion of $M$ is a finite $A$-module, then $M$ is complete.

Proof: There are morphism $\pi : A^0 \to \hat{M}$ that are surjective continuous, so by open mapping theorem (10.6.2.4), this map is open, so $\sum A x_i = \pi(A^0)$ is a nbhd of 0 in $\hat{M}$, because $\hat{A}$ is open (12.1.1.9) and then $\hat{M} = M + \sum A x_i$, because $M$ is dense in $\hat{M}$, then we are done by (12.1.1.10). □

Cor. (12.1.2.12) [Noetherian and Submodule Closed]. For a complete normed module over a $k$-Banach algebra $A$, $M$ is Noetherian iff all submodules of $M$ are closed. In particular, $A$ is Noetherian iff all ideals of $A$ are closed.

Proof: If $M$ is Noetherian, then the completion of any submodule is finite over $A$, so it is complete hence closed by (12.1.2.11). Conversely, if any ideal of $M$ is closed, then for a chain of ideals of $M : \cup M_i = M'$, $M'$ is complete hence Baire space by (3.6.9.2), so some $M_i$ must contain a nbhd of $M'$, because it is an ideal, but then $M_i = M'$. □
3 $p$-adic Analysis

Main References are [p-adic Analysis Robert].

Def. (12.1.3.1) [p-adic Fields]. For $p \in \mathbb{P}$, a $p$-adic field is a field $K$ of characteristic 0 that is complete w.r.t. a discrete valuation s.t. the residue field is perfect of characteristic $p$.

Prop. (12.1.3.2). For $b \in \mathbb{Z}_p$, we can define a power series in $\mathbb{Z}_p[[T]]$ as the limit of $(1 + a)^{bn}$ for $b_n \rightarrow b$ in $\mathbb{Z}_p$. So for $a \in \mathbb{C}_p$ with $v(a) > 0$, there can be defined an element $(1 + a)^b \in \mathbb{C}_p$, and we have $(1 + a)^b = \sum C^b_k a^k$.

Prop. (12.1.3.3). $\overline{\mathbb{Q}}_p$ is isomorphic to $\mathbb{C}$ as a field, uncanonically.

Proof: 

Cor. (12.1.3.4). The $p$-adic valuation on $\mathbb{Q}$ can be extended to $\mathbb{R}$ uncanonically.

Def. (12.1.3.5) [Topological Completion]. If $p \in \mathbb{P}$ and $K$ is a $p$-adic field, then we can define $\mathbb{C}_K = \overline{K}$, which is an alg.closed complete valued field, by (12.1.1.31)(12.1.1.28) and (12.1.1.25). Also denote $\mathbb{C}_p = \mathbb{C}_{\mathbb{Q}_p}$.

Fixed Fields in $\mathbb{C}_p$

Lemma (12.1.3.6). If $K$ a $p$-adic field and $P(X) \in \overline{K}[X]$ is a monic polynomial of degree $n$, and all of its roots satisfied $v_p(\alpha) \geq c$ for some constant $c$. Let $q = p^k$ if $n = p^k d, d \neq 1$ or $n = p^{k+1}$.

Then the derivative $P'(q)(X)$ has a root $\beta$ with $v_p(\beta) \geq c$ or in case $n = p^{k+1}$, $v_p(\beta) \geq c - \frac{1}{p_{p}(p-1)}$.

Proof: Let $P = X^n + a_{n-1}X^{n-1} + \ldots + a_0$, then $v_p(a_i) \geq (n-i)c$. And 

$$1/q! \cdot P'(q)(X) = \sum_{i=0}^{n-1} C^q_{n-i} a_{n-i} X^{-i-q}.$$

So at least one root $\beta$ satisfies $v_p(\beta) \geq \frac{1}{n-q} ((n-q)c - v_p(C^q_n)) = c - \frac{1}{p_{p}(p-1)}$.

Lemma (12.1.3.7). If $K$ is a $p$-adic field and $\alpha \in \overline{K}$, let $\Delta_K(\alpha) = \inf_{g \in \text{Gal}_K} v_p(g(\alpha) - \alpha)$, then there exists a $\delta \in K$ that $v_p(\alpha - \delta) \geq \Delta_K(\alpha) - p/(p-1)^2$.

Proof: We strengthen the assertion and use induction on $n = [K(\alpha) : K]$ to prove that there is a $\delta$ that $v_p(\alpha - \delta) \geq \Delta_K(\alpha) - \sum_{k=0}^{m} \frac{1}{p^k(p-1)}$, where $p^{m+1}$ is the largest power of $p$ that $\leq n$.

$n = 1$ is sure, let the minipoly of $\alpha$ over $K$ be $P(X)$. By lemma (12.1.3.6), there is a root $\beta$ of $P'(q)$ that $v_p(\beta - \alpha) \geq v_p(\alpha)$ or minus a factor when $n = p^{k+1}$. Then for any $\sigma$, $v_p(\sigma(\beta) - \beta) \geq v_p(\sigma(\alpha) - \alpha)$ or minus a factor. Then $\Delta(\beta) \geq \Delta(\alpha)$ or minus a factor. Now $[K(\beta) : K] < [K(\alpha) : K] = n$, so we can use induction hypothesis to get the result.

Remark (12.1.3.8). The constant $p/(p-1)^2$ can be replaced by $1/(p-1)$, and it is optimal: this is a theorem of Le Borgne in [Bor10].

Prop. (12.1.3.9) [Ax-Sen-Tate]. If $F$ is a $p$-adic field and if $K \subset F$, then $\overline{F}^{\text{Gal}_K} = \overline{K}$. Thus $\overline{L}^{\text{Gal}(L/K)} = \overline{K}$ for any alg.ext $L/K$.

Proof: Any $\alpha \in \overline{F}$ can be written as $\sum a_n$ with $a_n \in \overline{F}$. Then $\Delta_K(a_n) \rightarrow \infty$, and $a_n$ can be approximated by $\delta_n \in K$ by lemma (12.1.3.7), thus $\alpha \in \overline{K}$.
Holomorphic functions

**Def. (12.1.3.10).** For a $p$-adic field $L$, denote by $\mathcal{L}_L$ the set of Laurent series with coefficients in $L$, then the set of valuations that a Laurent series converges $\text{Conv}(f)$ is an interval of $[-\infty, +\infty]$. Let $A(I)$ denote the set of elements in $L$ of valuation in $I$.

If $f$ is bounded at $r_1, r_2$, then it is convergent on $(r_1, r_2)$.

**Def. (12.1.3.11).** Denote

$\mathcal{L}_L[r_1, r_2] = \{ f | f \text{ is convergent on } [r_1, r_2] \}$.

$\mathcal{L}_L(r_1, r_2] = \{ f | f \text{ is convergent on } (r_1, r_2] \}$.

$\mathcal{L}_L[r_1, r_2] = \{ f | f \text{ is convergent on } (r_1, r_2] \text{ and bounded at } r_1 \}$.

$\mathcal{B}_L(I)$ is the subset of bounded functions. These are all rings under addition and multiplication. And if we define $v^{(r)}(f)$ as the minimum of $v(a_n) + nr$, then it is a valuation on these rings.

**Proof:** Cf. [Foundations of Theory of $(\varphi, \Gamma)$-modules over the Robba Ring P31].

**Def. (12.1.3.12).** If we set for $\mathcal{L}_L[r_1, r_2]$ the the valuation $v^{[r_1, r_2]}(f) = \min\{v^{(r_1)}(f), v^{(r_2)}(f)\}$, then this is a valuation on it.

**Prop. (12.1.3.13).** $\mathcal{L}_L(\{ r \})$ is complete under valuation $v^{(r)}$. Similarly the valuation $v^{[r_1, r_2]}(f)$ makes $\mathcal{L}_L[r_1, r_2]$ a Banach space unless $r_1 = r_2 = \infty$.

**Proof:** We let $r = 0$. For a Cauchy sequence of Laurent series, we see that each coefficient is a Cauchy sequence, hence converges to some element in $L$, so it converges term-wise to a Laurent series $f$, so it converges to $f$ in $v^{(r)}$.

**Cor. (12.1.3.14).** We consider $\mathcal{L}_L(0, r]$, then it has a countable sequence of norms $v^{1/n, r}$, which makes it a locally convex space, and the last proposition shows that these valuations are complete, and a Cauchy sequence converges to the term-wise limit, so $\mathcal{L}_L(0, r]$ is a complete Fréchet space in the Fréchet topology.

**Cor. (12.1.3.15).** The same method shows that $\mathcal{L}_L(I)$ is a Fréchet space for any interval $I$.

**Def. (12.1.3.16)[Robba Ring and Overconvergent Elements].** We define $\mathcal{E}$ as the Laurent sequences that are bounded at 0 and $\lim_{n \to -\infty} v(a_n) = \infty$, and we define the overconvergent elements $\mathcal{E}^\dagger$ and Robba ring $\mathcal{R}$ as

$$
\mathcal{E}^\dagger = \bigcup_{r > 0} \mathcal{L}_L[0, r], \quad \mathcal{R} = \bigcup_{r > 0} \mathcal{L}_L(0, r], \quad \mathcal{E}^\dagger \subset \mathcal{R}
$$

and equip them with the final topology w.r.t. the Fréchet topologies on $\mathcal{L}_L(0, r]$. And denote by $\mathcal{E}^+ = \mathcal{E}^\dagger \cap L[[T]]$ and $\mathcal{R}^+ = \mathcal{R} \cap L[[T]]$.

For more properties of Robba ring, See [Foundations of Theory of $(\varphi, \Gamma)$-modules over the Robba Ring Chap4].

**Def. (12.1.3.17)[Newton Polygon].** For a non-Archimedean valued field $K$ and a polynomial or power series $P(X) = a_0 + a_1X + \cdots + a_dX^d \in K[X]$, we denote by Newton polygon as the lower convex hull of the set of points $(0, v(a_0)), (1, v(a_1)), \ldots, (d, v(a_d))$.

**Prop. (12.1.3.18)[Roots and Newton Polygon].** For a non-Archimedean valued field $K$ the number of roots of $P$ in $\bar{K}$ with valuation $\lambda$ equals the horizontal width of the segment of Newton polynomial of $P$ of slope $-\lambda$. 
Proof: We may assume $P$ is monic, then its coefficients are elementary polynomials of roots of $P$. And the conclusion follows as $K$ is non-Archimedean. □

For Newton polynomial of power series, see [Berger Galois Representations Chap3] and Reference [Zeros of Power Series over complete Valued Field Lazard].

Prop. (12.1.3.19). If $I = ]0, +\infty]$ and $f(X) \in \mathcal{H}(I)$, then the number of zeros of $f(X)$ in $\mathcal{A}(I)$ equals the length of the segment of $NP(f)$ whose slope is $-s$, and these roots gives a $P_s(X) \in K[X]$ that $f(X) = P_s(X)G(X)$, $G(X) \in \mathcal{H}(I)$.

Proof: Cf. [Zeros of Power Series over complete Valued Field Lazard]. □

Cor. (12.1.3.20). If $f(X) \in \mathcal{H}(I)$, then $f(X) \in \mathcal{B}_L(I)$ iff it has f.m. zeros in $\mathcal{A}(I)$.

Proof: Let $r = \inf I$ and $s = \sup I$. First notice that $f \in \mathcal{L}_L(I)$ is in $\mathcal{B}(I)$ iff $v(a_n) + nr$ is bounded from below as $n \to +\infty$ and $v(a_n) + nr$ is bounded below as $n \to -\infty$. And from the graph of $NP(f)$, this is equivalent to $f$ has f.m. zeros in $\mathcal{A}(I)$. □

Prop. (12.1.3.21). $\mathcal{H}(I)$ is a Bezout domain.

Formal Power Series

Cor. (12.1.3.22) [Convergence of Power Series]. Let $(R, \mathfrak{m})$ be a CDVR of characteristic 0 of residue characteristic $p$, then

- If $f(T) = \sum_{n \geq 1} a_n T^n \in (R \otimes \mathbb{Q})[[T]]$ with $a_n \in R$, then $f(x)$ converges in $R$ for $x \in \mathfrak{m}$.

- If $g(T) = \sum_{n \geq 1} b_n T^n \in (R \otimes \mathbb{Q})[[T]]$ with $b_n \in R$, then $f(x)$ converges in $R$ for $v(x) > v(p)/(p-1)$.

Proof: 1: $v(a_n x^n /n) \geq nv(x) - v(n) \geq nv(x) - \log_p(n) v(p)$ converges to $\infty$ for $n \to \infty$ when $v(x) > 0$.

2: $v(b_n x^n /n!) \geq nv(x) - v(n!) \geq nv(x) - (n-1)v(p)/(p-1)$ (20.1.2.2) converges to $\infty$ for $n \to \infty$ when $v(x) > v(p)/(p-1)$ □
12.2 Algebraic Number Theory


Notations(12.2.0.1).

• Use notations defined in Commutative Algebra II.
• Use notations defined in Valuations of Rank 1, all valuations are of rank1.
• Use notations defined in More on (Non-Commutative)Algebras.

1 Basics

Prop.(12.2.1.1). Let $p \in \mathbb{P}$, then

• $p$ can be written as the form $x^2 + y^2$ iff $p = 2$ or $p \equiv 1 \text{ mod } 4$.
• $p$ can be written as the form $x^2 + 2y^2$ iff $p = 2$ or $p \equiv 1, 3 \text{ mod } 8$.

Proof: □

2 Ramification Theory of Valued Fields

In this subsection ramification theory of local fields, or more generally Henselian valued fields are studied.

Notations(12.2.2.1).

• Let $(R, K, k)$ be a Henselian non-Archimedean valued field.

Lemma(12.2.2.2)[Extension is Monogenous]. For a finite extension of CDVR, if the residue field extension $\lambda/k$ is separable, then there exists a $x \in \mathcal{O}_L$ that $\mathcal{O}_L[x] = \mathcal{O}_L$.

Proof: If $\pi$ is an element of $\lambda$ that generate $\lambda$ over $k$, by primitive element theorem, then let $f$ be the minipoly of $\pi$, then let $f, x$ be lifting of them, then $f(x)$ is a uniformizer, otherwise $f'(x)$ has valuation 0, so $f(x + \pi_L)$ is a uniformizer. Now we see that $x^i f(x)^j$ is a basis of $\mathcal{O}_L$ over $\mathcal{O}_K$, □

Prop.(12.2.2.3). If $L/K$ is a finite separable extension and if $I$ is an ideal of $\mathcal{O}_L$, then $v_K(\text{tr}_{L/K}(I)) = [v_K(I \cdot D_{L/K})]$. 

Proof: By definition, $\text{tr}_{L/K}(x \mathcal{O}_L) \subset \mathcal{O}_K$ iff $x \in D_{L/K}^{-1}$, thus $\text{tr}_{L/K}(I) \subset J$ iff $I \subset D_{L/K}^{-1}J$, i.e. $\text{tr}_{L/K}(I)$ is the smallest ideal $J$ of $\mathcal{O}_K$ that contains $I \cdot D_{L/K}$, thus the result. □

Unramified Extensions

Def.(12.2.2.4)[Unramified Extensions]. For $K$ a Henselian non-Archimedean valued field, $L/K$ a finite extension is called unramified extension if the residue field extension $\lambda/k$ is separable and $[L : K] = [\lambda : k]$. Any algebraic extension is called unramified iff any finite extension is unramified.

This is compatible because unramified extensions form a distinguished class. So we can talk about the maximal unramified extension $T$ of $K$, and a field extension $L/K$ is called unramified if all finite subextensions are unramified.
Proof: It is faithfully transitive because the field extension degree is transitive, and for base change, as the residue field is separable, we let \( \lambda = k[\pi] \), and choose a lift \( \alpha \in \mathcal{O}_L \), the minipoly of \( \alpha \) is \( f(X) \in \mathcal{O}_K[X] \). Then we have

\[
[\lambda : k] \leq \deg \overline{f} = \deg f = [K(\alpha) : K] \leq [L : K] = [\lambda : k]
\]

So \( L = K(\alpha) \) and \( \overline{f} \) is the minipoly of \( \overline{\alpha} \). Then \( L' = K'(\alpha) \), and let \( g(X) \) be the minipoly of \( \alpha \) over \( K' \), then \( \overline{g} \) is a factor of \( \overline{f} \) so separable, hence irreducible by Hensel’s lemma. Noe:

\[
[\lambda' : k'] \leq [L' : K'] = \deg g = \deg \overline{g} = [k'(\alpha) : k] \leq [\lambda' : k].
\]

So \( [\lambda' : k'] = [L' : K'] \). \( \square \)

Prop. (12.2.2.5) [Maximal Unramified Extension]. The residue field of the maximal unramified extension \( K^{ur}/K \) is \( \overline{k} \), and the value group is the same as \( K \).

Proof: The first assertion is because for any separable polynomial, it has a lift which is irreducible has a root lifting \( \overline{\alpha} \), contradicting the maximality. For the second, look at finite subextensions, then it results from the fundamental inequality (10.3.3.20). \( \square \)

Tamely Ramified Extension

Def. (12.2.2.6) [Tamely Ramified Extension]. For \( K \) a Henselian non-Archimedean valued field, a finite field extension \( L/K \) is called a tamely ramified extension if the residue field extension is separable and \( ([L : T], p) = 1 \), where \( T \) is the maximal unramified subextension.

Prop. (12.2.2.7). Tamely unramified extensions form a distinguished class, so we can talk about the maximal tamely unramified extensions, and a field extension \( L/K \) is called tamely ramified if all finite subextensions are tamely unramified.

Proof: Cf. [Algebraic Number Theory Neukirch P156]. \( \square \)

Prop. (12.2.2.8). A finite extension \( L/K \) is tamely ramified if and only if the extension is generated by radicals over the maximal unramified extension: \( L = K^{ur}(\sqrt[\sqrt[p]{a_i}}), (m, p) = 1 \), where \( a_i \in K^{ur} \), (WARNING: make sure if \( a_i \in K \) or not?).

Proof: Cf. [Algebraic Number Theory Neukirch P155]. \( \square \)

Prop. (12.2.2.9). The value field of tamely ramified extensions. Cf. [Neukirch P157].

Totally Ramified Extension

Def. (12.2.2.10) [Eisenstein Polynomial]. Let \( K \) be a DVR with uniformizer \( \pi \), an Eisenstein polynomial in \( K[X] \) is a polynomial of the form

\[
f(x) = x^n + a_{n-1}x^{n-1} + \ldots + a_1x + a_0
\]

where \( a_i \in (\pi) \) for any \( i \) and \( a_0 \in (\pi) \setminus (\pi^2) \).
Ramification Groups

Def. (12.2.2.11)[Ramification Groups]. For a Galois field extension $L/K$ and a valuation extension $w/v$, denote $\lambda/k$ residue fields extension of $w/v$, and denote $m_w, m_v$ by $\mathfrak{P}, p$.

Then the decomposition group is $G_w(L/K) = \{\sigma \in G(L/K)| w \circ \sigma = w\}$. The decomposition field $Z_w$ is the fixed field of $G_w$.

When $w$ is non-Archimedean, we further define:

The inertia group is $I_w(L/K) = \{\sigma \in G_w(L/K)| \sigma(x) \equiv x \mod \mathfrak{P}\}$. The inertia field $T_w$ is the fixed field of $I_w$.

The ramification group is $R_w(L/K) = \{\sigma \in G_w(L/K)| \sigma(x)/x \equiv 1 \mod \mathfrak{P}\}$. The ramification field $V_w$ is the fixed field of $R_w$.

Prop. (12.2.2.12). For a local field, the ramification degree $e$ equals the order of inertia group $|I_{L/K}|$.

Prop. (12.2.2.13). $G_w(L/K) \cong G(L_w/K_v), I_w(L/K) \cong I(L_w/K_v), R_w(L/K) \cong R(L_w/K_v)$ by natural restriction.

Prop. (12.2.2.14)[$Z_w$].
- The restriction $w_Z$ of $w$ to $Z_w$ extends uniquely to $L$.
- If $v$ is non-Archimedean, $w_Z$ has the same residue field and value group as $v$.
- $Z_w = L \cap K_v \subset L_w$.

Proof: Cf.[Neukirch P171].

Prop. (12.2.2.15). When $v$ is non-Archimedean, the residue field extension $\lambda/k$ is normal and there is an exact sequence

$$1 \to I_w \to G_w \to \text{Gal}(\lambda/k) \to 1.$$ 

Proof: Cf.[Neukirch P172].

Prop. (12.2.2.16). $T_w/Z_w$ is the maximal unramified subextension of $L/Z_w$.

Proof: Cf.[Neukirch P173].

Prop. (12.2.2.17). If $v$ is non-Archimedean, there is an exact sequence

$$1 \to R_w \to I_w \to \chi_v(L/K) \to 0$$

where $\chi_v(L/K) = \text{Hom}(\Delta/\Gamma, \lambda^*)$, where $\Delta = w(L^*), \Gamma = v(K^*)$. Moreover, in case $L/K$ is a finite extension, this exact sequence splits.

Proof: For any $\sigma \in I_w$, define the map $\chi_\sigma : \Delta/\Gamma \to \lambda^*$ as follows: for any $\delta \in \Delta/\Gamma$, let $\delta = w(x)$ for some $x \in L^*$, let $\chi_\sigma(\delta) = \frac{\sigma(x)}{x} \mod \mathfrak{P}_w$. This is independent of $x$ chosen, because if $w(x) \equiv w(x') \mod \Gamma$, then $w(x) = w(ax)$ for some $a \in K^*$, thus $x = axu$ for some $u \in O_w^*$. Now $\frac{\sigma(x)}{x} \equiv 1 \mod \mathfrak{P}$ as $\sigma \in I_w$, so $\frac{\sigma(x)}{x} = \frac{\sigma(x')}{x'} \in \lambda^*$. And the kernel of this map is $R_w$ by definition.

The sequence is exact on the right by [Neukirch P175].

Prop. (12.2.2.18). $R_w$ is the unique pro-$p$-Sylow subgroup of $G_w(2.1.14.11)$.

Proof: Cf.[Neukirch P174].
Prop. (12.2.2.19). $V_w/Z_w$ is the maximal tamely ramified subextension of $L/Z_w$.

Proof: Cf. [Neukirch P175]. \hfill \Box

Prop. (12.2.2.20) [Tame Characters]. Let $K/Q_p$ be a local field, for any system of roots of unity $\{\xi_n| (n, p) = 1\}$, there is an isomorphism

$$I_K/R_K \cong \text{Gal}(K^{\text{tame}}/K^{\text{ur}}) \cong \prod_{l \neq p} \mathbb{Z}_l$$

and the projection to $\mathbb{Z}_l$ is called the $l$-adic tame character of $G_K$.

Equivalently, it is the character $t_l$ of $G_K$ that $\sigma(\xi_n^m) = \xi_n^\chi_l(\sigma)$.

Prop. (12.2.2.21). The maximal tamely ramified Abelian extension of $Q_p$ is finite over the maximal unramified Abelian extension of $Q_p$.

Proof: \hfill \Box

Prop. (12.2.2.22). The maximal unramified extension of $F_p((t))$ is $T = \mathbb{F}_p((t))$, and the maximal tamely unramified extension of $F_p((t))$ is $T(\sqrt[m]{u}|(m \geq 1, p) = 1}$.

Proof: \hfill \Box

Prop. (12.2.2.23). If the residue field $k$ is finite, then any finite quotient group of $G_w$ is solvable.

Proof: This follows from (12.2.2.18)(12.2.2.15)(12.2.2.17) and (2.1.14.12) and (2.1.7.2). \hfill \Box

Higher Ramification Groups

Def. (12.2.2.24) [Higher Ramifications]. For $L/K$ be a finite Galois extension of CDVRs, we define the $s$-th ramification group $G_s(L/K) = \{\sigma \in G| v_L(\sigma(x) - x) \geq s + 1 \text{ for all } a \in \mathcal{O}_L\}$.

Then we have $G = G_{-1} \supset G_0 \supset G_1 \supset \ldots$. And $G_0$ is the inertia group.

Prop. (12.2.2.25). When $K$ has finite residue field, $G_1$ is the ramification group $R_w(12.2.2.11)$. In this case, we have

$$G_s(L/K) = \{\sigma \in G_0| \frac{\sigma(\pi_L)}{\pi_L} \in U_L^s\}, \text{ for } s \geq 0.$$ 

So there are injective morphism $G_s/G_{s+1} \to U_L^s/U_L^{s+1}: \sigma \mapsto \sigma(\pi_L)/\pi_L$ for $s \geq 0$. (This is independent of $\pi_L$ chosen because units are mapped mod $U_L^{s+1}$).

Proof: $G_1 = R_w$: one direction is trivial, for the other, we use Teichmüller representatives, then $R_w$ preserves all them, and $\sigma(x) - x \equiv 0 \mod \mathfrak{P}^2$ is true for $\pi$, so it is true for all. \hfill \Box

Prop. (12.2.2.26). For local fields $L/K$, if $\sigma$ is in the inertia group, then

$$v_L\left(\frac{\sigma(x)}{x} - 1\right) \geq v_L\left(\frac{\sigma(\pi_L)}{\pi_L} - 1\right) + \delta_{v_L(x),0}$$

for any $x \in \mathcal{O}_L$ and a uniformizer $\pi_L$. Equality holds when $v_L(x) = 1$. 

Proof: if $L$ has residue field $\mathbb{F}_q$, then any element of $L$ can be written as $\sum \xi_n \pi^n_L$, where $\xi_n$ are all $q - 1$-th roots of unity. And because $\sigma$ is inertia group, all $q - 1$-th roots of unity are preserved, so $\sigma(\xi_n \pi^n_L) = \xi_n \pi_L^{\sigma(\pi_L)} - 1(\sigma(\pi_L)^{n-1} + \sigma(\pi_L)^{n-2} \pi_L + \ldots + \pi_L^{n-1})$ has valuation $\geq v^{(\pi_L)} - 1 + n$. Thus the result. \qed

In the sequel, we assume that the residue field extension is separable, as to use the proposition\((12.2.2.2)\).

**Lemma (12.2.2.27).** We define $i_{L/K}(\sigma) = v_L(\sigma x - x)$, where $x$ is the generator of $O_L/O_K$.

If $L/L'/K$ are Galois extensions that $e$ is the ramification index of $L/L'$. Then

$$i_{L/K}(\sigma') = \frac{1}{e} \sum_{\sigma|_{L'} = \sigma'} i_{L/K}(\sigma).$$

**Proof:** Cf.\([\text{Neukirch Algebraic Number Theory P}178]\). \qed

**Def. (12.2.2.28) [Upper Numbering].** We define the Herbrand function $\varphi_{L/K}(u) = \int_0^u \frac{dx}{(G_0, \sigma x)}$. It maps $\{x \geq 1\}$ to itself and is strictly increasing.

If $m \leq s < m + 1$, then it is just $\varphi_{L/K}(s) = \frac{1}{g_0} (g_1 + g_2 + \ldots + g_m + (s - m)g_{m+1})$, where $g_i = |G_i|$. By a double counting, it is

$$\varphi_{L/K}(s) = \frac{1}{g_0} \sum_{s \in G} \min\{i_{L/K}(\sigma), s + 1\} - 1.$$ 

The derivative of $\varphi_{L/K}$ is $\varphi'_{L/K}(s) = \frac{|G_s|}{g_0}$.

Let $\psi_{L/K}$ be the inverse function of $G = G_{\psi_{L/K}(t)}$, this is called the upper numbering.

**Lemma (12.2.2.29).** For $L/L'/K$ Galois extensions, one has $G_s(L/K)H/H = G_t(L'/K)$, where $t = \varphi_{L/L'}(s)$. Equivalently, $G_s/H_s = (G/H)\varphi_{L/L'}(s)$.

**Proof:** For $\sigma' \in G(L'/K)$, we choose a inverse image $\sigma \in G(L/K)$ of maximal $i_{L/K}(\sigma)$, then $i_{L'/K}(\sigma') - 1 = \varphi_{L/L'}(i_{L/K}(\sigma) - 1)$. To prove this, let $i_{L/K}(\sigma) = m$, then we see $i_{L/K}(\sigma \tau) = \min\{i_{L/K}(\tau), m\}$, so by\((12.2.2.27)\), $i_{L'/K}(\sigma') = \frac{1}{e} \sum_{\tau \in H} \min\{i_{L/K}(\tau), m\}$. And $e = |H_0|$ by\((12.2.2.12)\). So the assertion follows from\((12.2.2.28)\).

Now $\sigma'$ is in the image of $G_s$ is equivalent to $i_{L/K}(\sigma') - 1 \geq s \iff \varphi_{L/L'}(i_{L/K}(\sigma') - 1) \geq \varphi_{L/L'}(s)$, which by what proved is equivalent to $\sigma' \in G_t(L'/K)$. \qed

**Cor. (12.2.2.30).** For $L/L'/K$ Galois extensions, $\varphi_{L/K} = \varphi_{L'/K} \circ \varphi_{L/L'}$, hence similar formula holds for $\psi$.

**Proof:** By the proposition and multiplicity of ramification index $e$, we get

$$\frac{1}{e_{L/K}}|G_s| = \frac{1}{e_{L'/K}}|G/H|t \frac{1}{e_{L/L'}}|H_s|.$$ 

where $t = \varphi_{L/L'}(s)$, which is equivalent to the derivative $\varphi'_{L/K}(\sigma) = \varphi'_{L'/K}(t)\varphi'_{L/L'}(s) = (\varphi_{L'/K} \circ \varphi_{L/L'})'(s)$, and they are equal at 0, so the conclusion follows. \qed
Prop. (12.2.2.31) [Herbrand’s Theorem]. For $L/L'/K$ Galois extensions, $G^t(L'/K)$ is the image of $G^t(L/K)$ under the quotient.

Proof: Let $r = \varphi_{L'/K}(t)$, by the above lemma and corollary,

$$G^tH/H = G\varphi_{L/K}(t)H/H = G\varphi_{L'/L}(\psi_{L/K}(t)) = G\varphi_{L'/L}(\psi_{L'/K}(r)) = G_r(L'/K) = G^t(L'/K)$$

□

Prop. (12.2.2.32) [Hasse-Arf]. For an Abelian extension of CDVRs $L/K$ that the residue field extension is separable, the jump in the upper numbering of higher ramification group $G^v$ must happen at integers. (Note: The proof in the case where $K$ is a local field is much easier by Lubin-Tate group, see (12.4.2.28)).

Proof: The theorem is just saying that if $G_s \neq G_{s+1}$ for $s$ integer, then $\varphi_{L/K}(s)$ is an integer. This follows follows from the following lemma, because if $G$ is not totally ramified, then we can change it to the Galois field of $G_0$, this didn’t change anything by the definition of (12.2.2.28), and the fact $\varphi(0) = 0$. And when $G^v \neq G^{v+}$, then we consider splitting $G/G^{v+}$ into product of cyclic groups, thus there is one cyclic group $H$ that the projection of $G^v$ into $H$ is not trivial. Now $H$ is a Galois group of some $L'/K$, and Herbrand’s theorem shows that $H^v \neq H^{v+}$, hence $v$ is an integer by the following lemma. □

Lemma (12.2.2.33). For a cyclic totally ramified extension of CDVRs $L/K$ that the residue field extension is separable, if $\mu$ is the maximal integer that $G_\mu \neq 1$, then $\varphi_{L/K}(G_\mu)$ is an integer.

Proof: Cf.[Serre Local Fields P94]. □

Remark (12.2.2.34). An example: If $F_n = \mathbb{Q}_p(\zeta_{p^n})$, then

$$G(F_n/\mathbb{Q}_p)_s = G(F_n/F_i) \text{ for } p^j - 1 \leq s < p^{j+1} - 2.$$  

(This is because $\zeta_{p^n} - 1$ is a uniformizer of $F_n$). Thus $G(F_n/\mathbb{Q}_p)^i = G(F_n/F_i).

3 Local Fields

Def. (12.2.3.1) [Local Fields]. A local field is a locally compact valued field. A local field is clearly complete. The category of local fields is denoted by $\text{LField}$.

Prop. (12.2.3.2) [Complete Valued Fields]. A complete Archimedean valued field must be $\mathbb{R}$ or $\mathbb{C}$, by (10.3.3.18).

Any non-Archimedean complete valued field is discretely valued, and has finite residue fields of characteristic $p \in \mathbb{P}$. Such a field is called a $p$-adic local fields. The category of $p$-adic local fields is denoted by $p-\text{LField}$.

A $p$-adic local field is a $p$-adic field(12.1.3.1).

Proof: Cf.[Sutherland, L9]. □

Remark (12.2.3.3). The valuation ring of a $p$-adic local field is a Dedekind domain, thus the theory of Dedekind domains applies to this case.

Prop. (12.2.3.4) [$p$-adic Local Fields]. $p$-adic local fields are precisely the finite extensions of the field $\mathbb{Q}_p$ or $\mathbb{F}_p((t))$, called $p$-adic number field and $p$-adic function field respectively.

The category of $p$-adic number fields are denoted by $p-\text{NField}$, and the category of $p$-adic function fields are denoted by $p-\text{FField}$.

Proof: Cf.[Neukirch Algebraic Number Theory P135]. □
The Group Structure of Local Fields

Prop.(12.2.3.5). For $m > 0$, there is an isomorphism $(-)^m : U^n \cong U^{n+v(m)}$ when $n$ is sufficiently large.

Proof: Let $m = u\pi^v(m)$. For surjectivity, we need to find $x$, that $1 + a\pi^{n+v(m)} = -(1 + x\pi^n)^m$.

\[-a + ux + \pi^{n-v(m)}f(x) = 0.\]

This has a solution $x$ by Hensel’s lemma. \hfill \Box

Cor.(12.2.3.6). $(K^*)^m$ is an open subgroup of $K^*$, and $\cap_m(K^*)^m = 1$. (Because if $a \in \cap_m(K^*)^m = 1$, then $a$ is a unit, thus $a \in \cap_m(U)^m = 1$, thus $a \in U^n$ for every $n$ thus $a = 1$).

Prop.(12.2.3.7). $[K^* : (K^*)^m] = m \cdot |m|_p^{-1} : |\mu_m(K)|$.

Proof: Use the multiplicative Herbrand quotient (3.3.4.7), $(K^* : (K^*)^m) = q_{0,m}(K^*|\mu_m(K)|$. $q_{0,m}$ is additive, thus

$q_{0,m}(K^*) = q_{0,m}(K/U)q_{0,m}(U/U^n)q_{0,m}(U^n)$.

$q_{0,m}(K/U) = m$, $q_{0,m}(U/U^n) = 1$ as $U/U^n$ is finite (3.3.4.9). It for $q_{0,m}(U^n)$, when $n$ is large, it equals $(U^n : U^{n+v(m)})$ by (12.2.3.5), which is $|m|_p^{-1}$. \hfill \Box

Prop.(12.2.3.8) [p-adic Logarithm]. For a $p$-adic number field $K$, there is a unique $p$-adic logarithm function $\log : K^* \to K$ that $\log(p) = 0$, and for $x \in p$, it is defined to be

$\log(1 + x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \ldots$.

Moreover, for $n > \frac{\epsilon_K}{p-1}$, there is a map $\exp : p^n \to U^n$ which is an inverse to $\log$ on $U^n$, so $U^n \cong p^n$.

Proof: This follows from (7.5.4.8). \hfill \Box

Remark (12.2.3.9). In fact, this map can be extended to a function from $C_p^*$ to $C_p$.

Cor.(12.2.3.10). For a local field $K$, $O_K^*$ thus also $K^*$ are locally compact.

Proof: For $n$ large, $U^n \cong p^n$ is compact. \hfill \Box

Prop.(12.2.3.11) [Multiplicative Group Structure]. For a local field $K$,

- If char $K = 0$, then $O_K^* \cong \mathbb{Z}/(p-1)\mathbb{Z} \oplus \mathbb{Z}/p^d\mathbb{Z} \oplus \mathbb{Z}_p^\times$, where $d = [K : Q_p]$.
- If char $K = p$, then $O_K^* \cong \mathbb{Z}/(p-1)\mathbb{Z} \oplus \mathbb{Z}_p^\times$.

Proof: Cf.[Neukirch P140]. \hfill \Box

Prop.(12.2.3.12). Any automorphism of $\mathbb{R}$ or a $p$-adic number field is identity.

Proof: It suffices to show that an automorphism is continuous. For $\mathbb{R}$, this is because $a > 0 \iff a = b^2 \iff \sigma(a) = \sigma(b)^2 \iff \sigma(a) = 0$, and $\mathbb{Q}$ is dense in $\mathbb{R}$.

For a local field, we prove that $\sigma(O_K^*) \subset O_K^*$. $O_K^*$ is characterized by the property that $\{n|y^n = x\}$ are infinite. This is because $x^p = a$ has a root for $a \in O_K^*$ for $p$ large prime, by Henselian lemma. \hfill \Box

Def.(12.2.3.13) [Norm Groups]. For any extension of local fields $L/K$, $Nm_{L/K}$ is open, and $\mathcal{N}_{L/K} = Nm_{L/K} L^x \subset K^x$ is called the norm group of $L/K$. 

12.2. ALGEBRAIC NUMBER THEORY 1153

Ramifications of Cyclotomic Fields($\mathbb{Z}_p$-Extensions)

Prop.(12.2.3.14)[Unramified case]. For $K$ a finite extension of $\mathbb{Q}_p$ with residue field $\mathbb{F}_q$, we consider $L = K(\zeta_n)/K$, where $(n, p) = 1$. Then it is unramified of degree $f$ where $f$ is the minimal number that $q^f \equiv 1 \mod n$. And $\mathcal{O}_L = \mathcal{O}_K[\zeta_n]$.

Proof: $\zeta$ is a root of $\Phi_n | X^n - 1$, which is separable in $k$, so $\Phi$ and $\Phi$ are both irreducible of the same degree by Hensel’s lemma, so it is unramified, and $\lambda$ is the minimal extension of $\mathbb{F}_q$ that contains the $n$-th roots and are generated by it, thus the result by the theory of finite fields.

For the last assertion, notice it is unramified so $\mathcal{O}_L = \mathcal{O}_K[\zeta_n] + p\mathcal{O}_L$ hence the result follows from Nakayama.

Cor.(12.2.3.15). The maximal unramified extension of $K$ is generated by adjoining all $n$-th roots where $(n, p) = 1$. This is because there is an inclusion relation and their residue field $\mathbb{F}_p$ is already generated by roots of unity.

Prop.(12.2.3.16)[Totally Ramified case]. Consider $\mathbb{Q}_p$ (other local fields behave different), we have the $\mathbb{Q}(\zeta_{p^n})/\mathbb{Q}$ is totally ramified of degree $\varphi(p^n)$ the Galois group is $(\mathbb{Z}/p^n\mathbb{Z})^*$. The ring of valuation of $\mathbb{Q}(\zeta_{p^n})$ is $\mathbb{Z}_p[\zeta_{p^n}]$ and $1 - \zeta_{p^n}$ is a uniformizer.

Proof: $\zeta$ is a root of the polynomial $\Phi = X^{p^n-1}(p-1) + X^{p^n-2}(p-1) + \ldots + 1 = 0$, which equals $\frac{X^{p^n-1}}{X^{p^n-1}} \equiv (X - 1)p^{n-1}(p-1) \mod p$ and $\Phi(1) = p$, so $\Phi(1) = p$, so it is a uniformizer. The ring of integer is generated by a uniformizer by (10.3.3.20) as the extension is totally ramified.

Prop.(12.2.3.17). The cyclotomic field $\mathbb{Q}[\zeta_n]$ has integral basis.

Proof: Cf.[Algebraic Number Theory Milne P98].

Prop.(12.2.3.18)[Infinite Cyclotomic Field]. For a $p$-adic number field $K$, let $K_n = K(\zeta_{p^n})$ and $K_\infty = \cup K_n$ and $F = \mathbb{Q}_p$. Let $\chi$ be the cyclotomic character, then $\chi(G_K)$ is an open subgroup of $\mathbb{Z}_p^*$, thus contains a $U_n$ for some $n$. Thus there is an isomorphism of groups: $\chi^{-1}(U_n)/\chi^{-1}(U_{n+1}) \cap G_K \cong \chi^{-1}(U_n)G_K/G_K$, which has order $p$, for $n$ large.

So $K_{n+1}/K_n$ is totally ramified of degree $p$, because $K_n = K \cdot F_n$, and its value group extension is of degree $p$, too.

And $[K_n : F_n]$ is decreasing and eventually equals to $[K_\infty : F_\infty]$. This is because its order equals $\chi^{-1}(U_n)/\chi^{-1}(U_n) \cap G_K \cong \chi^{-1}(U_n)G_K/G_K$, which is eventually $\ker(\chi)G_K/G_K$, because $U_n \subseteq \chi(G_K)$.

Cor.(12.2.3.19). For $n$ large, if $x_i$ is a set of basis of $\mathcal{O}_{K_n}$ over $\mathcal{O}_{F_n}$, then they form a basis of $K_N$ over $F_N$ for all $N \geq n$. This is because it generate $K_N$ over $F_N$ and $[K_N : F_N] = [K_n : F_n]$.

Prop.(12.2.3.20). $p^n\nu_p(D_{K_n/F_n})$ is bounded and eventually constant. In particular $\nu_p(D_{K_n/F_n})$ converges to 0.

Proof: Cf.[Galois representation Berger P20].

Cor.(12.2.3.21). If $L/K$ is a finite extension, then $\text{tr}_{L_\infty/K_\infty}(\mathfrak{m}_{L_\infty}) = \mathfrak{m}_{K_\infty}$.
Prop. (12.2.3.23). If \( \delta > 0 \) and \( I \) is the ideal of elements of valuation \( \geq \frac{1}{p-1} - \delta \), then for \( n \) large, there is a map \( x \mapsto x^p : O_{K_{n+1}}/I \cap O_{K_{n+1}} \to O_{K_{n}}/I \cap O_{K_{n}} \), and it is surjective.

Proof: For \( n \) large, choose a uniformizer \( \pi_{n+1} \) of \( K_{n+1} \), then \( \pi_n = N_{K_{n+1}/K_{n}}(\pi_{n+1}) \) is the uniformizer of \( K_n \) because it is totally ramified (12.2.3.18), so any element \( x \in O_{K_{n+1}} \) can be written as \( \sum \pi_{n+1}^{v_i}[x_i] \), where \( x_i \in k_{K_{n+1}} = k_{K_n} \). Then \( x^p \equiv \sum \pi_{n+1}^{v_i}[x_i]^p \equiv \sum \pi_{n}^{v_i}[x_i]^p \mod I \) by the above proposition. And the surjection is verbatim.

Def. (12.2.3.24) [Tate's Normalized Trace]. The function \( R_n(x) = p^{-k} \text{tr}_{F_{n+k}/F_n}(x) \) is compatible with \( k \) and defines a \( F_n \)-linear projection from \( F_{\infty} \) to \( F_n \), and it commutes with \( G_F \) action, called the Tate's normalized trace.

From (12.2.3.25) it's easily verified that \( R_n(O_{F_{n+k}}) \subset O_{F_n} \), thus \( R_n(\pi_{n}^{i} O_{F_{n+k}}) \subset \pi_{n}^{i} O_{F_n} \). So we have \( v(R_n(x)) > v(x) - v(\pi_{n}) \). So \( R_n \) extends by continuity to a map \( R_n : F_{\infty} \to F_n \). If \( x \in F_{\infty} \), then \( R_n(x) = x \) for \( n \) large, thus \( R_n(x) \to x \) for any \( x \in F_{\infty} \).

Now for a finite extension \( K/Q_p \), for \( n \) large, \( e_j \) is a set of basis of \( O_{K_n}/O_{F_n} \), then for any \( x \in O_{K_{n+k}}, x = \sum x_i e_i^* \), where \( x_i = \text{tr}_{K_{n+k}/F_{n+k}}(x e_i) \in O_{F_{n+k}} \), as in the proof of (12.2.3.22). So we can define \( R_n(x) = \sum R_n(x_i) e_i^* \). Notice this is defined only for \( n \) large, and is independent of \( e_i \) chosen, and by the following lemma, it is continuous and extends to a \( K_n \)-linear projection \( R_n : \widehat{K}_{\infty} \to K_n \).

Lemma (12.2.3.25). Let \( k \geq 0 \) and \( n \geq 1 \), then \( R_n(\zeta_{p^{n+k}}^j) = 1 \) for \( j = 0 \) and vanishes otherwise.

Proof: This is clear from the fact \( \text{tr}_{F_{n+k}/F_n}(\zeta_{p^{n+k}}^j) = \zeta_{p^{n+k}}^j \sum \eta^{p^j} = 1 \).

Lemma (12.2.3.26). for any \( \delta > 0 \), when \( n \) is large, \( v(R_n(x)) \geq v(x) - \delta \).

Proof: We have \( v(x_i) > v(x) - v(\pi_{n+k}) \) by \( F_{n+k} \)-linearity, and \( v(R_n(x_i)) > v(x_i) - v(\pi_{n}) \) as in (12.2.3.24), and \( v(e_i^*) \geq -\delta \) when \( n \) is large, by (12.2.3.20). Thus the result.

Prop. (12.2.3.27) [Refinement of Hilbert's Theorem90]. There is a decomposition of \( \widehat{K}_{\infty} = K_n \oplus X_n \), where \( X_n = \ker R_n \). If \( \delta > 0 \), then for \( n \) large, \( \alpha \in Z_p^* \) and \( \gamma_n \) that \( \chi(\gamma_n) \) is a topological generator of \( \Gamma_{F_n} \), \( 1 - \alpha \gamma_n : X_n \to X_n \) (because \( \gamma_n \) commutes with \( R_n \)) is invertible and

\[
v_p((1 - \alpha \gamma_n)^{-1} x) \geq v_p(x) - 1/(p-1) - \delta,
\]

unless \( \alpha = -1 \) and \( p = 2 \), in which case it is only invertible on \( X_{n+1} \).
12.2. ALGEBRAIC NUMBER THEORY

Proof: As usual, \( x_i \) is a basis of \( \mathcal{O}_{K_n/F_n} \), then \( x = \sum x_i e_i \), \( x_i = \text{tr}_{K_\infty/F_\infty}(x e_i) \in \hat{F}_\infty \), and \( R_n(x) = 0 \). Then \( (1 - \alpha_\gamma_n) \) acts on \( x_i \), so it reduce to the case \( K = \mathbb{Q}_p \).

Injectivity: If \( \alpha = 1 \), this is Ax-Sen-Tate theorem. In other situations, \( (1 - \alpha_\gamma_n)(R_{n+k}(x)) = 0 \) for all \( k \geq 0 \), so \( R_{n+k}(x) = \alpha^p \gamma_n^{p^k} R_n(x) = \alpha^p R_n(x) \), so \( R_{n+k}(x) = 0 \), hence \( x = 0 \) by continuity.

Surjectivity: Let \( F_{n+k}^* = \bigoplus_{j=1,p^k} F_{n+j} \), then \( F_{n+k} = F_n^* \oplus F_{n+1}^* \oplus \cdots \oplus F_{n+k}^* \), and \( F_{n+k} \cap X_n = F_{n+1}^* \oplus \cdots \oplus F_{n+k}^* \). Now if \( x = \sum_{j=1, p^k} x_j \gamma_{j^p}^{p+n+k} \) with \( x_j \in \mathcal{O}_{F_n} \), then

\[
x = (1 - \alpha^{p^k-1} \gamma_n^{p^k-1}) \sum_{j=1, p^k} x_j \frac{\gamma_{j^p}^{p+n+k}}{1 - \alpha^{p^k-1} \gamma_{j^p}^{p^k-1}}.
\]

Now \( v_p(1 - \alpha^{p^k-1} \gamma_{j^p}^{p^k}) \leq 1/(p-1) \), and

\[
(1 - \alpha_\gamma_n)^{-1} = \frac{1 - \alpha^{p^k-1} \gamma_n^{p^k-1}}{1 - \alpha^{p^k-1} \gamma_n^{p^k-1}}(1 - \alpha^{p^k-1} \gamma_n^{p^k-1})^{-1},
\]

so \( \alpha_n : 1 - \alpha_\gamma_n : F_{n+k}^* \to F_{n+k}^* \) is invertible and

\[
v_p((1 - \alpha_\gamma_n)^{-1} x) \geq v_p(x) - 1/(p-1) - v_p(\zeta_p^n - 1)
\]

holds. And the assertion holds by uniform continuity. \( \square \)

Miscellaneous

Prop. (12.2.3.28). \( \sqrt{p} \) is contained in \( \mathbb{Q}(\zeta_p) \), in fact, \( (\sum_{i=0}^{p-1} \zeta_p^i)^2 = p \).

Proof: \( \square \)

Def. (12.2.3.29) [Lattices]. If \( K \) is a local field and \( V \) is a f.d. vector space over \( K \), then a lattice in \( V \) is

- a compact open \( \mathcal{O}_K \)-submodule of \( V \) if \( K \) is non-Archimedean.
- a discrete subgroup \( \Lambda \) of \( V \) s.t. \( V/\Lambda \) is compact if \( K \) is Archimedean.

Prop. (12.2.3.30). Let \( V \) be a f.d. vector space over a non-Archimedean local field \( K \) and \( \Lambda \) be an \( \mathcal{O}_K \)-submodule of \( V \), then \( \Lambda \) is a lattice in \( V \) iff it is a finite \( \mathcal{O}_K \)-module and generate \( V \) as a \( K \)-vector space.

Proof: If \( \Lambda \) is an \( \mathcal{O}_K \)-submodule, then it clearly generates \( V \) as a \( K \)-vector space, and the f.g. \( \mathcal{O}_K \)-submodules of \( \Lambda \) is a cover of \( \Lambda \), which has a finite subcover as \( \Lambda \) is compact open, thus \( \Lambda \) is f.g. over \( \mathcal{O}_K \).

Conversely, if \( \Lambda \) is a f.g. \( \mathcal{O}_K \)-submodule that generate \( V \) as a \( K \)-vector space, then it is a quotient of \( \mathcal{O}_K^n \) for some \( n \), thus compact. And let \( S \) be a \( K \)-basis of \( V \) contained in \( \Lambda \), then \( \mathcal{O}_K S \) is an open nbhd of \( 0 \subset \Lambda \), which means it is open. \( \square \)

Prop. (12.2.3.31). Let \( \Lambda \) be a subgroup of a f.d. real or complex vector space \( V \), then the following are equivalent:

- \( \Lambda \) is a lattice in \( V \).
• $\Lambda$ is discrete and contains an $R$-basis of $V$.

• $\Lambda$ has a $Z$-basis that is also an $R$-basis of $V$.

**Remark (12.2.3.32).** WARNING: This is not equivalent to $\Lambda$ is a f.g. $Z$-module and generated $V$ as an $R$-vector space: Consider $\text{span}(1, \alpha) \subset R$.

**Proof:** 1 $\rightarrow$ 2: Let $W$ be a complementary subspace of $\Lambda \otimes Z R \subset V$, then $W \cong W$ is closed thus compact in $V/\Lambda$, which implies $W = 0$.

2 $\rightarrow$ 3: We may assume $V = R^n$ and $\Lambda$ contains the canonical basis $e_1, \ldots, e_n$, then $\Lambda$ is generated by $S = \{ \lambda \in \Lambda | \max |\lambda_i| \leq 1 \}$. Because $\Lambda$ is discrete thus closed in $V$, $S$ is finite. Thus $\Lambda$ is a f.g. $Z$-module, and has no torsion, thus a free Abelian group. But $\Lambda/\mathbb{Z}\{e_i\}$ is finite, thus $\Lambda \cong \mathbb{Z}^n$. Hence a basis of $\Lambda$ must also be a basis of $V$.

3 $\rightarrow$ 1 is clear. □

**Def. (12.2.3.33) [Dual Lattice].** If $K$ is a non-Archimedean local field and $V$ is a f.d. vector space over $K$, $B$ is a non-degenerate bilinear form on $V$ and $\psi$ is a non-trivial character of $K$, then for any lattice $L \subset V$, the dual lattice $L' = \{ u \in V | \psi(2(B(u,v))) = 1, \forall v \in L \}$ is also a lattice in $V$.

**Proof:** It is an open group by no-small-subgroup argument, as $\psi, B$ are continuous. it is compact because take any basis $\{v_1, \ldots, v_n\}$ of $V$ that $v_i \in L$, $\{u \in V | \psi(2(B(u,v_i))) = 1, \forall i \}$ is compact. □

4 Global Fields

**Def. (12.2.4.1) [Global Fields].** A global field is a finite extension of $Q$ or $F_p((t))$, without a valuation. The former is called a number field and the latter a function field.

**Def. (12.2.4.2) [Ring of Integers], $Z \subset Q$ and $F_p[t] \subset F_p((t))$ are PIDs, thus Dedekind domains, thus for a global field $F(12.2.4.1)$, we can define the ring of integers $O_F$ of $F$ to be the integral closure of $Z$ or $F_p[t]$ in $F$, which is an Dedekind domain, by(4.2.7.12).

**Remark (12.2.4.3).** The theory of Dedekind domains7 applies to the ring of integers.

**Def. (12.2.4.4) [Roots of Unity],** For a global field $F$, let $\mu(F)$ be the set of roots of unity in $F$, which is a finite group.

**Def. (12.2.4.5) [Places].** For a field $F$,

- $\Sigma_F^{\text{fin}}$ is the equivalent classes of (non-Archimedean)valuations of $F$, called the finite places of $F$.

- $\Sigma_F^{\infty}$ is the equivalent classes of (Archimedean valuations) $| \cdot |_v = -\log |\tau(\cdot)|$ of $F$ corresponding to embeddings $\tau : K \rightarrow C(10.3.3.16)$, called the infinite places of $F$.

- $\Sigma_F^R$ is the set of infinite places $v$ of $F$ corresponding to embeddings $F \rightarrow R$, called the set of real places of $F$. Denote $r_1 = \# \Sigma_F^R$ if it is finite.

- $\Sigma_F^C$ is the set of infinite places $v$ of $F$ that is non-real, called the set of complex places of $F$. Notice two embeddings corresponds to the same place iff they are conjugate. Denote $r_2 = \# \Sigma_F^C$ if it is finite.

- For a maximal ideal $p \subset O_F$, $v_p$ is the valuation of $F$ corresponding to $F$. Most of the time we will not distinguish between a maximal prime $p$ and its corresponding valuation.

- For a finite extension $L/F$ and $v \in \Sigma_F^{\text{fin}}$, $\Sigma_L^v$ is the set of finite places over $L$ over $v_p$. 
For $v \in \Sigma_F$, denote $F_v$ the completion of $F$ w.r.t. $v$.

Def.(12.2.4.6) [Constant Fields].

Prop.(12.2.4.7) [Valuations]. Let $F$ be a global field, for any $v \in \Sigma_F$, let $p \in \mathcal{P} \cup \{\infty\}$ s.t. $v|p$, then define the inertia degree

$$f_v = \begin{cases} \left[ \kappa(v) : \kappa(p) \right], & v \in \Sigma^\text{fin}_F, \\ \left[ F_v : F_p \right], & v \in \Sigma^\infty_F. \end{cases}$$

$\|v\| = \|v\|^{-v(a)}$

This is compatible with the definition in (4.2.7.17) when $v \in \Sigma^\text{fin}_F$.

Prop.(12.2.4.8) [Product Formula]. Let $F$ be a global field and $a \in F^\times$, then $|a|_w = 1$ for a.e. $w \in \Sigma_F$, and

$$\prod_{w \in \Sigma_F} |a|_w = 1.$$

Proof: Let $F_0 = \mathbb{Q}$ or $\mathbb{F}_p(t)$ be the base field of $F$, then the assertion is easy to verify for $F_0$, and

$$\prod_{w \in \Sigma_F} |a|_w = \prod_{v \in F_0} \prod_{w|v} |a|_w = \prod_{v \in F_0} |\text{Nm}_{F/F_0}(a)|_v = 1.$$

□

Prop.(12.2.4.9) [Artin-Whaples]. Let $F$ be a field and $\Sigma_F$ the set of places of $F$, then $F$ is a global field iff

- There exists representatives $|\cdot|_v$ for $v \in \Sigma_F$ s.t. the product formula $\prod_{v \in \Sigma_F} |a|_v = 1$ for any $a \in F^\times$.
- For any $v \in \Sigma_F$, $F_v$ is a local field (12.2.3.1).

Proof: □

Prop.(12.2.4.10) [Global and Local]. Let $F$ be a global field, $v \in \Sigma_F$, then for any extension $L^w/F_v$, there exists a global field $L/F$ s.t. $L^w = LF_v$, and $[L : F] = [L^w : F_v]$.

Proof: Cf. [Sutherland, L11]. □

Def.(12.2.4.11) [Algebraic Integers]. An element $\alpha \in \mathbb{Q}$ is called an algebraic integer if it satisfies a monic polynomial equation $p(X) \in \mathbb{Z}[T]$. Then the set of algebraic integers equals

$$\bigcup_{F \subseteq \mathbb{C}} \mathcal{O}_F.$$

where the sum is taken over all number fields $F$.

Orders

Cyclotomic Fields

Prop.(12.2.4.12). $\text{Gal}(\mathbb{Q}[\mu_n]/\mathbb{Q}) \cong (\mathbb{Z}/(n))^\times$. 

Proof: We choose a prime $p$ prime to $n$ and show that $\mu_n^p$ is conjugate to $\mu_n$.

Let $X^n - 1 = f(X)h(X)$ with $f(X)$ minimal polynomial of $\mu_n$. If $f(\mu_n^p) \neq 0$, then $h(\mu_n^p) = 0$, thus $h(X^p) = f(X)g(X)$. So module $p$, $X^n - 1$ has a multi root, which is impossible. \hfill $\square$

Proposition (12.2.4.13). The ring of integers in a cyclotomic field is generated by the roots of identity.

Proof: First consider the case $n$ a prime power. Because $d(1, \zeta, \cdots, \zeta^{d-1}) = \pm t^s$, $\nu \mathcal{O} \subset \mathbb{Z}[\zeta] \subset \mathcal{O}$. Because $p$ totally splits, $\mathcal{O} = \mathbb{Z}[\zeta] + \pi \mathcal{O}$, thus $\mathcal{O} = \mathbb{Z}[\zeta] + \pi^t \mathcal{O}$. Choose $t = s \phi(n)$ yields $\mathbb{Z}[\zeta] = \mathcal{O}$.

Then for different $p$, the fields are disjoint and the discriminant are pairwisely coprime, thus by (2.11) in Neukirsch, the products of the integral basis form an integral basis. \hfill $\square$

Proposition (12.2.4.14) [Ring of Integers]. Let $n$ be an integer with no repeated primes, then

- If $n \equiv 3 \mod 4$, the ring of integers in $\mathbb{Q}(\sqrt{n})$ is $\mathbb{Z} [\sqrt{n}]$.
- If $n \equiv 1 \mod 4$, the ring of integers in $\mathbb{Q}(\sqrt{n})$ is $\mathbb{Z} [\sqrt{\frac{1+\sqrt{n}}{2}}]$.

Proof: 1: the minimal polynomial of $\sqrt{n}$ is $X^2 - n$, whose different is $4n$, which doesn’t have a proper divisor $\beta$ that $4n/\beta$ is a square and $\beta \equiv 0, 1 \mod 4$, so $\mathbb{Z} [\sqrt{n}]$ is the ring of integers.

2: the minimal polynomial of $\sqrt{\frac{1+\sqrt{n}}{2}}$ is $X^2 - X + \frac{1-n}{4}$, whose different is $n$, which doesn’t have a proper divisor $\beta$ that $4n/\beta$ is a square, so $\mathbb{Z} [\sqrt{\frac{1+\sqrt{n}}{2}}]$ is the ring of integers. \hfill $\square$

Proposition (12.2.4.15). $p \in \mathcal{P}$ splits in $\mathbb{Z} [\zeta_n]$ iff $p \equiv 1 \mod n$.

Proof: First, if it splits, then $f = 1$. Because the ring of integers is $\mathbb{Z} [\zeta_n]$, so $X^n - 1$ splits in $\mathbb{F}_p(12.2.4.13)$, thus $p \equiv 1 \mod n$. And if $p \equiv 1 \mod n$, it is unramified and $X^n - 1$ splits in $\mathbb{F}_p$, so $f = 1$. \hfill $\square$

Definition (12.2.4.16).

- $\mathbb{Z}[i]$ is called the ring of Gaussian integers.
- $\mathbb{Z} [\sqrt{-1/2}]$ is called the ring of Eisenstein integers.
- $\mathbb{Z} [\sqrt{1+\sqrt{-1/2}}]$ is called the ring of Kleinian integers.

These are all PIDs.

Minkowski Theory

Definition (12.2.4.17) [Global Lattices]. If $F \in \mathcal{G}Field$ and $V \in \mathcal{V}ect/F$, then an $(F)$-lattice in $V$ is a f.g. $\mathcal{O}_F$-module $\Lambda$ s.t. that generates $V$ as a $F$-vector space.

Proposition (12.2.4.18) [Local to Global Compatibility]. Let $F$ be a global field, then

- If $\Lambda$ is a $F$-lattice in $K^n$, then for any place $v \in \Sigma_F$, its completion in $F_v$ is a lattice in $V_v$, and for a.e. place $v$, $\Lambda_v = \mathcal{O}_{F,v}^n$.
- Conversely, if for any non-Archimedean place $v$, $\Lambda_v$ is a $F_v$-lattice in $F_v^n$, and $\Lambda_v = \mathcal{O}_{F,v}^n$ for a.e. $v$, then there is a unique $F$-lattice $\Lambda \in F^n$ s.t. $\Lambda_v$ is the closure of $\Lambda$ in $F_v$. In fact, $\Lambda = \cap_{v \in M_F} (F^n \cap \Lambda_v)$.

Proof: Cf. [B-G06]P609. \hfill $\square$
Prop. (12.2.4.19) [Minkowski]. Let \( a \neq 0 \) be an integral ideal of \( F \) and for each \( \tau \in \text{Hom}(F, \mathbb{C}) \) are given a real number \( c_\tau > 0 \) s.t. \( c_\tau = c_\tau \) and

\[
\prod_\tau c_\tau > \left( \frac{2}{\pi} \right)^{3/2} |d_K|^{1/2} (\mathcal{O}_K : a),
\]

then there exists \( a \in \alpha^x \) s.t. for any \( \tau \in \Sigma_F^\infty \),

\[ |\tau(a)| < c_\tau \]


Cor. (12.2.4.20). Let \( a \neq 0 \) be an integral ideal of \( K \), then there exists an \( a \in \alpha^x \) s.t.

\[
|\tau(a)| < \left( \frac{2}{\pi} \right)^{s/n} |d_K|^{1/2n} (\mathcal{O}_K : a)^{1/n}
\]

for any \( \tau \in \text{Hom}(K, \mathbb{C}) \).

Thm. (12.2.4.21) [Bounded Ramifications are Rare]. Let \( F \) be a number field and \( \Sigma_F^\infty \subset S \subset \Sigma_F \), \( \#S < \infty \), then there are only f.m. field extensions \( L/F \) of a given degree \( n \) that are unramified outside \( S \).

Proof: The power of a prime \( \mathfrak{B} \) in the discriminant is controlled by \( n \) by (4.2.7.31). Together with (4.2.7.33), thus shows the power of \( p \) in the discriminant of the extension is controlled by \( n \), independent of the field. Also we can assume \( \sqrt{-1} \in F \), because it changes the discriminant by a bounded factor, by (4.2.7.34). So it suffices to prove there are only f.m. field extension with fixed degree and discriminant. By (4.2.7.34), we can assume \( K = \mathbb{Q} \).

For the rest, we use Minkowski’s theorem, Cf. [Neukirch, P203]?

Prop. (12.2.4.22) [Lower Bounds for Discriminant]. The discriminant of a number field \( K \) of degree \( n \) satisfies

\[
|d_K|^{1/2} \geq \frac{n^n}{n!} \left( \frac{\pi}{4} \right)^{n/2}.
\]

Proof: Cf. [Neukirch, P204].

Cor. (12.2.4.23) [Hermit’s Theorem]. There are only f.m. number fields with a given discriminant.

Proof: (12.2.4.22) shows the degree is controlled by the discriminant, thus the theorem follows from (12.2.4.21).

Cor. (12.2.4.24) [Minkowski’s Theorem]. The discriminant of a number field \( K \neq \mathbb{Q} \) is not \( \pm 1 \).

Cor. (12.2.4.25). \( \mathbb{Q} \) doesn’t have any unramified extensions, by (4.2.7.35).

5 Adele and Idele

Notations (12.2.5.1).

- Let \( F \) be a global field.
**Restricted Direct Product**

**Def. (12.2.5.2) [Restricted Direct Product].** Let \( \{p\} \) be a set of indices and given a family of locally compact Abelian groups \( G_p \), and for a.e. \( p \) an open compact subgroup \( H_p \subset G_p \). Then the **restricted direct product** is defined to be

\[
G = \prod' (G_p, H_p) = \lim_{S \in \{p\}, |S| < \infty} \prod_{p \in S} G_p \times \prod_{p \notin S} H_p
\]

given the colimit space topology. And we denote \( \prod_{p \in S} G_p \times \prod_{p \notin S} H_p = G_S, \prod_{p \notin S} H_p = G^S \).

This topology is stronger than the product topology of \( \prod_p G_p \). It has an open basis \( N = \prod_p N_p \), where \( N_p \) is open in \( G_p \) and \( N_p = H_p \) for a.e. \( p \). It is locally compact because every \( G_S \) does.

**Prop. (12.2.5.3).** Every compact subset \( N \) of \( G \) is contained in a \( \prod_p N_p \), where \( N_p \) is compact and \( N_p = H_p \) for a.e. \( p \).

**Proof:** This is because \( G_S \) is an open covering of \( G \), and the union of f.m. \( G_S \) is also of the form \( G_S \). So \( N \) is contained in some \( G_S \), thus its projection in the \( S \)-coordinates is compact. \( \square \)

**Prop. (12.2.5.4) [Quasi-Characters on \( G \)].** Quasi-characters on \( G \) are all of the form \( \otimes_p c_p \) that \( c_p \) is trivial on \( H_p \) for a.e. \( p \).

**Proof:** Let \( c \) be a quasi-character, choose a nbhd of \( 1 \in U \subset C \) that contains no subgroup, then \( c^{-1}(U) \) has contains an open basis \( \prod_{p \in S} N_p \times G^S \), where \( N_p \) are open nbhds of 1, so \( c(G^S) = 1 \). Thus \( c(a) = \prod_p c_p(a_p) \) is true for any \( a \in G \).

Conversely, clearly \( \otimes_p c_p \) is a quasi-character on \( G \), it is continuous. \( \square \)

**Prop. (12.2.5.5) [Dual of \( G \)].** In each \( \widehat{G}_p \), by (10.9.3.7) \( H_p \) are compact, so \( \overline{H_p} = \widehat{G}_p/H_p \) are discrete, so \( H_p^\perp \) is open; \( H_p \) are open, so \( H_p^\perp = \widehat{G}_p/H_p \) are compact. So we can define the space \( \prod'(\widehat{G}_p, H_p^\perp) \).

Then the dual group \( \widehat{G} \cong \prod'(\widehat{G}_p, H_p^\perp) \) as a topological group.

**Proof:** (12.2.5.4) shows that this is an algebraic isomorphism, so it suffices to prove this is a topological homeomorphism (10.9.3.6):

For any compact \( B \subset G_1 = \prod_{p \in S} N_p \times \prod_{p \notin S} H_p \), for any \( \varepsilon > 0 \), if \( c \in \prod_{p \in S} N'_p \times \prod_{p \notin S} H_p^\perp \), where \( N'_p = \{c_p|c_p(N_p - 1)| < \varepsilon \}<|S|\), then \( |c(B) - 1| < \varepsilon \).

Conversely, if \( \varepsilon \) is small enough, then if \( c(\prod_{p \in S} N_p \times \prod_{p \notin S} H_p) - 1| < \varepsilon \), then \( c \in \prod_{p \in S} N'_p \times \prod_{p \notin S} H_p^\perp \), where \( N'_p = \{c_p|c_p(N_p - 1)| < \varepsilon \}\) \( \square \)

**Prop. (12.2.5.6) [Restricted Product Measure].** Let measures \( d\alpha_p \) be given on \( G_p \) that \( \alpha_p(H_p) = 1 \) for a.e. \( p \), define a Haar measure on \( G \) as follows:

On \( G_S \), \( d\alpha_S = \prod_{p \in S} d\alpha_p \cdot d\alpha^S \), where \( \alpha^S \) is the product measure on \( G^S \).

Then these can define a functional a positive left-invariant functional \( I \) that \( |I(f)| \leq \|f\| \) for any \( f \) that depends only on f.m. coordinates \( p \in S \). Then Stone-Weierstrass theorem shows these functions are dense in \( C(G) \), thus \( I \) can be uniquely extended to a functional on \( C(G) \), and this defines a Haar measure on \( G \) by Riesz representation (10.9.1.10), denoted by \( d\alpha = \prod_p d\alpha_p \), called the **restricted product measure**.

**Prop. (12.2.5.7).** For a function \( f \) on \( G = \prod'(G_p, H_p) \) measurable, if either \( f \geq 0 \) or \( f \in L^1(G) \), then

\[
\int_G f(a) d\alpha = \lim_{S \uparrow} \int_{G_S} f(a) d\alpha
\]
as a net limit.
Proof: The second case follows from the first case, as \( \int_G f = \lim_{B \to \text{compact}} \int_B f \) by monotone convergence theorem, and any \( B \) compact is contained in some \( G_S(12.2.5.3) \).

**Cor. (12.2.5.8).** If \( f(a) = \prod_p f_p(a_p) \), where \( f_p \in L_1(G_p) \) and \( f_p = \chi_{H_p} \) a.e. \( p \), then if

\[
\prod_p \int_{G_p} |f_p(a_p)|da_p < \infty,
\]

then \( f \in L^1(G) \), and

\[
\int_G f(a)da = \prod_p (\int f_p a_p da_p).
\]

**Def. (12.2.5.9) [Dual Measure].** Notice if \( f_p = \chi_{H_p} \), then

\[
\hat{f}_p(c_p) = \int_{H_p} \frac{c_p(a_p)}{a_p}da_p = da_p(H_p)\chi_{H_p}(c_p).
\]

So by Fourier transform\( (10.9.3.24) \), if \( dc_p \) is the dual measure on \( \hat{G}_p \), then \( \chi_{H_p} = dc_p(H_p)da_p(H)\chi_{H_p} \), which means \( dc_p(H_p) = 1, a.e.p \), thus we can define a measure on \( G \) as \( dc = \prod\hat{dc}_p \).

Then \( dc \) is the measure on \( \hat{G} \) dual to \( da \) on \( G \).

**Proof:** The duality is by the lemma below\( (12.2.5.10) \), applied to both \( f \) and \( \hat{f} \).

**Lemma (12.2.5.10) [Fourier Transform on Product],** if \( f_p \in B_1(G_p) \) and \( f_p = \chi_{H_p} \) a.e. \( p \), then \( f(a) = \prod f_p(a_p) \in B_1(G) \), and \( \hat{f}(c) = \prod \hat{f}_p(c_p) \).

**Proof:** For any character \( c \), because

\[
f(a)c(a) = \prod f_p(a_p)c_p(a_p)
\]

and every \( f_p(a_p)c_p(a_p) \in L^1(G_p) \). So\( (12.2.5.8) \) applies and shows the equations. Similarly, because \( \hat{f}_p = \chi_{H_p} \) a.e. \( p \), we have \( \hat{f} \in L_1(\hat{G}) \), so \( f(a) \in B_1(G) \).

Adele and Idele

**Notations (12.2.5.11) [Adeles].** For \( S \in \Sigma_F, \#S < \infty \),

- The **adele group** (adele=additive element) of \( F \) is defined to be \( A_F = \prod_{v \in S}(F_v, \mathcal{O}_v)(12.2.5.2) \).
- \( A_S = \bigoplus_{v \in S} F_v \).
- \( A^S = \prod_{v \notin S}(F_v, \mathcal{O}_v) \), called the group of \( S \)-**adeles** of \( F \).
- The **finite adeles** \( A^f_F = A^S_F = \prod_{v \notin S}(F_v, \mathcal{O}_v) \).
- The **infinite adeles** \( A_F, \infty = A_{F,S,\infty} = \prod_{v \in S}(F_v, \mathcal{O}_v) \).
- For \( v \in \Sigma_F, x \in F_v \), let \( [x]_p^{\mathbb{Z}} \) be the image of \( x \) under the map \( F_p \to A_F \).

**Notations (12.2.5.12) [Ideles].** For \( S \in \Sigma_F, \#S < \infty \),

- The **ideal group** (idele=ideal element) of \( F \) is defined to be \( I_F = \prod_{v}(F_v^*, \mathcal{O}_v^*)(12.2.5.2) \), which is set-theoretically \( A_F^\times \). Notice the topology on \( I_K \) is different with the subspace topology from \( A_K \).
• The ideal class group $C_F = I_F/F^\times$.
• $I_F$ is naturally a valuation ring with valuation $|\cdot|$, called the **idele norm**.
• $I^0_F \subset I_F$ is the subgroup consisting of elements of idele norm 1, called the set of **unit ideles**.
• $I^S_F = \prod_{p \in S} F_p^\times \times \prod_{\mathfrak{p} \not\in S} O_{F_{\mathfrak{p}}, \mathfrak{p}}$, called the group of **S-ideles** of $F$.
• $I_{F,S} = \prod_{v \in S} F_v^\times$.
• $F^S = F^\times \cap I^S_F$ is the set of S-units of $F$ (4.2.7.10).
• The **finite ideles** $I^f_F = A^{S,\infty}_F = \prod_{v \not\in S_\infty} (F_v^*, O_v^*)$.
• The **infinite ideles** $I^{\infty}_F = F_{F, S_\infty} = \prod_{v \in S_\infty} F_v^\times$.
• For $v \in \Sigma_F$, $x \in F_v^\times$, let $[x]_v^\times$ be the image of $x$ under the map $F_v^\times \to I_F$.

**Def. (12.2.5.13)** [Hecke Character].  A Hecke character on $F$ is a character of $C_F$.

**Def. (12.2.5.14)** [Unramified Places]. Let $\chi$ be a Hecke character of $C_K$, then for a.e. $v \in \Sigma_F^{\text{fin}}$, the conductor of $\chi_v$ is $O_v^\times$. For these $v$, $\chi$ is said to be **unramified** at $v$.

**Prop. (12.2.5.15)** [Extension of Adeles]. If $L/F$ is a separable extension of global fields then

$$A_F \otimes_F L \cong A_L$$

by diagonal embedding.

**Proof:** $A_K \otimes_F L \cong \prod'_v (F_v, O_v \otimes_{O_F} O_L)$, because for any element $x \in L$, $|\text{Nm}_{L/F}(x)|_v \neq 0$ for only f.m. $v$. And there are isomorphisms by diagonal maps.

$$F_v \otimes_F L \cong \prod_{w|v} L_w, \quad O_v \otimes_{O_F} O_L \cong \prod_{w|v} O_w.$$  \hfill $\square$

**Prop. (12.2.5.16)** [Product Formula]. If $a \in I_F$ is an idele and $a \in F^\times$, then $|a|_F = 1$.

**Proof:** Consider the restricted product measure $d\mu$ on $A_F$, then clearly $d\mu(ax) = |a|d\mu(x)$, and multiplying by $a$ induces an isomorphism of $A_F$, but preserves the counting measure on $F$. But $A_F$ is compact(12.2.5.19) thus has finite volume, so $|a| = 1$. \hfill $\square$

**Prop. (12.2.5.17)**. If $F$ is a field, the norm group $|I_F|$ of the Adelic norm is $|I_F| = q^Z$, where $q = \#F_0$ and $F_0$ is the maximal finite field contained in $F$.

**Proof:** This is because in this case, $F$ corresponds to smooth curve over $F_0$. Then by Weil conjecture(16.1.1.3), there exists a point of $F_0$ with residue order $q^n$ for any $n$ large. Then their quotient gives $q$. \hfill $\square$

**Prop. (12.2.5.18)** [Splitting of $I_F$].

- If $F$ is a number field, take $v \in \Sigma_F^\infty$, then the exact sequence $1 \to I^1_F \to I_F \xrightarrow{\nu} \mathbb{R}_+ \to 1$ splits, so there are non-canonical isomorphisms

$$I_F \cong I^1_F \times \mathbb{R}_+, \quad I_F/F^\times \cong I^1_F/F^\times \times \mathbb{R}_+.$$
• If $F$ is a global function field, take $v \in \Sigma_F$, then for some $q = (\text{char } k)^r$, the exact sequence $1 \rightarrow I_k^1 \rightarrow I_F \xrightarrow{\phi} q^\mathbb{Z} \rightarrow 1$ splits, so there are non-canonical isomorphisms

$$I_F \cong I_k^1 \times q^\mathbb{Z}, \quad I_F/F^\times \cong I_k^1/F^\times \times q^\mathbb{Z}.$$ 

Proposition (12.2.5.19) [K Cocompact in Adele]. $F$ is discrete in $A_F$ and $A_F/F$ is compact.

Proof: Let $\infty$ be any prime, consider $U = \{a \in A_F||a|_\infty < 1, |a|_v \leq 1\}$, then $U \cap K = 0$ by (12.2.5.16).

Now we show $A_F/F$ is compact. By (12.2.5.15), it suffices to show for $F = \mathbb{Q}$ or $F_p(t)$. Let $U_\infty = \{x \in F_\infty||x|_\infty \leq 1\}$, and Cf.[MIT notes, 22.12].

Proposition (12.2.5.20). $I_K$ is locally compact in the restricted product topology, and $F^\times$ is a discrete subgroup of $I_K$, thus $C_K$ is also Hausdorff locally compact.

Proof: $F^\times$ is discrete in $I_F$ because it is already discrete in $A_F(12.2.5.19)$.

Lemma (12.2.5.21). $I_k^1$ is closed in $A_F$, and the subspace topologies from $A_F$ and $I_F$ are the same on $I_k^1$.

Proof: 

Lemma (12.2.5.22) [Blichfeldt-Minkowski]. Let $F$ be a global field, then there exists $C > 0$ s.t. for any $x \in I_F$ s.t. $|x|_F \geq C$, let

$$W(x) = \{y \in I_F||y|_v \leq |x|_v, \forall v \in \Sigma_F\}.$$ 

Then $W(x) \cap F^\times \neq \emptyset$.

Proof: 

Lemma (12.2.5.23) [Strong Approximation for $G_a$]. Let $v \in \Sigma_F$, then the image of $F$ is dense in $A_F^{(v)}$, or equivalently, $FF_vU = A$ for any open subset $U \subset A^S$.

Remark (12.2.5.24). Cf.(13.3.3.9) for more general strong approximation theorems.

Proof: Cf.[MIT notes, 22.14].

Proposition (12.2.5.25) [$F^\times$ Cocompact in $I_k^1$]. $F^\times$ is discrete in $I_F$, and $I_k^1/F^\times$ is compact.

Proof: $F^\times$ is discrete in $I_F$ because it is already discrete in $A_F(12.2.5.19)$. By (12.2.5.21), use Minkowski (12.2.5.22), it suffices to show that for $|x|_F \geq C$, $W(x) \cap I_k^1 \rightarrow I_k^1/F^\times$ is surjective: If $y \in I_k^1$, then $|x/y|_F = |x|_F \geq C$, thus there exists $z \in K^\times \cap W(x/y)$, thus $zy \in W(x)$, and $y$ is in the image of $W(x) \cap I_k^1$.

Proposition (12.2.5.26). For a field extension $L/K$, $I_K \subset I_L$, and $I_L^G = I_K$, this is be the diagonal inclusion to all the primes above a given prime, and the action is by $(\sigma)_\mathfrak{q} = \sigma_{\mathfrak{q}-1}\mathfrak{q}$. This induces an inclusion $C_K \subset C_L$ and $C_L^G = C_K$. The last assertion uses long exact sequence and $H^1(G, L^\times) = 0$.

Lemma (12.2.5.27). The map $I_F \rightarrow A_F \times A_F : x \mapsto (x, x^{-1})$ is a homeomorphism of $I_F$ onto a closed subspace of $A_F \times A_F$. 

Prop. (12.2.5.28) [Idele Groups and Extensions]. For an extension of global fields $L/F$,
- the diagonal embedding $A_F \to A_L$ induces a closed embedding, and also a closed embedding $I_F \to I_L$ by (12.2.5.27), thus also a closed embedding $I_F/F^\times \to I_L/L^\times$.
- $A_F$ is a finite $A_K$-module, thus there is a norm map $\text{Nm}_{L/K} : A_L \to A_F$, which restricts to $\text{Nm}_{L/K} : I_L \to I_F$, which is compatible with $\text{Nm}_{L/K} : L^\times \to K^\times$, thus inducing a map $\text{Nm}_{L/K} : \mathcal{C}_L \to C_F$. Then this map is continuous, open, and proper.
- $\{n\} : C_F \to C_F$ is continuous and proper.

**Proof:**
- 2: It is continuous because it is compatible with the local norms $\text{Nm}_{L_p/F_p}$, and $\text{Nm}_{L_p/F_p}(\mathcal{O}_{F,p}^\times) = \mathcal{O}_{L,p}^\times$. To show it is open, use the fact the local norms are open and for unramified places $\text{Nm}_{L_p/F_p} \mathcal{O}_{L_p} = \mathcal{O}_{F,p}(12.2.3.13)(12.4.2.4)$. To show it is proper, use the splitting $C_F \cong I_F/F^\times \times \mathbb{Z}$ (12.2.5.18) and the fact $I_F/F^\times$ is proper (12.2.5.25).
- 3: Use the splitting (12.2.5.18).

Def. (12.2.5.29) [Norm Groups]. For an extension of global fields $L/F$, let $\mathcal{N}_{L/F} = \text{Nm}_{L/F} C_L$, called the norm group of $L/F$.

Prop. (12.2.5.30) [Connected Component of identity of $C_F$]. If $F$ is a number field, let $I_{F,\infty}^0 \cong \mathbb{R}_+^n \times (C^\times)^r$ be the connected component of identity of $I_{F,\infty}$, $D_F \subset C_F$ the closure of $I_{F,\infty}^0 \subset C_F$.
- $D_F$ is the connected component of identity of $C_F$.
- $D_F = \cap_{n \in \mathbb{Z}_+} C_F^n$ is the group of divisible elements of $C_F$.
- $C_F/D_F$ is a profinite group. (which will be isomorphic to $\text{Gal}_{F}^{ab}$, as we will see in (12.4.3.25)).

**Proof:** $I_{F,\infty}^0$ is divisible, thus so does its image in $C_F$. Then $D_F$ is also divisible as $\{n\} : C_F \to C_F$ is continuous and proper (12.2.5.28).

Consider the map $\prod_{v \in \Sigma_F} \mathcal{O}_{F,v}^\times \to C_F/D_F$, its cokernel is finite because $C_F/\prod_{v \in \Sigma_F} I_{F,v,\infty} \cong \text{Cl}(\mathcal{O}_F)$ is finite and $I_{F,\infty}^0$ is finite. But $\prod_{v \in \Sigma_F} \mathcal{O}_{F,v}^\times$ is a profinite group, thus $C_F/D_F$ is also a profinite group.
- To show $D_F = C_F^0$, firstly $C_F^0 \subset D_F$ by the fact $C_F/D_F$ is connected thus totally disconnected, and the reverse is true because $D_F$ is connected.
- To show $D_F = \cap_{n \in \mathbb{Z}_+} C_F^n$, notice any divisible element is in $D_F$ as a profinite group $C_F/D_F$ doesn’t contain non-trivial divisible elements.

Thm. (12.2.5.31) [Class Numbers and Unit Theorems]. For any $\Sigma_F^\infty \subset S \subset \Sigma_F$,
- The $S$-unit group $\text{Cl}(\mathcal{O}_{F,S}) \cong I_F/F^\times I_F^S$ is finite. In particular, $I_Q = \mathbb{Q}^\times \times \mathbb{R}_+^\times \times \prod_{p \in \mathcal{P}} \mathbb{Z}_p^\times$.
- The $S$-unit group (4.2.7.10) $F^S \cong \mathbb{Z}^{\# S - 1}$.
- For any $x \in F$, if $|x|_v = 1$ for any $v \in \Sigma_F$, then $x \in \mu(F)$.

**Proof:**
- 1: Let $(I_F^S)^1 = I_F \cap I_F^S$. As $\mathcal{O}_{F,S}^\times = F^\times \cap I_F^S$, there is an exact sequence
  
  $1 \to (I_F^S)^1/F^S \cong F^\times (I_F^S)^1/F^\times \to I_F^1/F^\times \to (I_F^S)^1/F^\times (I_F^S)^1 \to 1$.

The first term is an open subset, and $I_F^1/F^\times$ is compact by (12.2.5.25), thus $(I_F^S)^1/F^\times (I_F^S)^1$ is finite and $(I_F^S)^1/F^S$ is compact. There is also an exact sequence
  
  $1 \to (I_F^S)^1/F^\times (I_F^S)^1 \to I_F^S/F^\times I_F^S \cong \text{Cl}(\mathcal{O}_{F,S}) \to ||I_F||_{F/||I_F^S||_F} \to 1$.
and $||I_F||_F/||I_F^S||_F$ is always finite, so $\# \Cl(O_{F,S}) < \infty$.

2, 3: Consider the regulator map

$$\text{Reg} : \prod_{v \in S} F_v^\times \to \mathbb{R}^\# S : (x_v) \mapsto (-\log |x_v|_v).$$

Then this map restricted to $F_S$ has image a discrete subset of the hyperplane $H = \{\sum x_i = 0\}$. In fact the image is a full lattice in $H$: let $n_1$ be the number of infinite places in $S$ and $n_2$ the number of finite places in $S$, then $\text{Reg}((\prod_{v \in S} F_v^\times)^1) \cong \mathbb{R}^{n_1-1} \times \mathbb{Z}^{n_2}$ if $n_1 > 0$ and $\mathbb{Z}^\# S - 1$ if $n_1 = 0$. Then notice $(\prod_{v \in S} F_v^\times)^1/F_S$ is finite, which is true as $(I_F^S)^1/F_S$ is compact, so The image of $F_S$ is a full lattice of $H$.

Also notice if $x$ is in the kernel, then $|x|_v = 1$ for any $v \in \Sigma_F$, so $\{x^n | n \in \mathbb{Z}\}$ is a bounded subset in the lattice $\prod_{v \in S} F_v^\times$, but it is also contained in the discrete subset $F_S$, thus it is a finite subset, so $x$ is a root of unity.

**Cor. (12.2.5.32)** If $S \subset \Sigma_F$ is sufficiently large, then $I_F = I_F^S \cdot F^\times$ hence $C_F = I_F^S \cdot F^\times/F^\times$.

**Proof:** The ideal class group is finite, hence we can find a finite set of representatives for it. Only finite set of primes are involved in it, thus we let $S$ contain all these primes and infinite primes, then for any $a$, $\prod_{p | \infty} a_p = A_i \cdot (x)$, and $A_i \in I_F^S$, hence $a \in I_F^S \cdot K^\times$. □

**Cor. (12.2.5.33)** [Dirichlet Characters and Hecke Characters for $\mathbb{Q}$]. Hecke characters of $\mathbb{Q}$ are exactly of the form $\chi(x) = \chi_0(x)|x|^\lambda$ for some $\lambda \in i\mathbb{R}$, $\chi_1$ a Hecke character of finite order corresponding to a primitive Dirichlet character $\chi_0$ via (12.2.5.31).

To transit between these two, we need to use $\mathbb{Q}^\times$ to “clear the denominators”. For example, for $p$ prime to the conductor of $\chi_0$, $\chi_1(p_v) = \chi_0(p)$.

**Prop. (12.2.5.34)** Let $p \in \frak{P}, F \in p\text{-Field}$, and $\ell \in \frak{P} \backslash p, E \in \ell\text{-Field}$, then any continuous homomorphism $\chi : C_F \to O_E^\times$ that is unramified outside a finite set of places is of the form $\chi = \chi_1 \cdot c^{\deg(\cdot)}$, where $\chi_1 : C_F \to O_E^\times$ is of finite order and $c \in O_E^\times$.

**Proof:** Let $\sigma \in O_F^{ab}$ s.t. $\deg(\sigma) = 1$, let $c = \chi(\sigma)$, and $\chi_1 = \chi \cdot c^{-\deg(\cdot)}$, then $\chi_1(C_F) = \chi_1(I_F)$. But as $\# \Cl(F) < \infty$, by (12.4.5.7), it suffices to show that $\chi_1(F^\times U^1/F^\times)$ is finite. Then it suffices to show that $\# \chi(U^1) < \infty$. But if $\chi$ is unramified outside a finite set $S$ of places, then it suffices to show that $\# \chi(\prod_{v \in S} O_v^\times) < \infty$. But this is because $\prod_{v \in S} O_v^\times$ has a pro-$p$-group of finite index and $O_E^\times$ has a pro-$\ell$-group of finite index. □

### 6 Fourier Analysis on Adeles and Ideles

Main references are [Poo15], [R-V99] and [Tat65].

**Local Notations**

**Def. (12.2.6.1)** [Normalized Valuations]. Let $K$ be a local field and $d\mu$ a Haar measure on $K$. Let the valuation on $K$ be given by $d\mu(\alpha \xi) = |\alpha| d\mu(\xi)$. Then

$$|k| = \begin{cases} |k| & K = \mathbb{R} \\ |k|^2 & K = \mathbb{C} \\ \frac{1}{||p||^{1/2}(x)} & K \text{ non-Archimedean} \end{cases}.$$
Proof: If $K = \mathbb{R}, \mathbb{C}$, this is routine calculation. If $K$ is non-Archimedean, then by the translation invariance of $\mu$, $\mu(\alpha \mathcal{O}) = \frac{\mu(\mathcal{O})}{N(\alpha)} = |\alpha|\mu(\mathcal{O})$. 

Def. (12.2.6.2) [Unramified Quasi-Character]. The multiplicative group $K^\times$ is also a locally compact group. For a quasi-character $\chi$ of $K^\times$, it is called unramified iff $\chi(\mathcal{O}_K^*) = 1$.

An unramified quasi-character on $K^\times$ is equivalent to a continuous group homomorphism from $\text{val}(K^\times) \to \mathbb{Z}$. But $\text{val}(K^\times)$ must be isomorphic to $\mathbb{Z}$ or $\mathbb{R}$, so the assertion follows from (10.9.3.3). □

Lemma (12.2.6.3) [Canonical Character of Local Fields]. Consider the base field $k$ of $K$ (topologically), which is $\mathbb{R}, \mathbb{Q}_p$ or $F_p((t))$ by Ostrowski (10.3.3.18). Now let

$$\lambda(x) = \begin{cases} 
    x(\text{mod } 1) & k = \mathbb{R} \\
    \text{a rational number } \lambda(x) \text{ that } \lambda(x) - x \in \mathbb{Z}_p \text{ in } \mathbb{Q}/\mathbb{Z} & k = \mathbb{Q}_p \\
    a_{-1}/p = \text{res}(x)/p & k = F_p((t)) 
\end{cases}$$

Then $\lambda$ is a continuous additive function on $k$. Now let

$$\Lambda(x) = \begin{cases} 
    \lambda(\text{tr}_{K/k}(x)) & \text{number field case} \\
    \lambda(\text{tr}_{K/k_0}(x\omega_0)) & \text{function field case, where } \omega \text{ is a chosen global meromorphic form on } X. 
\end{cases}$$

And $X(x) = e^{2\pi i \Lambda(x)}$. Notice that this is just a rigorous definition of the character $e^{2\pi i \text{tr}_{K/k}(x)}$.

Cor. (12.2.6.4). $F(\eta) = e^{2\pi i \Lambda(\eta \xi)}$ is trivial on $\mathcal{O}_K$ is equivalent to $\xi \in \mathfrak{b}^{-1}$, where $\mathfrak{b} = \mathfrak{b}_{K/k}$. In other words, adopting the isomorphism of (10.9.3.35), $\mathcal{O} = \mathfrak{b}^{-1}, (\mathfrak{b}^{-1})^\perp = \mathcal{O}$.

Proof: Because $\Lambda(\eta \mathcal{O}) = 0$ iff $\text{tr}_{K/k}(\eta \mathcal{O}) \subset \mathcal{O}_k$, which is equivalent to $\eta \in \delta^{-1}$. □

Prop. (12.2.6.5) [Canonical Self-Adjoint Haar Measures]. We can calculate the self-adjoint Haar measure w.r.t. the canonical character on $K^+(12.2.6.3)$ as follows:

$$d\mu = \begin{cases} 
    \text{the measure that } \mu(\mathcal{O}) = \frac{1}{|b|^{1/2}} & K = \mathbb{R} \\
    2\text{dm} & K = \mathbb{C} \\
    \mu(\mathcal{O}) & \text{others} 
\end{cases}$$

Proof: We only calculate for the $p$-adic fields?.

Let $f = 1_{\mathcal{O}}$, then

$$\hat{f}(\eta) = \int_{\mathcal{O}} e^{-2\pi i \Lambda(\eta \xi)}d\mu(\xi) = \begin{cases} 
    \mu(\mathcal{O}) & \eta \in \mathfrak{b}^{-1} \\
    0 & \text{otherwise} 
\end{cases} = \mu(\mathcal{O})1_{\mathfrak{b}^{-1}}(\eta)$$

By (12.2.6.4) and (10.9.1.14). So

$$I_{\mathcal{O}}(\xi) = \int_{G} \hat{f}(F(\eta))(\xi, F(\eta))d\mu(\eta) = \int_{\mathfrak{b}^{-1}} \mu(\mathcal{O})e^{2\pi i \Lambda(\eta \xi)}d\mu(\eta) = \mu(\mathcal{O})\mu(\delta^{-1})I_{\mathcal{O}}(\eta).$$

So $\mu(\mathcal{O})\mu(\delta^{-1}) = N(\delta)\mu(\mathcal{O})^2 = 1$, which shows the desired result. □
Remark (12.2.6.6). In fact, if the conductor of $\psi$ is $p^k$, then $\mu(O) = ||p||^{k/2}$.

Cor. (12.2.6.7) [Quasi-Character of $K^\times$]. There is a continuous morphism from $K^\times \to O^*_K$: $\tilde{\alpha} = \alpha/\pi^{v(\alpha)}$ when $\alpha$ is non-Archimedean or $\tilde{\alpha} = \alpha/|\alpha|$ if $K$ is Archimedean. So any quasi-character $c$ is of the form $c(\alpha) = c(\tilde{\alpha})$ times an unramified quasi-character, which is of the form $|\cdot|^s$, where $\text{Re}(s)$ is called the exponent of $c$. Now $O^*_K$ is a compact group, so continuous quasi-characters $\tilde{c}$ on it must be a character.

Def. (12.2.6.8) [Haar Measure on $K^\times$]. Notice that if $g(\alpha) \in C_c(K^\times)$, then $\frac{g(\alpha)}{|\alpha|} \in C_c(K^\times \setminus 0)$, so if we define $\Phi(g) = \int_{K^\times \setminus \{0\}} g(\xi)|\xi|^{-1}d\xi$, then

$$\Phi(\psi g) = \int_{K^\times \setminus \{0\}} g(\alpha)|\alpha|^{-1}|\alpha|d\xi = \int_{K^\times \setminus \{0\}} g(\alpha)|\alpha|^{-1}d\alpha \xi = \Phi(g).$$

By (12.2.6.1). So By Riesz representation, there is a Haar measure $d\tilde{\chi}_\alpha$ on $K^\times$ so $\int_{K^\times} g(\alpha) d\tilde{\chi}_\alpha = \int_{K^\times} g(\xi)|\xi|^{-1}d\xi$, for any $g \in C_c(K^\times)$.

But when $K$ is non-Archimedean, renormalize $d\tilde{\chi}_\alpha = (1 - \frac{1}{Np})^{-1}d\tilde{\chi}_\alpha$.

Remark (12.2.6.9). The reason behind this normalization is when $d\mu$ is the canonical measure (12.2.6.5), we want to make $d\tilde{\chi}_\alpha(O^*) = ||b||^{-1/2}$. Thus

$$\int_{O^*} d\xi = \sum_{k=0}^{\infty} \int_{p^kO^*} d\xi = (1 + \frac{1}{Np} + \frac{1}{Np^2} + \ldots) \int_{O^*} d\xi = \frac{1}{1 - \frac{1}{Np}} \int_{O^*} d\xi$$

so

$$\int_{O^*} d\tilde{\chi}_\alpha = \int_{O^*} |\xi|^{-1}d\xi = \frac{||p||-1}{||p||} \int_{O^*} d\xi = \frac{||p||-1}{||p||} ||b||^{-1/2}(12.2.6.5)$$

Def. (12.2.6.10) [Schwartz-Bruhat Function]. For a local field $K$, we define the set $\mathcal{S}(K)$ of Schwartz-Bruhat functions on $K$ as Schwartz functions on $K$ if $F = \mathbb{R}, \mathbb{C}(10.7.2.1)$ and locally continuous constant functions of compact support if $K$ is non-Archimedean.

Prop. (12.2.6.11) [Local Schwarz Functions]. The space $\mathcal{S}(K)$ of Schwartz functions satisfy the following properties: If $f \in \mathcal{S}(K)$,

- $f, \hat{f} \in L^1(K^\times)$.
- $f(\alpha)|\alpha|^\sigma, \hat{f}(\alpha)|\alpha|^\sigma \in L^1(K^\times)$ for $\sigma > 0$.
- $f \in \mathcal{S}(K)$ too.

Proof: 3: $p$-adic case: Let $p^n$ be the conductor of $\psi$, then the Fourier transform of $\chi_{p^{-k}}$ is $V(p^{-k})\chi_{p^{n+k}}$. Then for $k$ large, $\chi_{p^{-k}} v = V(p^{-k})V(p^{n+k})v$, thus $v \in C_c^\infty(F)$.

Archimedean case: (10.10.2.5).

Global notations

Notations (12.2.6.12).

- There are natural Haar measures $d\mu_K, d\tilde{\chi}_\alpha$ on $A_F$ and $I_F$ defined by (12.2.5.6) and (12.2.6.5)(12.2.6.8). They satisfy $d\tilde{\chi}_\alpha = \frac{1}{||\cdot||} d\mu_K$.
- Let $b = b_{F/Q}$ when $F$ is a number field, or $b = \{x| \text{tr}(\text{res}(xO)) = 0\}^{-1}$ when $F$ is a function field.
• Fix \( \psi = \prod \psi_v \) a character of \( A_F / F \), then

\textbf{Def. (12.2.6.13)[Global Fourier Transform].} (10.9.3.35) shows \( \psi \) induces a canonical isomorphism

\[ A \cong \hat{A} : \eta \mapsto (\xi \rightarrow \psi(\eta \xi)) , \]

and we choose the corresponding self-dual Haar measure \( dx \), then the Fourier transform on \( A \) is then defined to be:

\[ \hat{f}(y) = \int_A f(x) \overline{\psi(xy)} \, dx, \quad f(x) = \int_A \hat{f}(y) \psi(xy) \, dy. \]

In fact \( dx = \prod x_p \) is the restricted product measure on \( A(12.2.5.6) \), where \( dx_p \) is the self-dual measure w.r.t \( \psi_p \) in (12.2.6.5), then \( dx \) is the self-dual Haar measure w.r.t the global canonical character \( \psi \) by (12.2.5.9), called the \textbf{Tamagawa measure} on \( A \).

\textbf{Def. (12.2.6.14)[Global Schwartz-Bruhat Functions].} For a global field \( F \), the set \( \mathcal{S}(F) \) of global Schwartz-Bruhat functions is defined to be

\[ \mathcal{S}(F) = \bigotimes_{v \in \Sigma_F} \mathcal{S}(F_v)(2.4.4.13). \]

\textbf{Prop. (12.2.6.15) [Schwartz-Bruhat Functions].} A Schwartz-Bruhat function \( f \in \mathcal{S}(A_F)(12.2.6.14) \) satisfies:

- \( f(x) \in L^1(A) \), \( \hat{f}(x) \in L^1(A) \) and \( f, \hat{f} \) is continuous.
- \( \sum_{\xi \in K} f(\alpha(x + \xi)) \) and \( \sum_{\xi \in K} \hat{f}(\alpha(x + \xi)) \) converges uniformly absolutely on compact sets of \( A \).
- \( f(\alpha)|\alpha|^{\sigma}, \hat{f}(\alpha)|\alpha|^{\sigma} \in L^1(I_F) \) for \( \sigma > 1 \).

\textit{Proof:} 1, 2 is the same as in (12.2.6.23), for 3: \( \int_{I_F} |f| |\alpha|^{\sigma} \, d\alpha = \prod_p \int_{I_{F_p}} |f_p| |\alpha|^{\sigma} \, d\alpha_p \), and for a.e. \( p \),

\[ \int_{K_p} |f_p| |\alpha|^{\sigma} \, d\alpha_p = \int_{K_p \cap \mathcal{O}_p} |\alpha_p|^{\sigma} \, d\alpha_p = \frac{1}{1 - (\frac{N_p}{p})^{\sigma}} \int_{\mathcal{O}_p} \, d\alpha_p = \frac{1}{1 - (\frac{N_p}{p})^{\sigma}}. \]

Thus the global integral converges by comparison with the Dedekind Zeta function (16.2.2.1). \( \qed \)

\textbf{Def. (12.2.6.16)[Global Canonical Character].} Define the \textbf{global canonical character}

\[ X : A_F \to \mathbb{C}^\times : x \mapsto e^{2\pi i \Lambda(x)}, \quad \Lambda(x) = \sum \Lambda_p(x_p)(12.2.6.3). \]

Notice this is definable because \( x_p \in \mathcal{O}_p \) a.e. \( p \), thus \( \Lambda_p(x_p) = 1 \) a.e..

Then \( X(K) = 1 \).

\textit{Proof:} In the number field case,

\[ \Lambda(\xi) = \sum_p \sum_{\mathfrak{p} | \mathfrak{p}^p} \lambda_p(\text{tr}_{\mathfrak{p}/\mathbb{Q}}(\xi)) = \sum_p \lambda_p(\text{tr}_{K/Q}(\xi)) \]

so to show \( \lambda \) is an integer, it suffices to show \( \Lambda(a) \) is a \( q \)-adic integer for any \( q \) and any \( a \in \mathbb{Q} \), but for this, notice

\[ \sum \lambda_p(x) = \sum_{p \neq q, \infty} \lambda_p(x) + \lambda_q(x) - x \]

is a \( q \)-adic integer, by definition (12.2.6.3).

In the function field case, this follows from the fact that the sum of residues of a meromorphic 1-form is 0?.
Prop. (12.2.6.17). $K^\perp = K$, i.e. $X(xy) = 0, \forall y \in K \iff x \in K$. 

Proof: Because $K^\perp \cong \hat{A}/\hat{K}$ and $A/K$ is compact (12.2.5.19), $K^\perp$ is discrete (10.9.3.7) and contains $K$. So $K^\perp/K$ is discrete hence finite in $A/K$. But $K^\perp$ is clearly a vector space over $K$, thus $K^\perp = K$ must be true, because $|K| = \infty$.

Cor. (12.2.6.18). By (10.9.3.35) and (12.2.6.17), any non-trivial character on $A_F/F$ is of the form $a \mapsto X(ka)$ for some $k \in K$. In particular, for any such character $\psi$, $\psi_v$ is non-trivial.

Def. (12.2.6.19) [Unramified Places]. Let $\chi$ be a Hecke character of $F$, then $v \in \Sigma_F$ is called unramified if $v \in \Sigma^\fin_F$, $b_v = 1$, $c(\psi_v) = \mathcal{O}_v$, $\chi_v$ is unramified (12.2.6.2). Notice a.e. place $v$ is unramified.

Proof: To show that for any unramified character $\psi$, the conductor of $\varphi_v$ is $\mathcal{O}_v$, consider the canonical character $X$ defined (12.2.6.16), it can be verified the conductor of $X_v$ is $\mathcal{O}_v$ for a.e. $v$, and $\psi$ must be of the form $\psi(x) = X(ax)$ for some $a \in K$ by (12.2.6.13) and (12.2.6.17), thus this is also true for $\psi$. □

Prop. (12.2.6.20).

$$V(I_F^1/F^\times) = \frac{2^{r_1}(2\pi)^{r_2}}{w_K \sqrt{|d_K|}} h_F \text{Reg}_F$$

where $w_F = F_\tor^\times$, $h_F$ is the class number, and $\text{Reg}_F$ is the regulator.


Lemma (12.2.6.21) [Poisson Formula]. If $F \in L^1(A_F)$ and $\sum_{\xi \in F} |\hat{f}(\xi)| < \infty$, then in the self-dual Haar measure

$$\sum_{\xi \in F} \hat{f}(\xi) = \sum_{\xi \in F} f(\xi).$$

and $V(A_F/F) = 1$.

Proof: By (12.2.6.17), this is a special case of (10.9.3.31). In fact, we know it is true for a constant $V(A/K)$, but it is symmetric, so $V(A/K)^2 = 1$. □

Prop. (12.2.6.22) [Riemann-Roch]. If $f(ax) \in L^1(A)$ and $\sum_{\xi \in F} |\hat{f}(a\xi)| < \infty$ for any idele $a \in I_F$, then for any idele $a$,

$$\frac{1}{|a|} \sum_{\xi \in F} \hat{f}(\xi/\bar{a}) = \sum_{\xi \in F} f(a\xi).$$

Proof: Consider $g(x) = f(ax)$, then

$$\hat{g}(x) = \int_{A_F} f(\alpha \eta) e^{-2\pi i \lambda(x\eta)} d\eta = \frac{1}{|a|} \int_{A_F} f(\eta) e^{-2\pi i \lambda(x/a\eta)} d\eta = \frac{1}{|a|} \hat{f}(x/a).$$

Then apply Poisson formula (12.2.6.21) to $g$. □

Prop. (12.2.6.23). Schwartz-Bruhat functions (12.2.6.14) satisfy the condition in (12.2.6.22).
Proof: \( \int_A |f| = \prod_v \int_{F_v} |f_v|dx_v < \infty \), noticing (12.2.6.5) and \( N(\delta) = 1 \) a.e. \( v \). And for any Schwartz function \( f \) and any \( x \), the set of \( k \) that \( f_v(x_v + k_v) \neq 0 \) is \( v \)-bounded for \( v \) non-Archimedean and \( |k|_v \leq 1 \) a.e., so in the function case, these \( k \) are finite because \( K \) is discrete in \( A \).

And in the number field case, these \( k \) is contained in some fractional ideal \( I \), but \( I \) is then a lattice in \( F_\infty \) by Minkowski theory, so

\[
\sum_{\xi \in K} |f(x + \xi)| \leq C \sum_{x \in K} \prod_{p \in S_\infty} |f_p(x + \xi)|
\]

but \( f_p \) is an Archimedean Schwartz function, thus this is absolutely convergent.

Now we showed that \( \int_{\xi \in F} \hat{f}(\xi) < \infty \), because \( \hat{f} \in \delta(A_F) \), by (12.2.6.11). \( \square \)

Prop. (12.2.6.24) [True Riemann-Roch For Function Fields]. Cf. [Handwritten Notes].
12.3 Quadratic Forms over Fields

Basic references are [Lam05], [Quadratic Forms Clark] and [Algebraic and Geometric Theory of Quadratic Forms].

All fields $K$ in this section has $\text{char} K \neq 2$.

1 Quadratic Forms

This subsection should be regarded as a continuation of §8. In fact, most materials in this subsection are trivial facts.

**Def. (12.3.1.1).** Given a field $K$ of char $\neq 2$, a quadratic form over $K$ is a bilinear form on $K^n$ for some $K$. It is represented by a symmetric matrix.

The reason that char $K \neq 2$ is because only in this case, a quadratic form $q$ is equivalent to a symmetric bilinear form $B$, and I will use this equivalence freely.

The determinant $\det$ is a function from the set of quadratic forms to $K \times (K \times)^2$ that is invariant under congruence.

**Def. (12.3.1.2) [Quadratically Closed].** A field is called quadratically closed iff $(K \times)^2 = K \times$, or equivalently $K$ has no quadratic field extensions.

**Def. (12.3.1.3).** The category of quadratic spaces is a category with objects as finite dimensional spaces with a quadratic form, and its morphisms are isometric embeddings.

**Def. (12.3.1.4) [Universal Quadratic Form].** For a quadratic form $A$, let $D_F(A)$ be the set of elements representable by $A$. A universal quadratic form is a quadratic form that represents every element of $K^*$.

**Prop. (12.3.1.5).** If every binary quadratic form over $K$ is universal, then any two non-degenerate quadratic forms over $K$ are isomorphic iff they have the same rank and determinant.

**Proof:** This is because $\langle a, b \rangle \cong \langle 1, ab \rangle$ and then use induction. □

**Non-Degeneracy**

**Def. (12.3.1.6) [Non-Degeneracy].** A quadratic space is called non-degenerate if $v \mapsto B(v, \cdot)$ is an isomorphism from $V$ to $V^*$. Notice if $\dim V = \infty$, this cannot happen, because $\dim V^* > \dim V(2.3.3.9)$. And in case $\dim V < \infty$, $\dim V = \dim V^*$, so it suffices to show $v \mapsto B(v, \cdot)$ is injective, i.e. if $v \neq 0$, then there is a $w$ that $B(v, w) \neq 0$.

**Prop. (12.3.1.7) [Radical Splitting].** The radical of a quadratic space is defined to be $\text{rad}(V) = V^\perp$. Then for any quadratic form $V$, there is an orthogonal decomposition $V = \text{rad}(Y) \oplus W$, where $W$ is a non-degenerate form.

**Proof:** In fact, by the definition, any complement space of $\text{rad}(V)$ in $V$ can be chosen as the orthogonal complement $W$. □

**Prop. (12.3.1.8).** If $W$ is a non-degenerate sub-quadratic space of $V$, then $W \oplus W^\perp = V$.

**Proof:** Since $W$ is non-degenerate, $W \cap W^\perp = 0$. and for any $v \in V$, $B(v, \cdot) \in W^*$, so by degeneracy, there is a $w \in W$ that $B(v, \cdot) = B(w, \cdot)$, then $z = v - w \in W^\perp$ and $v = w + z$. □
Prop. (12.3.1.9) [Orthogonal Complement and Non-Degeneracy]. If $V$ is a non-degenerate quadratic space, then for any non-degenerate subspace $W$, $\dim W + \dim W^\perp = \dim V$, and $(W^\perp)^\perp = W$.

Proof: The first is immediate from the fact $\dim \ker + \dim \Coker = \dim V$. The second is by dimensional reason. □

Cor. (12.3.1.10). A subspace $W$ of a non-degenerate quadratic space $V$ is a non-degenerate quadratic space iff $W \cap W^\perp = 0$.

Remark (12.3.1.11). We basically only care about non-degenerate forms, so from now on, we only care about non-degenerate forms.

Diagonalizability

Prop. (12.3.1.12) [Quadratic Form Representable]. Any quadratic forms over $K$ of char $\neq 2$ is diagonalizable, and if $\alpha \in K^*$ is represented by $K$, then it is diagonalizable to a matrix with first entry $\alpha$.

We will use the notation $\langle \alpha_1, \ldots, \alpha_n \rangle$ for the diagonal quadratic form $\sum \alpha_i x_i^2$.

Proof: Use (2.3.8.5), since in this case, a quadratic form is equivalent to a symmetric form. And if $\alpha = B(v, v)$, then we can choose $v$ in the first place in the proof of (2.3.8.5). □

Cor. (12.3.1.13). Over a quadratically closed field $K$ of char $\neq 2$, any non-degenerate quadratic form is congruent to $x_1^2 + \ldots + x_n^2$.

Proof: Because in this case, we can make $\sum a_i x_i^2$ into $\sum (\sqrt{a_i} x_i)^2$. □

Isotropic and Hyperbolic Spaces

Def. (12.3.1.14) [Isotropic]. Given a non-degenerate quadratic space $V$, a vector $v$ is called isotropic if $B(v, v) = 0$. $V$ is itself called isotropic if it is non-degenerate and there exists an isotropic vector, otherwise it is called anisotropic.

Def. (12.3.1.15) [Hyperbolic]. The hyperbolic plane $H$ is the 2-dimensional space with quadratic form $H(x, y) = xy$, which is congruent to $\frac{1}{2}(x^2 - y^2)$.

A quadratic space is called hyperbolic if it is isomorphic to a direct sum of hyperbolic planes.

Lemma (12.3.1.16). If $V$ is a non-degenerate isotropic space, then there is an isometric imbedding of the hyperbolic plane into $V$.

Proof: There is a $u \in V$ that $B(u, w) = 0$. By non-degeneracy, there is a $w$ that $B(u, w) \neq 0$. We may assume $B(u, w) = 1$. Now I claim there is an $\alpha$ that $q(\alpha u + w) = 0$: in fact, $q(\alpha u + w) = 2\alpha B(u, w) + q(w)$, so take $\alpha = -q(w)/2$. Let $v = \alpha u + w$, then $q(u) = q(v) = 0$, and $B(u, v) = 1$, so it is isomorphic to $H$. □

Prop. (12.3.1.17) [Isotropic Complement]. If $V$ is a non-degenerate quadratic space, and $W \subset V$ is an isotropic space with basis $u_1, \ldots, u_m$, then there is another isotropic space $W'$ with basis $v_1, \ldots, v_m$ that $B(u_i, v_j) = \delta_{ij}$.
12.3. QUADRATIC FORMS OVER FIELDS

\[12.3.1.18\] \langle a, -a \rangle \cong H, because it is isotropic, and it has dimension 2.

\[12.3.1.19\] **Isotropic Form is Universal.** A non-degenerate isotropic space is universal, because hyperbolic plane does.

\[12.3.1.20\] A maximal totally isotropic space in a non-degenerate quadratic space \(V\) has dimension at most \(\frac{1}{2} \dim V\), and equality holds if \(V\) is hyperbolic.

\[12.3.1.21\] **First Representation Theorem.** If \(q\) is a non-degenerate quadratic form, then \(q\) represents \(\alpha \in K^*\) iff \(q \oplus \langle -\alpha \rangle\) is isotropic.

\[12.3.1.22\] The following are equivalent:

- Any \(n\)-quadratic form over \(K\) is universal.
- Any \((n+1)\)-quadratic form over \(K\) is isotropic.

\[12.3.1.23\] **Transform of Binary Forms.** For any \(a, b \in F^*\) that \(a + b \in F^*\), \(\langle a, b \rangle \cong \langle a + b, (a + b)ab \rangle\).

\[12.3.1.24\] **Isotropy Criterion.** For two non-degenerate forms \(f, g\) over \(K\), \(h = \langle f, -g \rangle\) is isotropic iff there is an \(\alpha \in K^*\) that is represented by both \(f\) and \(g\).

**Proof:** Easy, notice to use isotropic form is universal \((12.3.1.19)\).

\[2\] Witt Theory

\[12.3.2.1\] **Witt Cancellation Theorem.** If \(U_1, U_2, V_1, V_2\) are quadratic spaces and \(V_1 \cong V_2\), \(V_1 \oplus U_1 \cong V_2 \cong U_2\), then \(U_1 \cong U_2\).

**Proof:** We may identify \(V_1 = V_2 = V\), and \(W = U_1 \oplus V = U_2 \oplus V\).

First if \(V\) is totally isotropic and \(U_1\) is non-degenerate, then there is a matrix \(M = \begin{bmatrix} A & B \\ C & D \end{bmatrix}\) that

\[M^t \begin{bmatrix} 0 & 0 \\ 0 & B_2 \end{bmatrix} M = \begin{bmatrix} 0 & 0 \\ 0 & B_1 \end{bmatrix}\]

So \(B_1 = D^t B_2 D\). As \(B_1\) is non-singular, so is \(D\), thus \(U_1 \cong U_2\).

Now if \(V\) is isotropic but \(U_1, U_2\) are not non-degenerate, then we may assume in their diagonalization, \(U_1\) has less 0s, it has \(r\) 0s, then we can extract from both \(U_i\) a zero part, thus reducing to the above case.
Now if $\dim V = 1$, $V = \langle a \rangle$, if $a = 0$, then we are done by the above argument, and if $a = 0$, then find $q(x) = a$, then by (12.3.2.13), we can find a $\tau \in O(W)$ that $\tau(V_1) = V_2$, so now $U_1, U_2$ as the orthogonal complement of $V_1, V_2$, they are isometric under the map $\tau$.

So now in general, we can cancel $V$ out by moving its diagonal part once a time. \hfill $\square$

**Cor. (12.3.2.2).** If $X$ is a quadratic space and $V_1, V_2$ are non-degenerate subspaces of $X$, then any isometry $V_1 \cong V_2$ extends to an isometry of $X$.

*Proof:* $V_i \oplus V_i^\perp = X$ by (12.3.1.8). \hfill $\square$

**Cor. (12.3.2.3) [Witt’s Extension Theorem].** If $X$ is a non-degenerate quadratic space and $f : W_1 \to W_2$ is an isometry of two subspaces of $X$, then $f$ extends to an isometry of $X$.

Notice this also holds for symplectic spaces $X$, by the same method of proof.

*Proof:* If $W_1$ is non-degenerate, then so does $W_2$, and we can use (12.3.2.2). By (12.3.1.7), we can write $W_i = U_i \oplus V_i$ where $U_i$ is totally isotropic and $V_i$ is non-degenerate. Now $X, V_i$ are non-degenerate, $V_i^\perp$ is non-degenerate also, so there is an isotropic complement $U'_i \subset V_i^\perp$ (12.3.1.17). Let $T_i = \langle U_i, U'_i \rangle V_i$, then $T_i$ is non-degenerate and $W \subset T$. As $U_i$ is the radical of $W_i$, $U_1 \cong U_2$, and then $\langle U_1, U'_1 \rangle \cong \langle U_2, U'_2 \rangle$. By Witt cancellation, $W_1 \cong W_2$. So we reduced to the non-degenerate case. \hfill $\square$

**Cor. (12.3.2.4).** If $V$ is a non-degenerate quadratic space, then the group of isometries of $X$ acts transitively on the set of all totally isotropic subspaces of a fixed dimension $d$.

**Prop. (12.3.2.5) [Witt’s Decomposition Theorem].** For any quadratic space $V$, there is an orthogonal decomposition

$$V \cong \text{rad}(V) \oplus \bigoplus_{1}^{k} H \oplus V'$$

where $V'$ is anisotropic (12.3.1.14). Moreover the number $k = I(V)$ which is called the **Witt index** of $V$ and the isometry class of $V' = w(V)$ which is called the **non-isotropic kernel** is independent of the decomposition.

*Proof:* The existence of the decomposition follows from (12.3.1.7) and an easy induction using (12.3.1.16). The uniqueness is an easy corollary of (12.3.1.16) and Witt’s cancellation theorem. \hfill $\square$

**Cor. (12.3.2.6).** The Witt index equals the maximal dimension of a maximal totally isotropic subspace of $W$, by (12.3.1.17).

**Remark (12.3.2.7).** This is a good reason that we will only consider non-degenerate quadratic forms from now on.

**Cor. (12.3.2.8) [Sylvester’s Law of Nullity].** Let $q_{r,s} = [r](1) \oplus [s](1)$, then any non-degenerate quadratic form $q$ over $R$ is congruent to exactly one of $q_{r,s}$, and $r - s$ is called the **signature** of $q$.

**Def. (12.3.2.9).** Two quadratic forms $q_1 = \langle a_1, \ldots, a_n \rangle$ and $q_2 = \langle b_1, \ldots, b_n \rangle$ are called **simply equivalent** iff there are two indices that $\langle a_i, a_j \rangle \cong \langle b_i, b_j \rangle$. Two quadratic forms are called **chain equivalent** iff there is a chain of simply equivalence between them.

**Prop. (12.3.2.10) [Witt’s Chain Equivalence Theorem].** Two diagonal quadratic forms over $K$ are equivalent iff they are chain equivalent.
12.3. QUADRATIC FORMS OVER FIELDS

Proof: Chain equivalent is clearly equivalent. Conversely, by Witt’s decomposition theorem, it is easy to reduce to the non-degenerate case.

Now if \( q = \{\alpha_1, \ldots, \alpha_n\} = q' = \{\beta_1, \ldots, \beta_n\} \), any form \( q = \{\gamma_1, \ldots, \gamma_n\} \) that is chain equivalent to \( q \) is equivalent to \( q' \), so \( \beta_1 \) is represented by it, choose a form that there is a minimal \( l \) that \( \beta_1 \) is represented by \( \{\gamma_1, \ldots, \gamma_l\} \), we prove that \( l = 1 \):

- if the minimal \( l \) is not 1, then \( d = \gamma_1 a_1^2 + \gamma_2 a_2^2 \neq 0 \); (otherwise \( l \) can be smaller), so \( \{\gamma_1, \gamma_2\} \) is an isomorphism, and this is smaller, contradiction.

Now \( l = 1 \), so we may assume \( \alpha_1 = \beta_1 \), and then Witt’s cancellation (12.3.2.1) shows that \( \{\alpha_2, \ldots, \alpha_n\} \cong \{\beta_2, \ldots, \beta_n\} \), so we win by induction. □

Orthogonal Group

Prop. (12.3.2.11). The orthogonal group of a quadratic form \( q \) is the set of matrixes \( M \) that \( g(Mx) = q(x) \). And it is clear \( det M = \pm 1 \), so we can also define \( O^+(V) \) and \( O^-(V) \).

Def. (12.3.2.12). A hyperplane reflection for a non-isotropic vector \( v \) is defined by \( x \mapsto x - \frac{2B(x,v)}{q(v)} v \), it is an element in \( O(V) \).

Prop. (12.3.2.13). If \( x, y \) are two non-isotropic vectors that \( q(x) = q(y) \), then there is a \( \tau \in O(V) \) that \( \tau(x) = y \).

Proof: First notice \( q(x + y) + q(x - y) = 2q(x) + 2q(y) = 4q(x) \neq 0 \), so one of \( x + y, x - y \) is non-isotropic. And it can be easily calculated that \( \tau_{x+y}(x) = y \) or \( -\tau_{x+y}(x) = y \). □

Prop. (12.3.2.14)[Cartan-Dieudonné]. Let \( V \) be a non-degenerate quadratic form of dimension \( n \), then every element of the orthogonal group \( O(V) \) can be represented as a product of \( n \) reflections.

Proof: Cf. [Quadratic Forms Clark P22]. □

3 Witt Ring

References are [Quadratic Forms 2, Clark].

Def. (12.3.3.1)[Witt Ring]. The Witt ring \( W(K) \) of \( K \) is a free commutative ring over \( \mathbb{Z} \) generated by equivalent classes of anisotropic(12.3.1.14) quadratic forms over \( K \), modulo the the relations \( [q_1] + [q_2] - [q_1 \oplus q_2] \) and \( [q_1] \cdot [q_2] - [q_1 \otimes q_2] \).

There is another ring, the Grothendieck-Witt ring \( \hat{W}(K) \) which is defined as the ring generated by all non-degenerate quadratic forms over \( K \).

Cor. (12.3.3.2) [Rank Functor]. There are rank functors from \( \hat{W}(K) \rightarrow \mathbb{Z} \), which is a ring homomorphism. In particular, two elements of the same rank are equal in \( \hat{W}(K) \) iff they are equal in \( W(F) \), by Witt’s cancelation theorem (12.3.2.1).

Prop. (12.3.3.3). The rank functor is an isomorphism \( \hat{W}(K) \rightarrow \mathbb{Z} \) iff \( K \) is quadratically closed. In this case, \( \hat{W}(K) \cong \mathbb{Z}/2\mathbb{Z} \).

Proof: This is equivalent to \( \langle a \rangle \cong \langle 1 \rangle \) for any \( a \in K^* \), which means \( K \) is quadratically closed. □

Prop. (12.3.3.4). The subgroup \( [H] \) generated by the hyperbolic plane is an ideal of \( \hat{W}(K) \). And \( \hat{W}(K)/\mathbb{Z}[H] \cong W(K) \).
Proof: \( \mathbb{Z}[H] \) is an ideal because \([H] \cdot ([a_1, \ldots, a_n]) \cong \sum (a_i, -a_i) \) which is a multiple of \([H] \), by (12.3.1.18). The last assertion follows from Witt’s decomposition (12.3.2.5).

Cor. (12.3.3.5). \([a_1, \ldots, a_n] + [-(a_1, \ldots, -a_n)] = 0 \in W(F)\), by (12.3.1.18).

Prop. (12.3.3.6) [Presentation of the Witt Ring]. \( \widetilde{W}(F) \) is isomorphic to the quotient of the free commutative ring generated by \( \{ [a] | a \in F^* \} \) module the following relations:

- \([1] - 1\).
- \([ab] - [a] - [b]\).
- \([a] + [b] - [a+b](1 + [ab])\), \(a, b, a+b \in F^*\).

Proof: Cf. [Lam, P39]. □

4 Quaternion Algebras

References are [Quaternion Algebras].

Notations (12.3.4.1).
- In this subsection, let \( k, F \in \text{Field} \).

Def. (12.3.4.2) [Quaternion Algebras]. Let \( a, b \in F^x \), define a Quaternion algebra \( Q(a, b) \) as

\[ Q_F(a, b) = Q(X, Y)/(X^2 - a, Y^2 - b, XY + YX). \]

Denote \( \bar{X} = i, \bar{Y} = j, \bar{XY} = k \).

Prop. (12.3.4.3). Let \( a, b \in F^x \), then

- \( \dim_{F} Q_F(a, b) = 4 \), thus any element of \( Q_F(a, b) \) is of the form \( x + yi + zj + wk \).
- \( Q_F(ax^2, by^2) \cong Q_F(a, b) \) for \( x, y \in F^* \).
- \( Q_F(-1, 1) \cong M(2, F) \).
- \( Q_F(a, b) \) is a simple algebra with center \( F \).

Proof: 1: \( Q_F(a, b) \otimes_F \bar{F} = Q_{\bar{F}}(-1, 1) \cong M_2(\bar{F}) \) has dimension 4 over \( \bar{F} \), by item 2 and 3.

2: trivial.

3: The map is given by \( \varphi : Q_F(-1, 1) \to M(2, F) : i \mapsto \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, j \mapsto \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} \). The verification is straightforward.

4: Consider \( Q_F(a, b) \otimes_F \bar{F} \cong \text{Mat}(2, \bar{F}) \) is simple with center \( \bar{F} \), the center of \( Q_F(a, b) \) has to be \( F \), and also simple. □

Def. (12.3.4.4) [Pure Tensors]. A quaternion element of the form \( yi + zj + wk \) is called a pure tensor. The space of pure tensor is denoted by \( A_0 \).

Let \( v \neq 0 \in Q_F(a, b) \), then \( v \in A_0 \) iff \( v \notin F \) but \( v^2 \in F \).

Proof: By direct calculation,

\[ (x + yi + zj + wk)^2 = (x^2 + ay^2 + bz^2 - abw) + 2x(yi + zj + wk). \]

□
Def. (12.3.4.5) [Bar Involution]. There is an anti-involution of $Q_F(a, b) = \frac{Q(X, Y)}{(X^2 - a, Y^2 - b, XY + YX)}$ given by $X \mapsto -X, Y \mapsto -Y$(thus $XY \mapsto (-Y)(-X) = YX$), called the bar involution.

Thus if we define the norm and trace $N : x \mapsto x\bar{x}, \text{tr} : x \mapsto x + \bar{x}$, then they have images in $F$.

If $\alpha = x + yi + zj + wk$, then $\text{tr}(\alpha) = 2x, N(\alpha) = x^2 - ay^2 - bz^2 + abw^2$.

Cor. (12.3.4.6). Notice the Bar involution can be defined intrinsically, by defining a pure vector to be a vector $x$ s.t. $x^2 \in F$ but $x \bar{x} \notin F$.

Cor. (12.3.4.7). For $x \in Q_F(a, b)$, if we let $T(x)$ be the left(or right) multiplication by $x$ on $Q_F(a, b)$, then the determinant of $T(x)$ equals $N(x)^2$.

Proof: After base change, all the values won’t change, thus it suffices to prove for $M(2, F)$, in which case, it can be verified by (12.3.4.3) that $\det(A) = N(A)$, and the $T(A)$ has determinant $\det(A)^2$. □

Prop. (12.3.4.8) [Norm Form]. Define a symmetric bilinear form on $Q_F(a, b)$: $B(x, y) = \text{tr}(x\bar{y})/2$.

Thus this symmetric space has $\{1, i, j, k\}$ as an orthonormal basis. It is non-degenerate and isomorphic to $\langle 1, -a, -b, ab \rangle \cong \langle 1, -a \rangle \otimes \langle 1, -b \rangle$.

Prop. (12.3.4.9). Let $A, A'$ be two quaternion algebras over $F$, then the following are equivalent:

• $A, A'$ are isomorphic as quaternion algebras.

• $A, A'$ are isomorphic as quadratic spaces.

• $A_0, A'_0$ (12.3.4.4) are isomorphic as quadratic spaces.

Proof: Cf. [Lam, P57]. □

Cor. (12.3.4.10). $Q_F(a, -1) \cong Q_F(a, a)$.

Proof: These algebras have norm forms $\langle 1, -a, -1, -a \rangle$ and $\langle 1, -a, -a, a^2 \rangle$, which are clearly isometric quadratic spaces. □

Prop. (12.3.4.11) [Split or Division Ring]. Let $A = Q_F(a, b)$, then the following are equivalent:

1. $A \cong \text{Mat}(2, F)$.

2. $A$ is not a division algebra.

3. $A$ is isotropic as a quadratic space.

4. $A$ is hyperbolic as a quadratic space.

5. $A_0$ is isotropic as a quadratic space.

6. $(\langle a \rangle - 1)(\langle b \rangle - 1) = 0$ in $W(F)$ (or $\hat{W}(F)$, by (12.3.3.2)).

7. (Hilbert’s Criterion) The binary form $\langle a, b \rangle$ represents 1.

8. $a \in \text{Nm}_{E/F}(E^*)$, where $E = F(\sqrt{b})$. 

Proof: 4 → 5 → 3 is clear. As $Q_F(-1,1) \cong M(2,F)$, 1, 4, 6, 7 are equivalent by (12.3.1.12) and (12.3.4.9). Also 3 $\iff$ 4 as the the norm form of $A$ has determinant in $(F^*)^2$. Also 1 $\rightarrow$ 2 $\rightarrow$ 3 is clear, as $x \in A$ is invertible if $N(x) \neq 0$. Thus 1 to 7 are all equivalent.

Now we show 7 $\iff$ 8: Firstly assume $b \notin (F^*)^2$, otherwise both are true. Let $E = F(\sqrt{b})$, then $N_{E/F}(x + y\sqrt{b}) = x^2 - by^2$, thus 8 says $a \in D_F(\langle 1, -b \rangle)$, which is equivalent to $\langle 1, -b, -a \rangle$ isotropic, which is equivalent to $\langle a, b \rangle$ represents 1, by representation theorem (12.3.1.21).

Cor. (12.3.4.12). Let $a \in F^*$,
- $Q_F(1,-a) \cong Q_F(a,-a) \cong M(2,F)$.
- If $a \neq 1$, then $Q_F(a,1-a)$ splits.
- $Q_F(-1,a)$ splits iff $a$ is a sum of two squares in $F$.

Proof: These follows from Hilbert’s criterion and representation theorem (12.3.1.21).

Prop. (12.3.4.13) [Characterizing Quaternion Algebras].
- If $A \neq F$ is a simple algebra over $F$ of dimension $\leq 4$ with center $F$, then $A$ is isomorphic to a quaternion algebra over $F$.
- If $B \neq F$ is a f.d. simple $F$-algebra with center $F$ equipped with an $F$-algebra involution $x \mapsto \overline{x}$ s.t. $x + \overline{x} \in F, x\overline{x} \in F$ for any $x \in B$, then $B$ is isomorphic to a quaternion algebra over $F$.

Proof: 1: Use Wedderburn’s theorem, then $A \cong M(n,D)$ where $D$ is a division ring over $F$ with center $F$. Then $A = M(2,F) \cong Q_F(1,-1)$ or $D$. If $A = D$, choose $i \notin F$, and $K = F(i)$ a subfield of $D$. Then $F \subset K \subset D$, thus dim $K = 2$, thus we may modify $i$ that $i^2 = a \in F$. The conjugation of $i$ on $D$ satisfies $(ad(i))^2 = id$, thus $A = A^+ \oplus A^-$ where $ad(i)$ acts by 1 and $-1$ resp.. Let $j \neq 0 \in A^-$, then $ij = -ji$, $j^2i = ij^2$, thus $j^2 \in A^+$. Now $K(j)$ is also a quadratic field over $F$, thus $j^2 + cj - b = 0$ for $c,b \in F$. Then $cj = b - j^2 \in A^+ \cap A^- = 0$ shows $c = 0$. Then $A = F + FiFjFij$ is the quaternion algebra $Q_F(a,b)$.

2: Use Wedderburn’s theorem, then $A \cong \text{Mat}(n,D)$ where $D$ is a central division ring over $F$. The hypothesis shows every element of $B$ satisfies a degree 2 equation $x^2 - (x + \overline{x})x + x\overline{x} = 0$, thus $n \leq 2$. If $n = 2$, then consider the diagonal elements, then we get $D = F$. If $B = D$, then the same argument as above shows we can find $i,j$ that $ij = -ji$ and $i^2 = a, j^2 = b, a \in F^*$. Then $j$ induces an isomorphism $A^+ \cong A^-$. If there are some $l \in A^+ \setminus F(i)$, then $\overline{l} = \overline{l} = il$, thus $il + \overline{l} = 2il \in F$, contradiction. Thus $A^+ = F(i)$, and $D = \text{Mat}(a,b)$.

Prop. (12.3.4.14) [Classifying Binary Forms]. Let $q = \langle a,b \rangle, q' = \langle a',b' \rangle$ be non-singular binary forms, then they are isomorphic iff det$(q) = \text{det}(q')$ and $Q_F(a,b) \cong Q_F(a',b')$.

Proof: If $q \cong q'$, then $ab = a'b' \in F^x/(F^x)^2$, thus $\langle 1,-a,-b,ab \rangle \cong \langle 1,-a',-b',a'b' \rangle$, thus $Q_F(a,b) \cong Q_F(a',b')$ by (12.3.4.11). The converse follows the same way by cancellation theorem (12.3.2.1).

Def. (12.3.4.15) [Hilbert Symbol]. For $a, b \in k^\times$, define the Hilbert symbol

$$\{a,b\}_k = \begin{cases} 1 & Q_k(a,b) \cong \text{Mat}(2;k) \\ -1 & \text{otherwise} \end{cases}$$
Splitting Fields

Def. (12.3.4.16) [Splitting Fields]. A quaternion algebra $A$ over $F$ is said to split in a field extension $K/F$ if $A \otimes_F K \cong \text{Mat}(2, K)$. $K$ is said to be a splitting field for $A$.

Prop. (12.3.4.17). Let $A = Q_F(a, b)$ and $K = F(\sqrt{c}), c \in F^\times$, then the following are equivalent:
- $A$ splits over $K$.
- $A \cong Q_F(c, d)$ for some $d \in F^\times$.
- $K$ is a subalgebra of $A$ over $F$.

Proof: 1 \rightarrow 2: Consider the pure tensor space $A_0 \cong \langle -a, -b, ab \rangle$. If it is isotropic, then $A_0 \cong \langle -c, -d, cd \rangle$ for some $d \in F^\times$. If it is anisotropic, then because $A_K \cong \text{Mat}(2, K)$, by (12.3.4.11), there exists $x_i, y_i$ not all zero s.t.

$$-a(x_1 + \sqrt{a}y_1)^2 - b(x_2 + \sqrt{a}y_2)^2 + ab(x_3 + \sqrt{a}y_3)^2 = 0$$

Thus $x$ is orthogonal to $y$ and $N(x) + cN(y) = 0$. $y \neq 0$, because otherwise $N(x) = 0$ and $x = 0$. Thus there is an orthogonal basis \{x, y, z\}, and

$$A_0 \cong \langle N(z), N(y), -cN(y) \rangle,$$

and because $\det(A_0) = 1, N(z) \in c(K^\times)^2$, thus item 2 holds.

2 \rightarrow 3: In fact, if $i^2 = c \in A$, then $F(i) \cong K$.

3 \rightarrow 1: This follows from (2.4.3.17).

Prop. (12.3.4.18).

5 over Local or Finite Fields

References are [Quadratic Forms 3, Clark]

In this subsection, Let $F$ be a local field or a finite field, of char $\neq 2$ with a non-trivial character $\psi$.

Prop. (12.3.5.1) [W(F_q)].

- If $q \equiv 1 \bmod 4$, then $W(F_q)$ is isomorphic to $\mathbb{Z}/2\mathbb{Z}/[F^*/(F^*)^2] \cong \mathbb{Z}/2\mathbb{Z}[\mathbb{F}_2]$ as rings.
- If $q \equiv 3 \bmod 4$, then $W(F_q)$ is isomorphic to $\mathbb{Z}/4\mathbb{Z}$ as rings.

Proof: 1: In this case, $-1$ is a square, let $s$ be a non-square, then there are only three anisotropic forms: $\langle 1 \rangle, \langle s \rangle, \langle 1, s \rangle$. Thus the assertion is clear.

2: In this case, we can take $s = -1$, thus any anisotropic form must be of the form $\langle 1, \ldots, 1 \rangle$ or $\langle -1, \ldots, -1 \rangle$. As $\langle 1, 1 \rangle$ is universal by (20.1.2.7), $\langle 1, 1, 1 \rangle \cong \langle -1 \rangle$ by representation theorem (12.3.1.21), thus $4[\langle 1 \rangle] = 0$.

Prop. (12.3.5.2). Every binary quadratic form over a finite field $F_q$ is universal.

Proof: By (12.3.5.1), if $s$ is a non-square, there are essentially three quadratic forms, $\langle 1, 1 \rangle, \langle s, s \rangle, \langle 1, s \rangle$. By (20.1.2.7), these are all universal.

Cor. (12.3.5.3). Any quaternion algebra over a finite field splits, by Hilbert’s criterion (12.3.4.11).
Prop. (12.3.5.4) \([W(R)]\).
- There exists two anisotropic forms at each rank \(n\): \((1,\ldots,1)\) and \((-1,\ldots,-1)\).
- \(W(R) \cong \mathbb{Z}\).
- (Sylvester’s Law of Inertia) Two non-degenerate forms over \(R\) are equivalent iff they have the same rank and signature.
- \(\hat{W}(R) \cong \mathbb{Z}[F_2]\) as a ring.

Proof: Only 4 need a proof: It suffices to show \([\langle 1 \rangle]\) and \([\langle -1 \rangle]\) are linearly independent in \(\hat{W}(R)\), because they generate all other rings. But if \(a[\langle 1 \rangle] + b[\langle -1 \rangle] = 0\), then \(a + b = 0\) by rank reason, but when pass to \(W(F)\), \(a - b = 0\), thus \(a = b = 0\).

Prop. (12.3.5.5). Let \(\langle a_1,\ldots,a_n \rangle_F\) be a quadratic space over a non-Archimedean local field \(F\), we may assume \(a_i \in \mathcal{O}_F\). If \(\langle a_1,\ldots,a_n \rangle_{\mathcal{O}_F/p^n}\) is isotropic for all \(n\), then \(\langle a_1,\ldots,a_n \rangle_F\) is isotropic.

Proof: This is because we can find non-zero elements \(v_n \in (\mathcal{O}_F/p^n)^d\) that \(q(v_n) = 0 \in \mathcal{O}_F/p^n\), thus we can find elements \(v \in \mathcal{O}_F^d\) that \(q(v) = 0\).

Prop. (12.3.5.6) [Unique Quaternion Algebra]. If \(F \not\cong \mathbb{C}\) is a local field, then there is a unique non-split quadratic algebra over \(F\).

Proof: Cf.[Lam, P156].

Cor. (12.3.5.7). For this unique quaternion algebra \(A\), the valuation \(|N(x)|\) is a valuation of \(A\), i.e. defines the topology.

Proof: This is because \(|N(\cdot)|\) is bounded on the compact subset \(\{x||x| = 1\}\).

Prop. (12.3.5.8) [Hilbert Symbol]. Let \(F\) be a local or finite field, then the Hilbert symbol \((\cdot,\cdot)_F : F^*/(F^*)^2 \times F^*/(F^*)^2 \to \{\pm 1\}\) satisfies
- It is symmetric and bi-multiplicative for both terms.
- It is non-degenerate: if \(F \not\cong \mathbb{C}\) is a local field, for any \(y \in F^*\backslash(F^*)^2\), then there exists a \(z \in F^*\) that \((y,z)_F = -1\).
- \((a,-a) = 1\).
- If \(a(a-1) \neq 0\), \((a,1-a) = 1\).

Proof: 1: To show it is multiplicative, by (12.3.4.11), \((a,b)_F = 1\) iff \(a \in N_{E/F}(E^*)\), where \(E = F(\sqrt{b})\). Notice \(N_{E/F}(E^*)\) has index 1 or 2 in \(F^*\) by class field theory (12.4.2.9), thus \(a \mapsto (a,b)_F\) is a character of \(a\) in any case.
2: Cf.[Lam, P160].
3: By (12.3.4.12).

Prop. (12.3.5.9) [Weil]. Let \((V,B)\) be a quadratic space over a local or finite field \(F\) of dimension \(d\), \(\psi\) a non-trivial character of \(F\). Let \(V\) be identified with \(V^*\) via \((v,v^*) \mapsto \psi(-2B(v,v^*))\), denote the Fourier transform \(\mathcal{F}\) to be compatible with this identification.

Let \(F_B(v) = \psi(B(v,v))\), then for any \(a \in F^*\), then \(\varphi \ast F_{aB} \in \mathcal{S}(V)\) for any \(\varphi \in \mathcal{S}(V)\), and there is a complex number \(\gamma(aB)\) with norm 1 that for any \(\varphi \in \mathcal{S}(V)\),
\[
\mathcal{F}(\varphi \ast F_{aB}) = |a|^{-d/2} \gamma(aB) \mathcal{F}(\varphi) F_{-a^{-1}B},
\]
which means \(|a|^{-d/2} \gamma(aB) F_{-a^{-1}B}\) is formally the Fourier transform of \(F_{aB}\).
Prop. (12.3.5.10) [Analytic Interpretation of Isotropy].
- If $(V_1, B_1), (V_2, B_2)$ are quadratic spaces, then $\gamma(B_1 \oplus B_2) = \gamma(B_1) \gamma(B_2)$.
- If $(V, B)$ is a quadratic space, then $\gamma(-B) = \gamma(B)^{-1}$.
- If $(V, B)$ is a hyperbolic quadratic space (12.3.1.15), then $\gamma(B) = 1$.
- $\gamma$ is a group homomorphism $W(F) \to \mathbb{C}^*(12.3.3.1)$.

Proof: 1, 2 follow from taking test functions $\varphi$ to be $\varphi_1 \otimes \varphi_2$ or $\overline{\varphi}$. 3 follows from the fact $\gamma((-1, 1)) = \gamma((1)) \gamma((-1)) = 1$. 4 follows from 1 and 3. \qed

Prop. (12.3.5.11). Situation as in (12.3.5.9),
- For any $\Phi \in \mathcal{S}(V)$, $\int_V (\Phi \ast F_B)(v) dv = \gamma(B) \int_V \Phi(v) dv$.
- If $F$ is non-Archimedean, then for any lattice in $V$ (12.2.3.29) sufficiently large, $\gamma(B) = \int_L F_B(v) dv$.
- If $F$ is finite, then $\gamma(B) = \int_V F_B(v) dv$.

Proof: 1 follows from (12.3.5.9) evaluated at $a = 1$ and $v = 0$.
2: Consider the dual lattice $L'(12.2.3.33)$, if $L$ is sufficiently large, then $L'$ is sufficiently small, s.t. $F_B(u) = 1$ for all $u \in L'$. Then
\[
(\chi_{L'} \ast F_B)(v) = \int_{L'} F_B(v-u) du = \psi(B(v, v)) \int_{L'} \psi(-2B(u, v)) du,
\]
which equals $V(L') \chi_L F_B$. Then let $\Phi = \chi_L'$ in item 1, we get the desired assertion.
3: This is the same as 2, take $\Phi = 1$. \qed

Prop. (12.3.5.12) [Weil’s Characterization of Hilbert Symbol]. Let $Q_F(a, b)$ be a quadratic algebra over a local field $F$ of characteristic $\neq 2$, let $q : Q_F(a, b) \to F$ be the norm form, then $\gamma(q) = (a, b)_F(12.3.4.15)$.

In particular, $(a, b)_F = \gamma((1, -a, -b, ab))$.

Proof: By (12.3.5.10) and (12.3.5.8), it suffices to show for a non-split $Q_F(a, b)$, $\gamma((1, -a, -b, ab)) = -1$.

If $F$ is Archimedean or finite, then the existence of a non-split $Q_F(a, b)$ over $A$ shows $F = \mathbb{R}$, and $a = b = -1$, and $\gamma((1, 1, 1, 1)) = (\gamma((1)))^4$. Let $\psi : \mathbb{R} \to \mathbb{C} : x \mapsto e^{2\pi ix}$ as in (12.2.6.3), and $\Phi(x) = e^{-\pi x^2}$, then it can be calculated using (12.3.5.9) that $\gamma(B)$ is an 8-th roots of unity, thus we are done.
If $F$ is non-Archimedean, denote the Haar measure on $A = Q_F(a,b)$ by $dz$, and then by \((12.3.4.7)\) and \((10.9.1.19)\), the Haar measure on $A^*$ is of the form $d^\times z = |N(z)|^{-2}dz$. By \((12.3.5.7)\), for large $n$, $L = N^{-1}(p^{-n})$ is a sufficiently large lattice in $V$, thus we can use \((12.3.5.11)\) to evaluate the sign of

$$\gamma(N) = \int_{L \setminus \{0\}} \psi(N(z)) |N(z)|^2 d^\times z.$$ 

But this integrand factors through $N : L \setminus 0 \to p^{-n}$, thus it suffices to evaluate the sign of

$$\int_{p^{-n} \setminus 0} \psi(x)|x|^2 d^\times x = \int_{p^{-n}} \psi(x)|x|dx,$$

which is $-q^{1-2r}(1-q^{-1})^{-1}$, where the conductor of $\psi$ is $p^r$. So $\gamma(N) = -1$. \hfill \Box

**Cor. (12.3.5.13).** Let $r_1 \in F^*$, then $\gamma(\langle ar_1, \ldots, ar_{2n} \rangle) = ((-1)^n r_1 \ldots r_{2n}, a)_F \gamma(\langle r_1, \ldots, r_{2n} \rangle)$.

**Proof:** By \((12.3.5.12)\), it suffices to show for $n = 1$. $\gamma(\langle r_1, r_2 \rangle) = (r_1, r_2)_F \gamma(\langle 1, r_1 r_2 \rangle)$, thus also $\gamma(\langle ar_1, ar_2 \rangle) = (ar_1, ar_2)_F \gamma(\langle 1, a^2 r_1 r_2 \rangle)$, so

$$\gamma(\langle ar_1, ar_2 \rangle) / \gamma(\langle r_1, r_2 \rangle) = (ar_1, ar_2)_F / (r_1, r_2)_F = (a, -r_1 r_2)$$

by \((12.3.5.8)\). \hfill \Box

**Cor. (12.3.5.14).** Let $(V, B)$ has dimension $2n$, then $\gamma(B) = ((-1)^n \det(B), -1)_F$.

**Proof:** It reduces to $n = 1$, in which case, it suffices to show that $\gamma(\langle r_1, r_2 \rangle) = (1, r_1 r_2)_F$. But $(-1, -r_1 r_2)_F = \gamma(\langle 1, 1, r_1 r_2, r_1 r_2 \rangle) = \gamma(\langle 1, r_1 r_2 \rangle)^2$. By \((12.3.5.12)\), $\gamma(\langle 1, -r_1, -r_2, r_1 r_2 \rangle)^2 = 1$, thus $\gamma(\langle 1, r_1 r_2 \rangle)^2 = \gamma(\langle r_1, r_2 \rangle)^2$. \hfill \Box

### 6 over Global Fields

References are [Quadratic Forms over Global Fields, Clark].

**Prop. (12.3.6.1).** Let $F = k(t)$ where $k$ is alg.closed, then any binary quadratic form $Q$ over $F$ is universal.

**Proof:** We may assume $Q = \langle 1, f \rangle$, where $f \in F^*$. We can assume $f \notin -(F^*)^2$, otherwise this is clearly universal. It is easy to see that the $F_2$ vector space $F^*/(F^*)^2$ has a basis $\{t - a | a \in k\}$. Notice $D_F(Q)$ is a subgroup of $F^*$ as it is the norm group of $F(\sqrt{-f})$, it suffices to show that $t - a \in D_F(Q)$. After a change of variable, it suffices to show that $t \in D_F(Q)$, or $\langle 1, f, -t \rangle$ is isotropic, or equivalently $-f \in \langle 1, -t \rangle$ for any $f$. The same argument show that it suffices to show that $\langle 1, t, -a \rangle$ is isotropic. But $t - a + (-t) + (\sqrt{a})^2 = 0$. \hfill \Box

**Cor. (12.3.6.2).** Any quaternion algebra over $\bar{k}(t)$ splits, by Hilbert's criterion \((12.3.4.11)\).

**Prop. (12.3.6.3) [Examples].**

- $Q_\mathbb{Q}(-1, -1) \cong Q_\mathbb{Q}(-2, -3)$.
- $Q_\mathbb{Q}(-1, -1) \not\cong Q_\mathbb{Q}(-2, -5)$.
- Let $p$ be a prime number, $Q_\mathbb{Q}(-1, p)$ splits iff $p = 2$ or $p \equiv 1 \mod 4$.
- Let $p$ be a prime number, $Q_\mathbb{Q}(-2, p)$ splits iff $p = 2$ or $p \equiv 1, 3 \mod 8$. 


• $Q(−3,5)$ is a division ring, but splits over $K = Q(√17)$.

Proof: 1: By (12.3.1.23), $Q(1,1,1,1) \cong (1,1,2,2) \cong (1,3,6,2)$, thus $Q(−1,−1) \cong Q(−2,−3)$ by (12.3.4.11).

2: if they are isomorphic, then $⟨2,5,10⟩ \cong ⟨1,1,1⟩ \cong ⟨2,2,1⟩$, thus $⟨5,10⟩ \cong 1,2$, which is impossible as 1 is not representable by $⟨5,10⟩$.

3: By Hilbert’s criterion (12.3.1.23), if $Q(−1,p)$ splits, then $−x^2 + py^2 = z^2$ for some $x,y,z \in \mathbb{Z}$ that $(x,y,z) = 1$, thus $−1$ is a square in $F_p$, which means $p \equiv 1 \mod 4$ or $p = 2$. Conversely, if $p \equiv 1 \mod 4$, then by (12.2.1.1), $p = x^2 + y^2$ for some $x,y \in \mathbb{Z}$, thus $⟨−1,p⟩$ represents 1, so $Q(−1,p)$ splits. If $p = 2$, then $⟨−1,2⟩$ represents 1, thus it splits.

4: By Hilbert’s criterion (12.3.1.23), if $Q(−1,p)$ splits, then $−2x^2 + py^2 = z^2$ for some $x,y,z \in \mathbb{Z}$ that $(x,y,z) = 1$, thus $−2$ is a square in $F_p$, which means $p \equiv 1,3 \mod 8$ or $p = 2$. Conversely, if $p \equiv 1 \mod 4$, then by (12.2.1.1), $p = x^2 + y^2$ for some $x,y \in \mathbb{Z}$, thus $⟨−1,p⟩$ represents 1, so $Q(−1,p)$ splits. If $p = 2$, then it splits as above.

5: If it splits, then $−3x^2 + 5y^2 = z^2$ for some $x,y,z \in \mathbb{Z}$ that $(x,y,z) = 1$. This is a contradiction modulo 3. In $K = Q(√17)$, however, $5 \cdot 2^2 − 3 = 17$, thus $Q(√17)(−3,5)$ splits.

□

Prop. (12.3.6.4) [Hasse-Minkowski Principal]. If $q$ is a quadratic form over a global field $F$ of characteristic $\neq 2$, then $q$ is isotropic over $F$ iff $q$ is isotropic over $F_p$ for all place $p$.

Proof: Cf. [Lam, P170].

□

7 Algebraic Extensions
12.4 Cohomology of Number Fields

Main references are [Neu15], [Cohomology of Number Fields, Neukirch], http://www.math.columbia.edu/~chaoli/docs/ClassFieldTheory.html#sec28 and [Mil20].

1 Abstract Class Field Theory

Def.(12.4.1.1)[Class Formations]. A profinite formation consists of a profinite group $G$ regarded as a Galois group $G(K)$ and a $G$-module $A$. It is called a field formation iff for any normal extension $L/K$, $H^1(L/K, A^L) = 0$.

For a field extension, by (10.1.1.13), inf is an injection on $H^2$. We denote $H^2(K)$ as the profinite cohomology group $H^2(G, A) = Br(K)$. Inflation should be thought of as inclusions.

It is called a class formation if moreover for every normal extension $L◁K$, there is an canonical isomorphism $\text{inv}_{L◁K}$ that is compatible with inflation and restriction in the sense that:
- If $N/L/K$ with $N/K$ and $L/K$ normal, then $\text{inv}_{L/K} = \text{inv}_{N/K} \circ \text{res}_L = [L : K] \cdot \text{inv}_{N/K}$.
- If $N/L/K$ with $N/L$ and $N/K$ normal, then $\text{inv}_{N/L} \circ \text{res}_L = [L : K] \cdot \text{inv}_{N/K}$.

$\text{inv}_{L/K}^{-1}(1 + 1) ∈ H^2(L/K)$ is called the fundamental class $u_{L/K}$.

Prop.(12.4.1.2). $\text{inv}$ also commutes with cor and conjugation:

\[ \text{inv}_{N/K}(\text{cor}_K c) = \text{inv}_{N/L} c, \quad \text{inv}_{\sigma N/\sigma K}(\sigma^* c) = \text{inv}(c). \]

The first is because $\text{inv}$ commutes with $\text{res}$ thus $\text{res}$ is surjective, thus there is a $c'$ that $c = \text{res} c'$. Because of $\text{cor} \text{ res} = [L : K]$ we have $\text{cor}_K(c) = c' [L : K]$. Thus $\text{inv}_{N/K}(\text{cor}_K c) = [L : K] \cdot \text{inv}_{N/K}(c') = \text{inv}_{N/L}(\text{res}_L c') = \text{inv}_{N/L}(c)$.

For the conjugation, Cf.[Neu15]P69.

Cor.(12.4.1.3). From this we easily get that

\[ u_{L/K} = (u_{N/K})^{[N:L]}, \quad \text{res}_L(u_{N/K}) = u_{L/K} \]
\[ \text{cor}_K(u_{N/L}) = (u_{N/K})^{[L:K]}, \quad \sigma^*(u_{N/K}) = u_{\sigma N/\sigma K}. \]

Prop.(12.4.1.4)[Class Formation Main Theorem]. Tate’s theorem (10.1.1.24) tells us for a class formation, for $L/K$ normal extension, there is an isomorphism

\[ u_{L/K} \cup - : H^q(\text{Gal}(L/K), \mathbb{Z}) ∼= H^{q+2}(L/K). \]

Especially, for $q = -2$, there is a canonical isomorphism $\text{Gal}^{ab}(L/K) ∼= A_K/\text{Nm}_{L/K} A_L$. Its inverse is called reciprocity isomorphism and induces a norm residue symbol map $(-, L/K)$

\[ 1 → \text{Nm}_{L/K} A_L → A_K \xrightarrow{(-, L/K)} \text{Gal}^{ab}(L/K) → 1. \]

This norm residue symbols induce a universal norm residue symbol map

\[ (-, K) : A_K → \text{Gal}^{ab}_K = \lim_{L/K} \text{Gal}^{ab}(L/K) \]

that has dense image.
Lemma (12.4.1.5). Let $L/K$ be a normal extension, $a \in A_K$ and $\chi \in \text{Gal}^\text{ab}(L/K)^\vee = H^1(G(L/K), \mathbb{Q}/\mathbb{Z})$ is a character, then

$$\chi((a, L/K)) = \text{inv}_{L/K}(a \sim \delta \chi) \in \frac{1}{[L : K]}\mathbb{Z}/\mathbb{Z}.$$ 

Proof: Cf. [Neukirch CFT P71].

Prop. (12.4.1.6) [Properties of Norm Residue Symbols]. For formal field extensions $N/L/K$ with $N/K$ normal, there are commutative diagrams:

$$\begin{align*}
A_K & \xrightarrow{(-,N/K)} \text{Gal}(N/K)^\text{ab} & A_K & \xrightarrow{(-,N/K)} \text{Gal}(N/K)^\text{ab} & A_L & \xrightarrow{(-,N/L)} \text{Gal}(N/L)^\text{ab} \\
\text{id} & & \text{pr} & & \text{Nm}_{L/K} & \\
A_K & \xrightarrow{(-,L/K)} \text{Gal}(L/K)^\text{ab} & A_L & \xrightarrow{(-,N/L)} \text{Gal}(N/L)^\text{ab} & A_{\sigma L} & \xrightarrow{(-,\sigma N/\sigma L)} \text{Gal}(\sigma N/\sigma L)^\text{ab}
\end{align*}$$

Where $\text{Ver}$ is the transfer map defined in ??.

Proof: Cf. [Neukirch CFT P72].

Remark (12.4.1.7) [Non-Abelian Problems]. For a finite normal extension $L/K$, $\text{Nm}_{L/K} A_L = \text{Nm}_{L^K/K} A_{L^K}$. This is because the quotient both correspond to $G(L/K)^\text{ab}$. So class field theory doesn’t tell about non-Abelian extension.

Prop. (12.4.1.8) [Norm Groups and Abelian Extension]. The map $L \mapsto \mathcal{N}_{L/K} = \text{Nm}_{L/K} A_L$ defines an inclusion reversing isomorphism between the lattice of Abelian extension $L$ of $K$ and the lattice of norm groups of $A_K$, i.e.:

$$\mathcal{N}_{L_1 L_2/K} = \mathcal{N}_{L_1/K} \cap \mathcal{N}_{L_2/K}, \quad \mathcal{N}_{L_1 \cap L_2/K} = \mathcal{N}_{L_1/K} \cdot \mathcal{N}_{L_2/K}.$$ 

And any group that contains a norm group is a norm group.

Proof: By the first commutative diagram of inv, if $(a, L_i/K) = 0$, then $(a, L_1 L_2/K)$ is trivial on $G_{L_i/K}$, thus trivial on $G_{L_1 L_2/K}$, thus $a \in I_{L_1 L_2}$. so $I_{L_1} \cap I_{L_2} \subset I_{L_1 L_2}$, the other side is easy. the second is because $|I_{L_1 \cap L_2}/I_{L_1}| = |G_{L_1 \cap L_2/L_1}| = |G_{L_1 L_2/L_1}| = |I_{L_1} I_{L_2}/I_{L_1}|$. Also we deduce $I_{L_1} \subset I_{L_2} \iff L_2 \subset L_1$, thus by canonical isomorphism, groups containing $\text{Nm}_{L/K} A_L$ are one-to-one correspondence with middle fields of $L/K$ by counting numbers.

Remark (12.4.1.9). This shows the philosophy of CFT, i.e. the property of Abelian extensions of a field is can be read from its multiplicative group structure. Of course, determining and characterizing these norm groups requires some work.

Weil Groups

Main references are [A-T67].
2 Local Class Field Theory

Unramified Extensions

Lemma (12.4.2.1). Let $L/K$ be an unramified extension, then $H^q(G_{L/K}, U_L) = 0$ for all $q$.

Proof: Cf.[Neukirch P83].

Prop. (12.4.2.2) [Witt Residues]. The unramified extensions of $K$ form a class formation.

Proof: We first define the inv map: use the exact sequence $1 \rightarrow \mathcal{O}_L^* \rightarrow L^\times \xrightarrow{\nu_L} \mathbb{Z} \rightarrow 0$, using the lemma (12.4.2.1), we have an isomorphism

$$H^2(\text{Gal}(L/K), L^\times) \xrightarrow{\nu_L} H^2(\text{Gal}(L/K), \mathbb{Z}) \xrightarrow{\delta^{-1}} H^1(\text{Gal}(L/K), \mathbb{Q}/\mathbb{Z}) = \text{Gal}(L/K)^\vee.$$

And there is an isomorphism

$$\varphi: \text{Gal}(L/K)^\vee \cong \frac{1}{[L:K]} \mathbb{Z}/\mathbb{Z}, \quad \varphi(\chi) = \chi(\varphi_{L/K})$$

where $\varphi_{L/K}$ is the Frobenius which generates $\text{Gal}(L/K)$. Then define

$$\text{inv}_{L/K} = \varphi \circ \delta^{-1} \circ \nu_L : H^2(\text{Gal}(L/K), L^\times) \cong \frac{1}{[L:K]} \mathbb{Z}/\mathbb{Z}.$$

To verify this is a class formation, we should verify (12.4.1.1), Cf.[Neukirch P85]?

Prop. (12.4.2.3) [Local Norm Symbol is given by Frobenius]. If $L/K$ is unramified, then $(a, L/K) = \varphi_{L/K}^{v_K(a)}$. The same holds for $L$ replaces by $K^\text{ur}$, in which case

$$1 \rightarrow \mathcal{O}_K^* \rightarrow K^\times \rightarrow \text{Gal}(K^\text{ur}/K) \rightarrow 0$$

is exact. Cf[Neukirch P88].

Proof: We use (12.4.1.5), then $\chi(a, L/K) = \text{inv}_{L/K}(\pi \sim \delta \chi) = \varphi \circ \delta^{-1} \circ v_K(\pi \sim \delta \chi) = \varphi(\delta^{-1}(v_K(a)\delta \chi)) = \varphi(v_K(a)\chi) = v_K(a)\chi(\varphi_{L/K}) = \chi(\varphi_{L/K}^{v_K(a)})$, for any $\chi$. The second assertion follows from the last prop (12.4.2.4).

Cor. (12.4.2.4) [Norm Group of Unramified Extensions]. The norm group of an unramified extension of degree $f$ is

$$\mathcal{O}_K^* \times (\omega_f)_K^Z.$$

In particular, $L/K$ is unramified iff $\mathcal{O}_K^* \subset N_{L/K}$.

Ramified Extensions

Lemma (12.4.2.5). If $L/K$ is normal, then $\#H^2(L/K) \mid [L:K]$.

Proof: Cf.[Neukirch CFT P89]. Should use the fact that $G_{L/K}$ is solvable and Herbrand quotient.
Lemma (12.4.2.6) [Invariant Maps]. If \(L/K\) is a normal extension and \(L'/K\) is another unramified extension of the same degree, then \(H^2(L/K) = H^2(L'/K) \subset \text{Br}(K)\). In particular, we can define an invariant map \(\text{inv} : \text{Br}(K) \to \mathbb{Q}/\mathbb{Z}\).

Proof: In view of (12.4.2.5) and (12.4.2.2), we only need to prove \(H^2(L'/K) \subset H^2(L/K)\). For this, we let \(N = LL'\), then there is an exact sequence (10.1.1.13)

\[
1 \to H^2(L/K) \to H^2(N/K) \xrightarrow{\text{res}_L} H^2(N/L)
\]

then we only need to prove \(\text{res}_L(c) = 0\), and this follows from \(\text{inv}_{N/L}(\text{res}_L c) = 0\). This will follow, if we have

\[
\text{inv}_{N/L}(\text{res}_L c) = [L : K] \cdot \text{inv}_{L'/K} c.
\]

This follows from (12.4.2.7). \(\square\)

Lemma (12.4.2.7). For two subextensions \(L/K, L'/K\) in \(M/L\) normal with \(L'/K\) unramified extension, \(N = LL'\), for \(c \in H^2(L'/K)\),

\[
\text{inv}_{N/L}(\text{res}_L c) = [L : K] \cdot \text{inv}_{L'/K} c.
\]

Proof: Cf [Neukirch CFT P90]. \(\square\)

Lemma (12.4.2.8). \((\text{Gal}_K, (K^*)^\times, \text{inv}_K)\) forms a class formation.

Proof: This almost follows from that of unramified extensions (12.4.2.2). We verify axioms (12.4.1.1) that inf is natural and commutes with res. It is natural because it is natural on unramified extensions, it commutes with res because we can assume \(c \in H^2(L'/K)\) unramified and use (12.4.2.7). \(\square\)

Cor. (12.4.2.9) [Local Artin’s Reciprocity Law]. Let \(L/K\) be a normal extension, then the homomorphism

\[
u_{L/K} \cup - : H^q(\text{Gal}(L/K), \mathbb{Z}) \cong H^{q+2}(L/K)
\]

is an isomorphism.

Cor. (12.4.2.10). \(H^3(L/K) = 1, H^4(L/K) = \text{Gal}^{\text{ab}}(L/K) \vee\), by (10.1.1.6).

Thm. (12.4.2.11) [Artin’s Reciprocity Law]. By (12.4.1.4), cup product with the fundamental class in \(H^2(L/F)\) define an isomorphism

\[
\text{Art}_{L/F} : \text{Gal}^{\text{ab}}(L/K) \cong H^{-2}(\text{Gal}(L/K), \mathbb{Z}) \to H^0(L/K) = K^\times / \text{Nm}_{L/K} L^\times,
\]

called the Artin reciprocity map. And the reverse map is called the norm residue symbol \((- , L/K)\)

\[
1 \to \text{Nm}_{L/K} L^\times \to K^\times \xrightarrow{(- , L/K)} \text{Gal}^{\text{ab}}(L/K) \to 1.
\]

This norm residue symbols induce a universal norm residue symbol map

\[
(- , K) : K^\times \to \text{Gal}^{\text{ab}}_K
\]

with dense image.
Cor. (12.4.2.12). By (12.4.1.6), there are commutative diagrams

\[
\begin{align*}
\begin{array}{ccc}
K^\times & \xrightarrow{(-N/K)} & \text{Gal}(N/K)^{ab} \\
\downarrow \text{id} & & \downarrow \text{id} \\
K^\times & \xrightarrow{(-L/K)} & \text{Gal}(L/K)^{ab}
\end{array}
\end{align*}
\]

\[
\begin{align*}
\begin{array}{ccc}
K^\times & \xrightarrow{(-N/K)} & \text{Gal}(N/K)^{ab} \\
\uparrow \text{Nm}_{L/K} & & \uparrow \text{Nm}_{L/K} \\
L^\times & \xrightarrow{(-N/L)} & \text{Gal}(N/L)^{ab}
\end{array}
\end{align*}
\]

Where \( \text{Ver} \) is the transfer map defined in ??.

Cor. (12.4.2.13) [Quadratic Character]. Let \( L/K \) be a quadratic extension, then \( N_L/K \) is a subgroup of \( K^\times \) of order 2. Let \( \chi \) be the non-trivial character of \( K^\times \) that is trivial on \( N_E/F(E^*) \), called the \textbf{quadratic character} of \( K^\times \) attached to \( L/K \).

Prop. (12.4.2.14) [Higher Ramification Groups]. For an Abelian extension \( L/K \), the higher principal units \( U^n_K \) are mapped under the higher ramification groups of \( G_L/K \) under the upper numbering. ?

Proof: \( \square \)

Def. (12.4.2.15) [Conductors]. For an Abelian extension \( L/K \), define the \textbf{conductor} \( f_{L/K} \) to be the smallest positive integer \( n \) s.t. \( U^n_K \subset N_{L/K} \).

Cor. (12.4.2.16). For an Abelian extension \( L/K \), \( f_{L/K} = 1 \) iff \( L/K \) is unramified, by (12.4.2.4).

Characterize the Norm Groups of \( K^\times \)

Prop. (12.4.2.17) [Norm Group and Abelian Extension]. The map \( L \mapsto N_{L/K} \) defines an inclusion reversing isomorphism between the lattice of Abelian extension \( L \) of \( K \) and the lattice of norm groups of \( K^\times \), i.e.: \[
N_{L_1L_2/F} = N_{L_1/K} \cap N_{L_2/K}, \quad N_{L_1\cap L_2/K} = N_{L_1/K} \cdot N_{L_2/K}.
\]
And any group that contains a norm group is a norm group. This follows from (12.4.1.8) and (12.4.2.8).

Prop. (12.4.2.18). The norm groups are precisely the open(closed) subgroups of finite index in \( K^* \). In fact finite index is itself open because it contains \( (K^*)^n \) which is open.

Proof: One part follows from (12.4.2.17) and the fact that \( (K^*)^m \) is open (12.2.3.6). For the converse, we only need to prove \( (K^*)^m \) is a norm group. This uses Kummer theory and Cf. [Neukirch CFT P96]. \( \square \)

Prop. (12.4.2.19) [Norm Groups of Local Fields]. The norm groups of \( K^* \) are exactly the groups containing \( U^n_K \times (\pi^f) \) for some \( n, f \).

Proof: \( U^n_K \times (\pi^f) \) is a norm group because it is closed of finite index. Conversely, any norm group contains some \( U^n_K \) because it is open and contains some \( (\pi^f) \) because it is of finite index. \( \square \)

Prop. (12.4.2.20) [Weil Groups]. The universal norm residue map \( (-, K) : K^\times \to \text{Gal}_K^{ab} \) is injective because \( (K^\times)^n \) are all norm groups by (12.4.2.18), so the kernel is their intersection with is 1 by (12.2.3.6). It image is called the \textbf{Weil group} of \( K \).
12.4. COHOMOLOGY OF NUMBER FIELDS 1189

Totally Ramified Extensions

Notations (12.4.2.21).
- Use notations defined in Lubin-Tate Formal Groups3.

Prop. (12.4.2.22) [Tate Modules]. There is an isomorphism of \( O \)-modules \( \Lambda_{f,n} \cong O/\pi^nO \), Cf.[Neukirch CFT P101]. Thus the automorphism of \( \Lambda_{f,n} \) is all of the form \( u_f \) for units, isomorphic to \( U_K/U_K^n \).

So we can define a Tate module \( TG = \varprojlim \ker[\pi^n_K] \), it is a free \( O_K \)-module of rank 1.

Def. (12.4.2.23). As \( TG \) is a free \( O_K \)-module of dimension 1, and \( G_K \) acts on \( TG \), there can be attached a Lubin-Tate character \( \chi_K : G_K \to O_K^* \) by \( g(\alpha) = [\chi_K(g)](\alpha) \), this depends on \( \pi_K \), but its restriction on \( I_K \) doesn’t depend on \( \pi_K \), and is just the local CFT isomorphism composed with \( x \to x^{-1} \).

Proof: \( [\chi_K(g)] \) is, by definition, the morphism that is id on \( K^{nr} \) and \( g \) on \( L_{ur} \). So it equals \( g \) on all \( K^{ab} \) iff \( g \) is id on \( K^{nr} \), that is, \( g \in I_K \). So if \( g \in I_K \), by local CFT, \( (\chi(g))^{-1} \) corresponds to \( g \), uniquely.

Prop. (12.4.2.24). \( G_{\pi,n} \cong O_K^*/U_K^n \), thus we have \( G_\pi \cong O_K^* \). \( L_{\pi,n}/K \) is Abelian totally ramified of degree \( p^{n-1}(p - 1) \) generated by a Eisenstein polynomial with constant coefficient \( \pi \) so \( \pi \) is in the norm group.

Proof: For this, first note Galois action induce an isomorphism on \( \Lambda_{f,n} \), thus correspond to an element of \( U_K/U_K^n \) by (12.4.2.22), this is an injection because \( \Lambda_{f,n} \) generate \( L_{\pi,n} \). Then we use the canonical polynomial \( f(Z) = \pi Z + Z^p, f^n = f^{n-1}\varphi(n) \), where \( \varphi(n) \) is a Eisenstein polynomial, thus \( L_{\pi,n}/K \) is totally ramifies with \( |G_{\pi,n}| = q^{n-1}(q - 1) = |U_K/U_K^n| \), thus the result.

Prop. (12.4.2.25)[Explicit Local Norm Residue Symbol]. Now we can write the universal residue symbol little bit more explicitly. For \( a = u\pi^m \), \((a, K)\) acts by \( \varphi^m \) on \( T \) and generated by the action \((u^{-1})f \) on \( \Lambda_{f,n} \) on \( L_{\pi,n} \). Cf.[Neukirch CFT P106].

Thus the norm group of \( L_{\pi,n} \) is just \( U_K^n \) by (12.4.2.24).

Cor. (12.4.2.26)[Norm Groups of Totally Ramified Extensions]. The norm groups of the totally ramified Abelian extension is precisely the groups that contains some \( U_K^n \times (\pi) \) for some uniformizer \( \pi \). And every totally ramified Abelian extension \( L/K \) is contained in some \( L_{\pi,n} \).

Proof: For any totally ramified extension, choose a uniformizer, then its norm is a uniformizer \( \pi \) of \( K \). And \( \text{Nm}_{L/K} \) is open, thus it contains some \( U^n \). The rest follows from local CFT(12.4.2.17).

Cor. (12.4.2.27) [Maximal Abelian Extension of \( p \)-adic Local Fields]. Let \( L_\pi = \cup L_{\pi,n} = K(\Lambda_f) \), where \( \Lambda_f = \cup \Lambda_{f,n} \), then \( T \cdot L_\pi \) is the maximal extension of Abelian extension of \( K \). Hence \( G_K^{ab} = G_{T,K} \times G_\pi \). This follows immediately from (12.4.2.19).

Cor. (12.4.2.28) [Hasse-Arf]. We can prove Hasse-Arf(12.2.32) in the case where \( K \) is a local field. This is because we already know the maximal Abelian extension, and \( G(K^{ab}/T) \cong G(L_{\pi}/K) \cong \mathbb{Z}_p \) for which we know the Galois action well (12.4.2.22)(12.4.2.24), so \( i(\sigma) = v(\sigma(\alpha_n) - \alpha_n) = v([\sigma - 1](\alpha)) \), which jumps at \( U_K^n \)(the same pattern as \( K = Q_p(12.2.34) \)), thus the result.

Cor. (12.4.2.29) [Cyclotomic Fields]. When \( K = Q_p \), we can choose \( f(Z) = (1 + Z)^p - 1 \), thus \( L_{\pi,n} \) is just \( Q_p(\zeta_p^m) \). And we have \( r_f = (1 + Z)^r - 1 \), thus we have

\[
(a, Q_p(\xi_{p^m})/Q_p)(\zeta) = \zeta^r
\]

where \( a = up^m \), and \( r \equiv u^{-1} \mod p^n \).
3 Global Class Field Theory

The ideal class group \( C_F = I_F/F^* \) is a the main object of global class field theory. We will denote \( H^q(G_{L/F}, C_L) \) by \( H^q(L/F) \). \( H^2(G_{L/F}, I_L) \) is the secondary object.

**Prop. (12.4.3.1)** Let \( \mathfrak{p} \) be a prime of \( L \) lying over \( p \), then \( H^q(G, I^p_L) \cong H^q(G_{\mathfrak{p}}, L^\ast_\mathfrak{p}) \). If \( p \) is a finite unramified prime of \( L \), then \( H^q(G, U^p_L) = 1 \) for all \( q \).

**Proof:** Notice \( I^p_L = \prod_{\sigma \in G/\mathfrak{p}} L^\ast_{\sigma \mathfrak{p}} = \prod_{\sigma \in G/\mathfrak{p}} \sigma L^\ast_{\mathfrak{p}} \) is an induced module, so by (10.1.2.7), we have \( H^q(G_{\mathfrak{p}}, L^\ast_{\mathfrak{p}}) \), and similarly for \( U_{\mathfrak{p}} \), which vanish by (12.4.2.1). \( \square \)

**Cor. (12.4.3.2)**

\[
H^q(G, I_S^L) = \bigoplus_{p \in S} H^q(G_{\mathfrak{p}}, L^\ast_{\mathfrak{p}}), \quad H^q(G, I_L) = \bigoplus_p H^q(G_{\mathfrak{p}}, L^\ast_{\mathfrak{p}}).
\]

And the isomorphism is natural, by restriction to components.

**Proof:** For this, just notice \( I_L = \bigcup_S I_S^L \), then use the last proposition, notice group cohomology commutes with colimits (10.1.2.2). \( \square \)

**Cor. (12.4.3.3)** \( H^1(G, I_L) = H^3(G, I_L) = 0 \), by (12.4.2.10).

**Cor. (12.4.3.4)** An idele \( \alpha \in I_K \) is the norm of an idele \( \beta \) in \( I_L \) if each component \( \alpha_p \) is the norm of an element \( b_{\mathfrak{p}} \in L^\ast_{\mathfrak{p}} \).

**Prop. (12.4.3.5)** The decomposition commutes with inf, res and cor. Cf. [Neukirch CFT P125].

**Cyclic Extensions**

**Lemma (12.4.3.6)** For a cyclic extension \( L/K \) of order \( p \), \( C_L \) is a Herbrand module with Herbrand quotient \( h(C_L) = p \).

**Proof:**

**Prop. (12.4.3.7)** [First Fundamental Inequality]. \( (C_K : N_{K/L} C_L) \geq p \)

**Proof:**

**Prop. (12.4.3.8)** If \( K \) contains \( p \)-th roots of unity and \( L/K \) is a cyclic extension of order \( p \), then \( (C_K : N_G C_L) \leq p \).

**Proof:**

**Cor. (12.4.3.9)** [Second Fundamental Inequality]. If \( L/K \) is a cyclic extension of order \( p \), then \( (C_K : N_G C_L) = p \).

**Proof:**

**Cor. (12.4.3.10)** [Hasse Norm Theorem]. For a cyclic extension \( L/K \), an element \( x \in K^* \) is a norm iff it is locally a norm everywhere.
Proof: Use the long exact sequence for \( 1 \to L^* \to I_L \to C_L \to 1 \), we see that \( H^0(G, L^*) \to H^0(G, I_L) \) is an injection, which is
\[
0 \to K^\times / \text{Nm}_{L/K} L^\times \to \bigoplus_p K_p^\times / \text{Nm}_{L_p/K_p} L_p^\times.
\]
In fact, by (12.4.3.3), we say that this is equivalent to \( H^1(G_{L/K}, C_L) = 1 \), which is equivalent to second fundamental inequality. □

Prop. (12.4.3.11). For \( L/K \) normal extension, \( \#H^2(G, C_L)[L : K] \).
Proof: Cf. [Neukirch P137]. □

Prop. (12.4.3.12). Let \( K \) be a number field, then
\[
\text{Br}(K) = \bigcup_{L/K \text{ cyclic}} H^2(\text{Gal}(L/K), L^\times), \quad H^2(\text{Gal}_K, I_K) = \bigcup_{L/K \text{ cyclic}} H^2(\text{Gal}(L/K), I_L).
\]
Proof: Cf. [Neukirch P127]. □

Def. (12.4.3.13) [Invariant Maps]. For \( c = (c_p) \in H^2(G_{L/K}, I_L) \), define the invariant map
\[
\text{inv}_{L/K} c = \sum_p \text{inv}_{L_p/K_p} c_p (12.4.2.8).
\]

Prop. (12.4.3.14). If \( c \in H^2(G_{L/K}, L^*) \), then \( \text{inv}_{L/K} c = 0 \). Cf. [Neukirch P141].

Cor. (12.4.3.15). Now we can define the inv map for \( C_K \) when . By the exact sequence \( 1 \to L^* \to I_L \to C_K \to 1 \), we have
\[
1 \to H^2(\text{Gal}(L/K), L^*) \to H^2(\text{Gal}(L/K), I_L) \to H^2(\text{Gal}(L/K), C_L) \to H^3(G_{L/K}, L^*)
\]
The last one is 1 if \( L/K \) is cyclic, thus by this proposition, inv is defined for \( H^2(G_{L/K}, C_L) \).

Prop. (12.4.3.16). If \( L/K \) is normal and \( L'/K \) is cyclic and they have the same degree, then \( H^2(L'/K) = H^2(L/K) \subset H^2(K/K) \).

Cor. (12.4.3.17). \( H^2(K/K) = \bigcup_{L/K \text{ cyclic}} H^2(L/K) \), thus the homomorphism \( H^2(G_K, I_K) \to H^2(K/K) \) is surjective by (12.4.3.15).

Prop. (12.4.3.18). The inv map is defined for \( H^2(K/K) \), and \( \text{inv}_{L/K} : H^2(L/K) \to \frac{1}{[L : K]} \mathbb{Z}/\mathbb{Z} \) is an isomorphism for every normal extension \( L/K \).

Lemma (12.4.3.19) [Main Lemma]. The formation \((\text{Gal}_F, C_{F^*}, \text{inv}_F)\) is a class formation (12.4.1.1).
Proof: □

Thm. (12.4.3.20) [Artin’s Reciprocity Law]. By (12.4.1.4), cup product with the fundamental class in \( H^2(L/F) \) define an isomorphism
\[
\text{Art}_{L/F} : \text{Gal}^{ab}(L/F) \cong H^{-2}(\text{Gal}(L/F), \mathbb{Z}) \to H^0(L/F) = C_F / \text{Nm}_{L/F} C_L,
\]
called the Artin reciprocity map. And the reverse map is called the norm residue symbol map \((-, L/F)\)
\[
1 \to \text{Nm}_{L/F} C_L \to C_F \xrightarrow{(-, L/F)} \text{Gal}^{ab}(L/F) \to 1.
\]
This norm residue symbols induce a universal norm residue symbol map
\[
(-, F) : C_F \to \text{Gal}^{ab}_F
\]
Prop.(12.4.3.21) [Local-Global Compatibility]. For $L/F$ and $a \in I_F$:

$$(a, L/F) = \prod_p (a_p, L_{\mathfrak{p}}/K_{\mathfrak{p}}) \in \text{Gal}^\text{ab}(L/F)(12.4.11).$$

In particular, if $v \in \Sigma_F^\text{fin}$ is unramified in $L$, then

$$([\varpi_p]_v, L/F) = \varphi_{L_{\mathfrak{p}}/F_v} \in \text{Gal}_{L_{\mathfrak{p}}/F_v} \subset \text{Gal}_F.$$

Proof: Cf.[Neukirch CFT P154].

Prop.(12.4.3.22). There are commutative diagrams:

$$
\begin{array}{ccc}
C_F & \xrightarrow{(-,N/F)} & \text{Gal}(N/F)^\text{ab} \\
\downarrow \text{id} & & \downarrow \text{pr} \\
C_F & \xrightarrow{(-,L/F)} & \text{Gal}(L/F)^\text{ab} \\
\end{array}
\quad
\begin{array}{ccc}
C_F & \xrightarrow{(-,N/F)} & \text{Gal}(N/F)^\text{ab} \\
\downarrow \text{Nm}_{L/F} & & \downarrow \text{Ver} \\
C_L & \xrightarrow{(-,N/L)} & \text{Gal}(N/L)^\text{ab} \\
\end{array}
\quad
\begin{array}{ccc}
C_L & \xrightarrow{(-,N/L)} & \text{Gal}(N/L)^\text{ab} \\
\downarrow \sigma & & \downarrow \sigma^* \\
C_{\sigma L} & \xrightarrow{(-,\sigma N/\sigma L)} & \text{Gal}(\sigma N/\sigma L)^\text{ab} \\
\end{array}
$$

Where Ver is the transfer map defined in ??.

Proof: 

Cor.(12.4.3.23). By(12.4.1.8), the map $L \mapsto N_{L/F} = \text{Nm}_{L/F} C_L$ defines a inclusion reversing isomorphism between the lattice of Abelian extension $L/K$ and the lattice of norm groups of $C_F$, i.e.:

$$N_{L_1L_2/F} = N_{L_1/F} \cap N_{L_2/F}, \quad N_{L_1 \cap L_2/F} = N_{L_1/F} \cdot N_{L_2/F}.$$

And any group that contains a norm group is a norm group.

Prop.(12.4.3.24) [Existence Theorem]. The norm groups of $C_F$ are precisely the (open)closed subgroups of finite index.

Proof: Cf.[Neukirch P162] or notes taken by Chao Li.

Cor.(12.4.3.25) [The Kernel of $(-, F)$].

- If $F$ is a number field, the kernel $\cap_{L/F} N_{L/F}$ of universal norm residue symbol $(-, F)$ is exactly the connected component $D_F$ of $1 \in C_K$, which is the group of divisible elements in $C_K(12.2.5.30)$. Moreover, $(-, F) : C_F/D_F \rightarrow \text{Gal}_F^\text{ab}$ is an isomorphism.

- If $F$ is a global function field, then $(-, F)$ is injective but not surjective. In fact, there is an exact sequence(?? by etale fundamental group)

$$
0 \longrightarrow I^1_{F/F^\times} \longrightarrow I_{F/F^\times} \longrightarrow q^\mathbb{Z} \longrightarrow 0 \\
\downarrow \cong \quad \downarrow (-, F) \quad \downarrow \\
0 \longrightarrow I_{F}^\text{ab} \longrightarrow \text{Gal}_{F}^\text{ab} \longrightarrow \text{Gal}_k \cong \hat{\mathbb{Z}} \longrightarrow 0
$$

thus $C_F$ can be regarded as the Weil group of $F$. 

Proof: 1: As Gal_{F}^{ab} is totally disconnected, it must factors through D_{F}. But C_{F}/D_{F} is a profinite group, thus D_{F} is an intersection of open subgroups of finite index, thus it is in the kernel, by (12.4.3.24).

2: The map is injective because by splitting it is a product of q^{Z} and a profinite group, thus the intersection of open subgroups of finite index is trivial (12.4.3.24). To show the diagram is commutative, it suffices to show that (x, F) acts as Frob_{k}^{(x)|F} on \bar{F}: This is because on any finite unramified Abelian extension L/F, (x, F) acts via \phi_{L/F,F} by definition (12.4.2.3), and these add up to |x|_{o} as L/F is cyclic. □

Cor. (12.4.3.26). 1: If F is a number field, there is an inclusion reversing isomorphism between the lattice of Abelian extensions L/F and the lattice of closed subgroups of C_{F} containing the image of (I_{F,\infty}^{0}), by (12.4.1.8) and (12.2.5.30). To show it is surjective, notice that

4  Brauer Groups of Local and Global Fields

Prop. (12.4.4.1) [Brauer Groups of Local Fields]. For K \in L\text{Field},

- the invariant map (12.4.2.6) is a canonical injection

inv : Br(K) \hookrightarrow \mathbb{Q}/\mathbb{Z}

whose image is

\begin{align*}
\mathbb{Q}/\mathbb{Z}, & \quad K \in p\text{-LField} \\
\frac{1}{2}\mathbb{Z}/\mathbb{Z}, & \quad K = \mathbb{R} \\
0, & \quad K = \mathbb{C}
\end{align*}

- Every Azumaya algebra over K is cyclic.
- Every element of Br(K) has period equal to index.

Proof: 1: This follows from the definition of a class formation (12.4.1.1).

The rest follow from [Poonen, P25]. □

Thm. (12.4.4.2) [Hasse]. For F \in N\text{Field},

- there is a canonical exact sequence

1 \rightarrow Br(F) \rightarrow \bigoplus_{p \in \Sigma_{F}} Br(F_{p}) \xrightarrow{\text{inv}_{F}} \mathbb{Q}/\mathbb{Z} \rightarrow 0,

and in the characterization via central simple algebras??, the first map sends [D] to the family ([D \otimes_{F} F_{v}])_{v}.

- Every Azumaya algebra over K is cyclic.
- Every element of Br(K) has period equal to index.

Proof: Cf. [Neukirch P146] and [Poonen, P26]. □
5 Decomposition Law

Prop. (12.4.5.1). If \(L/F\) is an Abelian extension, then \(N_{L/K} \cap K^\times = N_{L_p/K_p}\).

Proof: For the non-trivial part, notice if \(a \in N_{L_p/L}^\times\) is a norm times a \(a \in K^\times\), then it is a norm at all primes except \(p\), thus it is also norm at \(p\) by the multiplicative definition of the inv map (12.4.3.13).

Cor. (12.4.5.2) [Ramifications]. Let \(L/K\) be an Abelian extension of global fields and \(N = \text{Nm}_{L/K} C_L\) be the norm group, then

- \(p\) is unramified in \(L\) iff \(O_{F,F}^\times \subset N_{L/F}\).
- \(p\) splits completely in \(L\) iff \(F^\times \subset N_{L/F}\).

Proof: □

Prop. (12.4.5.3) [Decomposition Law]. Let \(L/K\) is an Abelian extension of degree \(n\) and \(p \in \Sigma_F\) is an unramified place of \(F\) and \(\varpi_p\) is a uniformizer, then if \(f\) is the smallest positive integer s.t. \([\varpi_p]^f \in N_{L/F}\), then \(p\) factors in the extension \(L\) into \(r = n/f\) distinct primes of degree \(f\).

Notice to determine whether a place is ramified or not, we use conductors (12.4.5.16).

Proof: The degree the extension of \(p\) is just the order of the Frobenius automorphism of \(G_{K_p/p}\), which is just the order in \(G_{L/K} \cong C_K/\text{Nm}_{L/K} C_L\). The Frobenius of \(p\) correspond exactly to \((\ldots, 1, \pi, 1, \ldots)\) by (12.4.3.21) and (12.4.2.3), so the result follows. □

Prop. (12.4.5.4) [Unramified Kummer Extensions are Rare]. Let \(F\) be a global field or the function field of a smooth curve over an alg.closed field \(k\), and \(S \subset \Sigma_F\) be a finite set of places, and \(m \in \mathbb{Z} \cap F^\times\), then there are only f.m. Kummer extensions over \(F\) that have Galois group of exponent \(m\) and are unramified at all finite places outside \(S\).

Proof: We may add all the \(m\)-th roots of unity to \(F\). Then by Kummer theory (2.2.7.8), Kummer extensions of exponent \(m\) over \(F\) corresponds to \(F(\sqrt[m]{a})\), where \(a \in F\). But we can only add those \(a\) s.t. \(\text{ord}_v(a) \equiv 0 \mod m\) in order to get unramified extensions, so the desired Kummer extensions correspond to \(T_S = \{a \in F^\times/(F^\times)^m| \text{ord}_v(a) \equiv 0 \mod m, \forall v \in \Sigma_K \setminus S\}\).

If \(F\) is a global field, after enlarging \(S\), we may assume \(O_{K,S}\) is PID, then this group is a quotient of \(O_{K,S}^\times/O_{K,S}^{m}\), which is finite by unit theorem (12.2.5.31). If \(F = K(C)\), where \(C\) is a complete non-singular curve, then by Riemann-Roch there is an exact sequence

\[0 \rightarrow T_{\varphi} \rightarrow T_S \rightarrow (\mathbb{Z}/(m))^{\#S} \rightarrow 0\]

And for \(f \in T_{\varphi}\), \(\text{div}(f) = mD_f\) for some \(D_f \in \text{Pic}(C)[m]\). Notice \(\# \text{Pic}(C)[m] < \infty\) by (5.11.2.18), thus the theorem follows. □

Ray Class Fields

Def. (12.4.5.5) [Notations].

- A modulus \(m\) is a a formal product \(\prod_{p \in \Sigma_F} p^{e_p}\) where \(e_p \geq 0\), and \(e_p = 0\) if \(p \in \Sigma_F^C\), and \(e_p = 0, 1\) if \(p \in \Sigma_F^R\).
12.4. COHOMOLOGY OF NUMBER FIELDS

For a modulus $\mathfrak{m}$,

$$U^\mathfrak{m} = \prod_{v \in \Sigma_F, \mathfrak{e}_v = 0} \mathbb{F}_v^\times \times \prod_{v \in \Sigma_F, \mathfrak{e}_v = 1} \mathbb{R}^\times_+ \times \prod_{p \in \Sigma_F, \mathfrak{e}_p = 0, 0} \mathbb{F}_p \times \prod_{p \in \Sigma_F, \mathfrak{e}_p > 0} (1 + p^{\mathfrak{e}_p}) \subset I_F$$

and $C^\mathfrak{m}$ is the image of $U^\mathfrak{m}$ in $C_F$, which is an open subgroup of finite index.

Def. (12.4.5.6) [Ray Class Fields]. For a modulus $\mathfrak{m}$,

- $F^\mathfrak{m}$ is the Abelian extension corresponding to $C^\mathfrak{m}$ (12.4.3.24), called the ray class field of $\mathfrak{m}$.
- $J^\mathfrak{m}$ is the group of all ideals of $O_F$ relatively prime to $\mathfrak{m}$, $P^\mathfrak{m} = F^\times \cap U^\mathfrak{m}$, called the ray mod $\mathfrak{m}$.

Def. (12.4.5.7) [Ray Class Groups]. For a modulus $\mathfrak{m}$,

$$\text{Cl}_\mathfrak{m}(F) = J^\mathfrak{m}/P^\mathfrak{m} \cong C_F/C^\mathfrak{m}$$

is finite, called the ray class group of $\mathfrak{m}$.

Proof: Cf. [Neukirch CFT P176].

Prop. (12.4.5.8) [Cyclotomic Fields]. When $F = \mathbb{Q}, m \in \mathbb{Z}_+$ and $m = m \cdot \infty$, $Q_m = \mathbb{Q}(\zeta_m)$.

In particular, we can think of the ray class fields for general function fields as “generalized cyclotomic fields”.

Proof: For any $p \in \mathcal{P}$, let $m = p^{e_p} \times m'$, then $Q(\zeta_m) = Q(\zeta_{p^{e_p}})Q(\zeta_{m'})$. Notice both $N_{Q(\zeta_{p^{e_p}})/Q}$ and $N_{Q(\zeta_{m'})/Q}$ contains $(1 + p^{e_p})$ by (12.4.2.29)(12.4.2.25) and (12.4.2.4). Thus by (12.4.3.23), the $N_{Q(\zeta_{m})/Q}$ also contains $(1 + p^{e_p})$. Thus $U^\mathfrak{m}$ is contained in $Nm_{Q(\zeta_{m})/Q}I_{Q(\zeta_{m})}$.

To show the reverse inclusion, we calculate $(C_Q : C^\mathfrak{m})$. As $(C_Q : C^1_Q) = \text{Cl}(Q) = 1$,

$$(C_Q : C^\mathfrak{m}) = (U^1_Q \mathbb{Q}^\times : U^{m, \infty}_Q \mathbb{Q}^\times) = (U^1_Q : U^{m, \infty}_Q)(U^1_Q \cap \mathbb{Q}^\times : U^{m, \infty}_Q \cap \mathbb{Q}^\times) = \varphi(m) = [Q(\zeta_m) : Q].$$

Cor. (12.4.5.9) [Kronecker]. Every Abelian extension $F/Q$ is a subfield of $Q(\zeta_m)$ for some $m \in \mathbb{Z}_+$.

Def. (12.4.5.10) [Hilbert Class Fields]. The ray class field mod 1 is important, it is the Hilbert class field of $F$, denoted by $F_1$. Its Galois group is isomorphic to $C_K/C^1_K \cong J_K/P_K$ (12.4.5.7). In particular, $[F_1 : F] = h(F)$.

Conductors

Def. (12.4.5.11) [Admissible Modulus].

- For an Abelian extension of global fields $L/F$, an admissible modulus for $L/F$ is a modulus $\mathfrak{m}$ s.t. $C^\mathfrak{m} \subset \text{Nm}_{L/F}C_L$. Equivalently, $L \subset F^\mathfrak{m}$.

All subgroups of $J^\mathfrak{m}/P^\mathfrak{m}$ are called ideal groups defined mod $\mathfrak{m}$.

- If $L/F$ is an Abelian extension with an admissible modulus $\mathfrak{m}$, then $H^\mathfrak{m}_{L/F} = \text{Nm}_{L/F} J^\mathfrak{m}_L \cdot P^\mathfrak{m}_F$ is called the ideal group defined mod $\mathfrak{m}$.

Prop. (12.4.5.12). For an Abelian extension $L/F$, $\mathfrak{m}$ is an admissible modulus for $L/F$ iff $U^\mathfrak{m} \subset N_{L/F}(I_L)$. 
Chapter 12. Algebraic Number Theory

Proof: This is because \( N_{L/F} \cap K_p = N_{L_p/K_p} \) by (12.4.5.1).

Cor. (12.4.5.13). The norm subgroups of \( C_F \) are exactly those containing some \( C^m \).

Proof: This is because \( N_{L/F} A_L \) is open in \( A_K \), by (12.2.5.28), so it must contain some \( U^m \). The converse is also clear.

Def. (12.4.5.14) [Conductors]. For an Abelian extension of global fields \( L/F \), by (12.4.5.13), there is a minimal admissible modulus for \( L/F \), called the conductor of \( L/F \), denoted by \( \mathfrak{f}_{L/F} \).

Prop. (12.4.5.15) [Local and Global Conductors]. For an Abelian extension \( L/F \),

\[
\mathfrak{f}_{L/F} = \prod_{p \in \Sigma_F} \mathfrak{f}_{L_p/F_p} \quad (12.4.2.15).
\]

Proof: This follows from (12.2.5.28).

Cor. (12.4.5.16) [Conductor Detects Ramifications]. Let \( L/F \) be an Abelian extension, then \( p \in \Sigma_F \) is ramified in \( L/F \) iff \( p \mid \mathfrak{f}_{L/F} \), by (12.4.2.15).

In particular, \( F_m/F \) is unramified at all \( p \in \Sigma_F \setminus S(m) \).

Prop. (12.4.5.17). For a field \( K \), if \( S \) is a finite set of primes that contains all the infinite primes and all the primes lying above the primes dividing \( n \), and \( I_K = I_K^S \cdot K^* \), then \( C_K^S \cdot U_K^S \) is a norm group. If \( K \) contains the \( n \)-th roots of unity, then it corresponds to the Kummer extension \( T = K(\sqrt[n]{K^S}/K) \).

Hilbert Class Fields

Prop. (12.4.5.18). The Hilbert class field \( F_1(12.4.5.10) \) is the maximal unramified Abelian extension of \( F \), by (12.4.5.16).

Def. (12.4.5.19) [Hilbert Class Field Tower]. Let \( F \) be a global field, then let \( F_1 \) be the Hilbert class field of \( F \), and for any \( n \in \mathbb{Z}_+ \), let \( F_{n+1} \) be the Hilbert class field of \( F_n \), then such a series of extensions is called the Hilbert class field tower of \( F \).

Similarly for \( p \in \mathbb{P} \), we can consider the maximal Abelian \( p \)-extensions of \( F \), which gives us a series

\[
F \subset F_1^{(p)} \subset F_2^{(p)} \subset \ldots \subset F_\infty^{(p)}.
\]

Prop. (12.4.5.20). Let \( F \) be a global field, then each \( F_n \) is Galois over \( F \), and \( F_1 \) is the largest Abelian subfield of \( F_2/F \).

Proof: For the last assertion, notice that that largest Abelian subfield of \( F_2/F \) is unramified Abelian over \( F \), then use (12.4.5.18).

Prop. (12.4.5.21) [Principal Ideal Theorem]. In the Hilbert class field over \( F \), every ideal \( \alpha \) of \( F \) becomes a principal ideal.

Proof: As \( J_F/P_F \cong C_F/C_F^1 \), It suffices to show that the map \( i : C_F \to C_{F_1} \) has image in \( C_{F_1}^1 \). By the commutative diagram (12.4.3.22)

\[
\begin{array}{ccc}
C_K & \xrightarrow{(-, F_2/F)} & \text{Gal}(F_2/F)^{ab} \\
\downarrow i & & \downarrow \text{Ver} \\
C_{F_1}^1 & \xrightarrow{(-, F_2/F_1)} & \text{Gal}(F_2/F_1)^{ab} \\
\end{array}
\]

It suffices to show that \( \text{Ver} \) is trivial. Then this follows from (12.4.5.20) and (2.1.10.3).
Thm. (12.4.5.22) [Brumer]. Let \( F \) be a number field, \( p \in \mathbb{P} \), and \( t_F^{(p)} \) be the number of primes \( \ell \in \mathbb{P} \) s.t. \( p|\ell_{\mathbb{F}/\ell} \) for any prime \( \mathbb{F} \) above \( \ell \), then
\[
\dim_{\mathbb{F}_p} \mathrm{Cl}(F)/p\mathrm{Cl}(F) \geq t_F^{(p)} - 2(d - 1)
\]

Proof: \( \square \)

Prop. (12.4.5.23) [Golod-Shafarevich]. Let \( F \) be a number field of degree \( d \) and \( p \in \mathbb{P} \), if \( [F_\infty^{(p)} : F] < \infty \), then
\[
\dim_{\mathbb{F}_p} \mathrm{Cl}(F)/p\mathrm{Cl}(F) \leq 1 + 2\sqrt{d + 1}.
\]

Proof: \( \square \)

Cor. (12.4.5.24). By (12.4.5.22), if \( t_F^{(p)} \geq 2d + 2\sqrt{d + 1} \), then \( [F_\infty^{(p)} : F] = \infty \).

For example, if we take \( F = \mathbb{Q}(\sqrt{d}) \) where \( d \) is square-free with at least 8 different prime factors, then \( [F_\infty^{(p)} : F] = \infty \).

Classical Formulation

Def. (12.4.5.25) [Artin Symbols]. There is a homomorphism \( J^m \to \mathrm{Gal}(L/K) \) called the Artin symbol \( (L/K) \). On primes \( p \), it maps a prime \( p \) which is unramified by (12.4.5.11) to its local Frobenius \( \text{Frob}_p \in G_{\mathbb{K}/p} \subset G_{L/K} \). This is well-defined only up to conjugacy in \( \mathrm{Gal}(L/K) \), and thus well-defined when \( L/K \) is Abelian.

Lemma (12.4.5.26). If \( m \) is an admissible modulus for \( L/K \), the restriction to finite part defines isomorphism \( N_{L/F}/C^m \cong H_{L/F}^m/P^m \).

Proof: Cf. [Neukirch CFT P176]. \( \square \)

Prop. (12.4.5.27) [Classical Artin Reciprocity Law]. If \( L/K \) is an Abelian extension and \( m \) is an admissible modulus, then there is a commutative diagram
\[
\begin{array}{ccc}
1 & \longrightarrow & N_{L/K} \\
\downarrow & & \downarrow \\
1 & \longrightarrow & H_{L/K}^m/P^m
\end{array}
\begin{array}{ccc}
& & \longrightarrow \\
& & \longrightarrow \end{array}
\begin{array}{ccc}
C_K^{(-L/K)} & \longrightarrow & G_{L/K} \\
& \longrightarrow & \end{array}
\begin{array}{ccc}
\longrightarrow & J^m/P^m & \longrightarrow \\
& \longrightarrow & \end{array}
\begin{array}{ccc}
& & \longrightarrow \end{array}
\begin{array}{ccc}
G_{L/K} & \longrightarrow & 1
\end{array}
\]

Thus the second row is exact by (12.4.3.20), and \( \mathrm{Gal}(L/K) \cong J^m/H_{L/K}^m \).

Proof: Cf. [Neukirch CFT, P178]. \( \square \)

Prop. (12.4.5.28) [Decomposition Law]. Let \( L/F \) is an Abelian extension of degree \( n \) with an admissible modulus \( m \) (e.g. the conductor) and \( p \nmid m \). then if \( f \) is the smallest number that \( p^f \in H_{L/F}^m \), then \( p \) factors in the extension \( L \) into \( r = n/f \) distinct primes of degree \( f \).

Proof: The degree the extension of \( p \) is just the order of the Frobenius automorphism of \( G_{\mathbb{K}/p} \), which is just the order in \( G_{L/K} \cong J^m/H^m \). The Frobenius of \( p \) correspond exactly to \( p \) by (12.4.2.3), so the result follows. \( \square \)
n-th Powers


Prop. (12.4.5.29) [Grunwald-Wang]. Let $F \in \mathbb{GField}$, $n = 2^t \cdot m \in \mathbb{Z}_+$, and assume $F$ is a function field or $F(\zeta_{2^t})/F$ is cyclic. Then $a \in F$ is in $F^n$ iff $a \in F^n_v$ for a.e. $v \in \Sigma_F$.

Proof: Cf. [Chao Li's notes] or [Mil20] P229. □

Thm. (12.4.5.30) [Grunwald-Wang]. Let $F \in \mathbb{GField}$, $n = 2^t \cdot m \in \mathbb{Z}_+$, and assume $F$ is a function field or $F(\zeta_{2^t})/F$ is cyclic. Then for $S \in \Sigma_F$ finite, if for each $v \in S$, $\chi'_v$ is a character of $F^*_v$ of finite order $n_v$, then there exists a Hecke character $\chi$ of $F$ with the $\chi_v = \chi'_v$.

Proof: Cf. [Chao Li's notes] or [Mil20] P232. □

Higher Reciprocity Law


Prop. (12.4.5.31) [Quadratic Reciprocity].

Prop. (12.4.5.32) [Cubic Reciprocity].

Prop. (12.4.5.33) [Quadric Reciprocity].

6 L-Series and Density of Primes

Def. (12.4.6.1). In this subsection, for two functions $f(s), g(s) : (1, \infty) \to \mathbb{C}$, write $f \sim g$ iff $f - g$ is bounded on $(1, 1 + \varepsilon)$ for some $\varepsilon > 0$.

Def. (12.4.6.2) [Densities]. Let $F$ be a number field and $T \subset \Sigma_F^{\text{fin}}$, then $T$ is said to have

- **polar density** $m/n \in \mathbb{Q}$ if

$$\zeta_{F, T} = \prod_{v \in T} \frac{1}{1 - ||v||^{-s}}$$

satisfies $\zeta_{F, T}^n$ extends to a nbhd of $s = 1$ with a pole of order $n$.

- **Dirichlet density** $\delta$ iff

$$\sum_{p \in T} \frac{1}{(Np)^s} \sim \frac{\delta}{s - 1}.$$  

- **natural density** $\delta$ if

$$\lim_{x \to \infty} \frac{\# T \cap \{p \in \Sigma_F^{\text{fin}} | Np \leq x\}}{\# \{p \in \Sigma_F^{\text{fin}} | Np \leq x\}} = \delta.$$  

Prop. (12.4.6.3). If the polar density exists, then so does the Dirichlet density, and they are equal. If the natural density exists, then so does the Dirichlet density, and they are equal.

Thm. (12.4.6.4) [Effective Chebotarev]. Let $L/F$ be a finite Galois extension of number fields, then for any subset $C \subseteq \text{Gal}(L/F)$ that is stable under conjugation, for $X > 0$, let

$$\pi_C(X) = \{ p \in \Sigma_F | (p, L/F) \in C, ||p|| \leq C \},$$

then

$$\#\pi_C(x) = \frac{#C \cdot X}{\#\text{Gal}(L/F) \log X} + O\left( \frac{X}{\log X} \right).$$

Proof: Cf. [Lagarias and Odlysko (Algebraic Number Fields, Ed. Frohlich, 1977)]. □

Cor. (12.4.6.5) [Chebotarev]. Let $L/F$ be a finite Galois extension of number fields, then for any subset $C \subseteq \text{Gal}(L/F)$ that is stable under conjugation, let

$$T = \{ p \in \Sigma_0^F | p \text{ unramified in } L, (p, L/F) \subseteq C \},$$

then $T$ has Dirichlet density $\delta(T) = \#C / \#\text{Gal}(L/F)$.


Prop. (12.4.6.6) [Chebotarev for Function Fields]. Cf. [Sta].

Splitting of Primes

Def. (12.4.6.7) [Splitting Sets]. Let $L/F$ be a finite separable extension of global fields, let $\text{Spl}(L/F) \subseteq \Sigma_\text{fin}_F$ be the set of finite places of $F$ that splits completely in $L$. By (4.2.7.24), If $N/F$ is the Galois closure of $L/F$, then $\text{Spl}(N/F) = \text{Spl}(L/F)$.

Prop. (12.4.6.8) [Splitting in Cyclotomic Fields]. Let $L/Q$ be Galois, then $L \in \text{Q}(\zeta_m)$ for some $m \in \mathbb{Z}_+$ by (12.4.5.9), and let $\Lambda = N_{L/Q}/\mathbb{Z}_m^m \subseteq (\mathbb{Z}/(m))^*$ corresponds to $L$, then $p \in \mathbb{P}$ splits in $L$ iff $p(\text{mod } m) \in \Lambda$.

Prop. (12.4.6.9) [Frobenius]. If $L/K$ is a finite Galois extension of global fields, then $\text{Spl}(L/K)$ has Dirichlet density $1/[L : K]$.

Proof: For $v \in \Sigma_\text{fin}_F$ unramified, it splits in $L$ iff $(p_v, L/F) = \text{id}$, by (12.4.3.21). So we can use Chebotarev theorem (12.4.6.5) for $C = \{ \text{id} \}$. □

Cor. (12.4.6.10). If $L/F, L/F'$ satisfies $\text{Spl}(L/F) = \text{Spl}(L'/F)$, then $L = L'$.

Proof: The hypothesis implies that $\text{Spl}(L/F) = \text{Spl}(LL'/F) = \text{Spl}(L'/F)$, which then implies $L = LL' = L'$, by (12.4.6.9). □

Cor. (12.4.6.11). If $L/K$ is a finite separable extension of global fields s.t. $\text{Spl}(L/K)$ has Dirichlet density $[L : K]$, then $L/K$ is Galois, by (12.4.6.7).

Cor. (12.4.6.12). If $L/K$ is a finite separable extension of global fields s.t. $\text{Spl}(L/K)$ has Dirichlet density $1$, then $L = K$, by (12.4.6.7).
7 Explicit Construction of Class Fields

The explicit class field theory is the subject that tries to write the maximal Abelian extension of a field $K$ as splitting field of polynomials.

Prop. (12.4.7.1) [Known Cases].
- $\mathbb{Q}^{ab} = \mathbb{Q}(\{\zeta_m | m \in \mathbb{Z}\})$ (12.4.5.9).
- If $F = \mathbb{Q}(\sqrt{-d})$ is a quadratic imaginary field, $F^{ab}$ is given by adjoining all the torsion points of elliptic curves over $F$ with complex multiplications (13.9.8.1).
- If $F$ is a global function field, the theory of Drinfeld modules gives most Abelian extensions of $F$.
- If $K$ is a $p$-adic number field, $K^{ab}$ is given by adjoining all torsion points of Lubin-Tate formal groups over $K$ (12.4.2.27).
- If $F$ is a CM field, the complex multiplication theory gives all the Abelian extensions.
- If $F$ is a totally real field, the conjecture of Stark gives all the Abelian extensions.

8 Cohomology of Local Fields

9 Cohomology of Global Fields
12.5 Transcendental Number Theory

1 Transcendental Numbers

Prop.(12.5.1.1)[Lindemann]. If $\alpha \in \mathbb{Q}$, then $e^{\alpha} \notin \mathbb{Q}$.

Proof:

Cor.(12.5.1.2). $\pi$ and $e$ are not in $\mathbb{Q}$.

Proof: $e^{2\pi i} = 1$, and $e^1 = e$.

Prop.(12.5.1.3). If $\alpha, \beta \in \mathbb{Q}$ with $\alpha \neq 0, 1$ and $\beta \notin \mathbb{Q}$, then $\alpha^\beta \notin \mathbb{Q}$.

Proof: Cf.[Sil16] P286.

Cor.(12.5.1.4). $(\sqrt{2})^{\sqrt{2}} \notin \mathbb{Q}$.

2 Periods

Main references are [Periods, Zagier].

Def.(12.5.2.1)[Algebraic Functions]. Let $F$ be a field contained in $\mathbb{C}$, then an algebraic function of degree $d \in \mathbb{Z}_+$ in $n$ variable over $F$ is a function $f(X) \in C(\mathbb{R}^n)$ that is continuous in its domain and satisfies an equation $P(X, f(X)) = 0$ where $P \in F[X, T]$ that is of degree $d$ in $T$.

Def.(12.5.2.2)[Periods]. A period number is a complex number that is an integral combinations of real numbers of the form $\int_U f(x)dx$ where $f$ is an algebraic function over $\mathbb{Q}(12.5.2.1)$ and $U$ is a precompact connected open domain of $\mathbb{R}^n$ defined by polynomial inequalities with rational coefficients, for some $n \in \mathbb{N}$. The set of periods is denoted by $P$. The extended Period ring is defined to be $\hat{P} = \mathbb{P}[\frac{1}{2\pi i}]$.

Clearly $\overline{\mathbb{Q}} \subset P \subset \mathbb{C}$, and they form an algebra. Also, $\#P = \aleph_1$.

Prop.(12.5.2.3). In defining periods, we can even consider domains defined by inequalities by algebraic functions over $\mathbb{Q}(12.5.2.1)$ defined on a larger open subset.

Proof: If $U$ satisfies $f < a$ and $f$ satisfies a polynomial function $P(X, f(X)) = 0$, then $U$ satisfies $P(X, a) > 0$ or $P(X, a) < 0$. We can assume the first one holds, and we can isolate the part $P(X, a) > 0, f(X) < a$ and the part $P(X, a) > 0, f(X) > a$ by segments, so we are reduced to the polynomial case.

Prop.(12.5.2.4)[Algebraic Varieties]. If $X$ is a smooth variety of dimension $d$ over $\mathbb{Q}$ and $D \subset X$ a divisor with normal crossing, $\omega \in \Omega^d(X)$ vanishing on $D$, and $\gamma \in H_d(X(\mathbb{C}), D(\mathbb{C}), \mathbb{Q})$ is a singular $n$-chain with boundary in $Y(\mathbb{C})$, then the integral $\int_C \omega \in P$.

In fact, any integration on a variety over $\mathbb{Q}$ can be reduced to this case, by resolution of singularity and restriction of divisors, and any period number comes from these.

Proof: Roughly because we can represent $\gamma$ by a semi-algebraic chain.

Example(12.5.2.5).

- $\sqrt{2} = \int_{2x^2 < 1} dx \in \mathbb{P}$. 
\[ \pi = \int_{x^2+y^2<1} dx dy \in \mathbb{P}. \]
\[ \log 2 = \int_1^2 \frac{dx}{x} \in \mathbb{P}. \]

**Prop. (12.5.2.6).** For \( n \in \mathbb{Z}_+, n \geq 2, \zeta(n) \in \mathbb{P}. \)

**Conj. (12.5.2.7) [Non-Examples].** There are no natural examples of numbers proven to be non-period. \( e, 1/\pi \) and Euler-Mascheroni constant \( \gamma \) are conjectured to be non-periods. Notice \( e \) is known to be transcendental but \( \gamma \) is not known to be rational or not yet!

**Remark (12.5.2.8)[How to Distinguish Different Periods].** There may be numbers that can be written in different ways, such as
\[ \sqrt{11} + 2\sqrt{29} + \sqrt{11} - 2\sqrt{29} + \sqrt{5}. \]
But as they are both algebraic numbers we can check this by brutal force:
1. Find polynomials satisfied by them and use Euclidean division to find their common divisor, and use inequalities to bound its roots.
2. Calculate these two numbers to sufficiently high precision and use the fact two algebraic numbers of bounded degree cannot be too close to each other by Diophantine geometry.

But how to do this for periods? **Proof:** They are both equal to the expression
\[ \sqrt{11} + 2\sqrt{29} + \sqrt{11} - 2\sqrt{29} + \sqrt{5} \]
by using the equality \( \sqrt{a} + \sqrt{b} = \sqrt{a+b+\sqrt{ab}}. \)

**Conj. (12.5.2.9)[Periods Conjecture].** Any two integral representations of a period can be transformed to each other by means of cut-and-paste, change of variables and Stoke’s formula.

**Prop. (12.5.2.10)[Calabi].** We give one indication of this conjecture by proving \( \zeta(2) = \pi^2/6: \)
\[ (1 - \frac{1}{4})\zeta(2) = 1^{-2} + 3^{-2} + 5^{-2} + \cdots = \int_{(0,1)^2} \frac{1}{(1 - x^2 y^2)} dx dy. \]
But the change of variables
\[ (x, y) = \left( \frac{\sin u}{\cos v}, \frac{\sin v}{\cos u} \right) \]
has Jacobian \( (1 - x^2 y^2) \) and maps the triangle \( T = \{u, v > 0, u + v < \pi/2\} \) bijectively to \((0,1)^2\), so
\[ \int_{(0,1)^2} \frac{1}{(1 - x^2 y^2)} dx dy = \int_T dudv = \text{Vol}(T) = \pi^2/8 \]

**Def. (12.5.2.11)[Exponential Periods].** An exponential period number is a complex number that is an integral combinations of real numbers of the form \( \int_U f(x) \exp(g(x)) dx \) where \( f, g \) are algebraic functions over \( \mathbb{Q}(12.5.2.1) \) and \( U \) is a precompact connected open domain of \( \mathbb{R}^n \) defined by polynomial inequalities with rational coefficients, for some \( n \in \mathbb{N} \). The set of periods is denoted by \( \mathbb{P}_{\text{exp}}. \)

3 Periods and Differential Equations
4 Periods and L-Functions
5 Periods and Motives
13 | Arithmetic Geometry

13.1 Pseudo-Algebraically Closed Fields

References are [Field Arithmetic].

1 Hilbertian Fields
2 Haar Measures
3 Problems
4 Frobenius Fields
5 Undecidability
13.2 Diophantine Geometry

Main references are [Serre Galois Cohomology Chap2.4.5], [B-G06], [Fundamentals of Diophantine Geometry, Lang].

Arithmetic of varieties (i.e. varieties over global and local fields and more) that are not necessarily Abelian varieties are studied in this section.

1 over Local Fields
2 over Global Fields

abc-Conjecture

Conj.(13.2.2.1)[Strong abc-Conjecture, Masser-Oesterlé]. Given a global field $F$, for any $\varepsilon > 0$, there is a constant $C_\varepsilon$ that for any $a, b, c \in \mathcal{O}_F$ that $a + b = c$,

$$H_K([a, b, c]) \leq C_\varepsilon |N_{K/Q}(\prod_{p|abc} p)|^{1+\varepsilon}.$$

Proof:

□

3 Artin’s Conjecture

Def.(13.2.3.1)[Cd-Fields]. A field $K$ is called $C_d$ or for any homogenous polynomial $F(X_1, \ldots, X_n)$ of degree $d$ with coefficient in $K$ that $d^k < n$ has a non-zero solution in $K^n$.

$C_0$ fields are just alg.closed fields, $C_1$ fields are also called quasi-algebraically closed.

Prop.(13.2.3.2). Algebraic extensions of a quasi-alg.closed field is quasi-alg.closed.

Proof: For a homogenous polynomial $F(X_1, \ldots, X_n)$, its coefficient lies in a finite extension of $K$ contained in $L$, so we may assume $L/K$ is finite. Then choose a basis $\{e_1, \ldots, e_m\}$ of $L$ over $K$, then consider the function $f(x_{11}, \ldots, x_{1m}, \ldots, x_{n1}, \ldots, x_{nm}) = N_{L/K}(F(x_{11}e_1 + \ldots + x_{1m}e_m, \ldots, x_{n1}e_1 + \ldots + x_{nm}e_m))$, which is a homogenous polynomial of degree $nm$ with coefficient in $K$, because it has values all in $K$. So it has a nonzero solution in $K^{nm}$ by (5.10.2.3), Krull’s height theorem and $k$ is alg.closed. □

Prop.(13.2.3.3)[Chevalley-Warning]. Any finite field $\mathbb{F}_q$ is quasi-algebraically closed. In fact, for any system of homogenous polynomials $f_i$ of $n$ variables, if $\sum_{i=1}^r \deg f_i < d$, then the number of solutions to this equation on $\mathbb{F}_q$ is divisible by $p$, where $q$ is a $p$-power.

Proof: The number of solutions to this system is equivalent to

$$\sum_{x \in \mathbb{F}_q} \prod (1 - f_i^{q-1}(x))$$

modulo $p$.

But notice that if $i < q - 1$, then $\sum_{x \in \mathbb{F}_q} x^i = 0$ in $\mathbb{F}_q$ by (20.1.2.9), but as the degree of the highest term of $\sum_{x \in \mathbb{F}_q^n} \prod (1 - f_i^{q-1}(x))$ modulo $p$ is smaller than $n(q-1)$, some $x_i$ has power smaller than $q - 1$, thus when summed over $\mathbb{F}_q$, it vanishes. □
Remark (13.2.3.4). This may follow from the fact any smooth projective Fano variety over \( \mathbb{F}_q \) has a rational point (13.2.6.3).

Prop. (13.2.3.5) [Tsen]. Algebraic function fields of dimension 1 over an alg.closed field \( K \) is quasi-alg.closed.

Proof: By (13.2.3.2), it suffice to consider the case \( K = k(t) \) purely transcendental. for a polynomial \( F \) with coefficient in \( k(t) \), we can assume it has coefficient in \( k[t] \), then let \( \delta \) be their maximal degree. If substituted with \( X_i = \sum_{j=0}^{N} a_{ij} t^j \), the function becomes a system of \( \delta + dN + 1 \) homogeneous equation with \( n(N+1) \) unknowns \( a_{ij} \), since \( d < n \), \( \delta + dN + 1 < n(N+1) \) for \( N \) large. In this case, □

Prop. (13.2.3.6). If \( K \) is quasi-alg.closed, then \( H^2(G(K_s/K), K^*_s) = 0 \).

Proof: Cf.[Etale Cohomology Fulei 5.7.15]. □

Cor. (13.2.3.7). By this and (13.2.3.2), the condition of (10.1.2.17) are satisfied. So if \( K \) is quasi-alg.closed, then \( cd(G(K_s/K), K_s^*) = 0 \) for \( i \geq 1 \).

Prop. (13.2.3.8) [Ax-Kochen]. For any \( d \), there is a \( N_d \) that if \( p > N_d \), then any homogenous polynomial \( f(X_1, \ldots, X_n) \) of degree \( d \) with coefficient in \( \mathbb{Q}_p \) that \( d^k < n \) has a non-zero solution in \( \mathbb{Q}_p^n \).

Proof: The proof uses Model theory. □

4 Weil Heights

Def. (13.2.4.1) [Equivalent Height function]. Let \( X \) be a projective scheme, two height functions \( X(K) \to \mathbb{R} \) are called equivalent iff they differ by a bounded function.

Prop. (13.2.4.2). There is a way of constructing the Weil heights as a special case of the global heights, which are sum of local heights, Cf.[Diophantine Geometry, Chap2].

Heights of Projective Spaces

Def. (13.2.4.3) [Canonical Heights on Projective Spaces]. For a local field \( K \) with base field \( K_0 \), let \( x = (x_0, \ldots, x_n) \in K^{n+1} \), then for a normalized place \( u \) on \( K \) and a normalized place \( v \) of \( K \) that \( u|v \), suppose log(0) = -\infty and define

\[
h_u((x_0, \ldots, x_n)) = \max_i (\log |x_i|_u), \quad H_u((x_0, \ldots, x_n)) = \exp(h_u((x_0, \ldots, x_n)))
\]

\[
h_v((x_0, \ldots, x_n)) = [K_v : (K_0)_v] h_u((x_0, \ldots, x_n)), \quad H_v((x_0, \ldots, x_n)) = \exp(h_v((x_0, \ldots, x_n))).
\]

And if \( F \) is a global field over base field \( F_0 \), for \( x \in \mathbb{P}^n(F) \), define

\[
h(x) = \frac{1}{[F : F_0]} \sum_v h_v((x_0, \ldots, x_n)), \quad H(x) = \exp(h(x))
\]

- \( h_u((x_0, \ldots, x_n)) \) is invariant under finite extensions of fields \( K'/K \), thus this local height is defined on all \( K^{n+1} \).
- \( h(x) \) is well-defined.
• $h(x) \geq 0$.
• $h(x)$ is invariant under finite extensions of fields $F'/F$, thus the height is defined on all $\mathbb{P}^n(F)$.
• For $\sigma \in \text{Gal}(F/F)$, $h(\sigma(x)) = h(x)$.

These are called **canonical heights** and **multiplicative canonical heights** on $\mathbb{P}^n$.

**Proposition (13.2.4.4).** If $P_1, \ldots, P_r \in \overline{K}^n$, then

$$h_u(P_1 + \ldots + P_r) \leq h_u(P_1) + \ldots + h_u(P_r) + \varepsilon_u \log |r|_u,$$

where $\varepsilon_u = 0$ if $u$ is non-Archimedean and 1 otherwise.

**Definition (13.2.4.5) [Height of Algebraic Numbers].** For an algebraic number $\alpha \in \overline{Q}$, the height is defined to be:

$$h(\alpha) = h([1, \alpha]).$$

**Lemma (13.2.4.6).** For $\alpha \in \overline{Q} \neq 0$ and $\lambda \in \mathbb{Q}$, we have $h(\alpha^\lambda) = |\lambda|h(\alpha)$.

**Proof:** For $\lambda > 0$, this is easy. So it suffices to consider $\lambda = -1$. Notice

$$\log |\alpha|_v = \max\{0, \log |\alpha|_v\} - \max\{0, \log |1/\alpha|_v\},$$

summing over all places $v$ and use the product formula, we get the desired results.

**Lemma (13.2.4.7) [Northcott].** Let $F$ be a global field and $C > 0, d > 0$, then $\{x \in \mathbb{P}^n(F) | h(x) \leq C, \deg(x) \leq d\}$ is finite.

**Proof:** We first reduce to the case $k(x) = Q$ or $\mathbb{F}_p(t)$: for a point $x$ with $[k(x) : Q] \leq d$, consider the point $(X_0, \ldots, X_m)$ in the projective space $\mathbb{P}^m$ of forms of degree $\deg(x)$ in $n + 1$ variables corresponding to $\text{Nm}(\sum x_i T_i)$. Notice the inverse image of any closed point in $\mathbb{P}^m$ is a finite set in $\mathbb{P}^n(\overline{K})$, and the height of $h((X_0, \ldots, X_m)) \leq d! (n+1)h(x)$, so it suffices to prove for $\mathbb{P}^m(\mathbb{Q})$. In this case, we normalize a point to a unique point with integral coordinates with no common divisors, then $\max_i \log |x_i|_p = 0$ for any $p$, thus $h(x) = h_\infty(x)$, and clearly only f.m. points has bounded heights.

**Proposition (13.2.4.8) [Change of Coordinates].** Let $h_1, h_2$ be heights of $\mathbb{P}(\overline{K})$ defined w.r.t. two coordinates systems, then $h_1 \sim h_2$. Thus we can consider heights in any particular coordinates that is convenient.

**Proof:** The proof is straightforward.
And if $F$ is a global field over base field $F_0$, for $x \in \mathbb{P}^n(F)$, define

$$h^{Ar}(x) = \frac{1}{[F : F_0]} \sum_v h_v(x), \quad H^{Ar}(x) = \exp(h^{Ar}(x)).$$

Then $h^{Ar}(x), H^{Ar}(x)$ are well-defined, positive, and invariant under finite extensions of fields for the same reason as (13.2.4.3). Then they extends to the algebraic closure, called the Arakelov heights and multiplicative Arakelov heights on $\mathbb{P}^n$.

**Cor. (13.2.4.10).** The Arakelov height is the height associated to the locally bounded metrized line bundle on $\mathcal{O}_{\mathbb{P}^n}(1)$ with Fubini-Study metrics in the Archimedean places and standard metric in the non-Archimedean places, so it is equivalent to the canonical height.

**Def. (13.2.4.11)[Arakelov Heights on Matrices].** The Arakelov heights induces a height function on the Grassmannians by the canonical embedding, and for any matrix $A \in M_{n \times m}(F)$ of rank $m$, let the Arakelov heights of $A$ be defined as the height of the point in the Grassmannian $Gr_m(F)$ associated to the space spanned by the columns of $A$. And if $A \in M_{m \times n}(F)$ of rank $m$, then its Arakelov height is defined to be $H^{Ar}(A) = H^{Ar}(A^t)$.

Equivalently, it is the height of the point in $\mathbb{P}^{n-1}_m(F)$ represented by the $m \times m$-minors of $A$. And we can also define the local heights of $A$ in this form.

**Prop. (13.2.4.12).** Let $K = \mathbb{R}$ or $\mathbb{C}$ and $A \in M_{n \times m}(\overline{K})$ has rank $m$, then $H_u(A) = \det(A^*A)^{1/2}$, by Binet’s formula (2.3.10.11).

**Prop. (13.2.4.13).** Let $K$ be a local field and $A = [B, C] \in M_{n \times m}(\overline{K})$ has rank $m$, then

$$H_u^{Ar}(A) \leq H_u^{Ar}(B)H_u^{Ar}(C).$$

**Prop. (13.2.4.14).** Let $F$ be a global field and $W$ be a subspace of $F^n$ and $W^\perp \in (F^n)^* \cong F^n$ be the annihilator of $W$, then $h^{Ar}([W]) = h^{Ar}([W^\perp])$.

**Proof:** Cf.[B-G06]P68.

**Prop. (13.2.4.15).** Let $K$ be a local field and $V, W$ be subspaces of $\overline{K}^n$, then

$$h_u^{Ar}([V + W]) + h_u^{Ar}([V \cap W]) \leq h_u^{Ar}([V]) + h_u^{Ar}([W]).$$

**Proof:** Cf.[B-G06]P69.

**Prop. (13.2.4.16)[Metric on Projective Space].** Let $K$ be a local field, for a normalized place $u$ on $\overline{K}$ and a normalized place $v$ of $K$ that $u|v$, for $x, y \in (\overline{K})^n \setminus \{0\}$, define

$$\delta_u(x, y) = \frac{H_u^{Ar}(x \wedge y)}{H_u^{Ar}(x)H_u^{Ar}(y)}, \quad \delta_v(x, y)[K_u:(K_v)_{uv}],$$

then $\delta(x, y) \in [0, 1]$ by (13.2.4.15), and defines a metric on $\mathbb{P}^n(\overline{K})$, called the projective metric on $\mathbb{P}^n$. In the complex case, it is just the Fubini-Study metric.

And if $F$ is a global field over base field $F_0$, for $x, y \in \mathbb{P}^n(\overline{F})$, define

$$\delta(x) = \prod_v \delta_v(x, y)[\overline{F} : F_0].$$

**Proof:** Cf.[B-G06]P70.

**Prop. (13.2.4.17).** Let $F$ be a global field and $x, y \in \mathbb{P}^1(\overline{F})$, then

- If $O = [0, 1]$, then $H^{Ar}(x) = \frac{1}{\delta(x, O)}$.
- If $x = [1, \alpha], y = [1, \beta]$, then $\delta(x, y) = \frac{1}{H^{Ar}(\alpha)H^{Ar}(\beta)}$. 


**Weil Heights**

**Prop. (13.2.4.18).** Let $X$ be a complete variety over $K$ and $\varphi : X \to \mathbb{P}^k, \psi : X \to \mathbb{P}^l$ are two $K$-morphisms. If $\varphi^*(\mathcal{O}_{\mathbb{P}^k}(1)) \cong \psi^*(\mathcal{O}_{\mathbb{P}^l}(1))$, then the induced height function $h_\varphi - h_\psi$ is bounded on $X(K)$.

**Proof:** Let $\varphi^*(\mathcal{O}_{\mathbb{P}^k}(1)) \cong \psi^*(\mathcal{O}_{\mathbb{P}^l}(1)) \cong L$, then $L$ is very ample. Consider a basis $\{s_0, \ldots, s_n\}$ of $\Gamma(X, L)$, then it induces a closed embedding $\chi : X \to \mathbb{P}^n : x \mapsto [s_0(x), \ldots, s_n(x)]$ and $\chi^*(\mathcal{O}_{\mathbb{P}^n}(1)) \cong L$. Then it suffices by symmetry to prove $h_\varphi \sim h_\chi$.

We may assume $\varphi(X)$ is not contained in any proper linear subspace of $X$, so we can choose a basis $T_0, \ldots, T_k$ of $\varphi^*(\Gamma(\mathbb{P}^k, \mathcal{O}_{\mathbb{P}^k}(1)))$, and let $s_0, \ldots, s_k = T_0, \ldots, T_k$. Let $x \in X(K)$, let $(x_0, \ldots, x_n)$ be the coordinate of $\chi(x)$ and $(x_0, \ldots, x_k)$ the coordinates of $\varphi(x)$. Then by the formula (13.2.4.3) clearly $h_\varphi \leq h_\chi$.

For the converse, let $I$ be the homogenous ideal corresponding to $X \subset \mathbb{P}^n$, then $X$ has coordinate ring $R = K[T_0, \ldots, T_n]/I$. The $T_0, \ldots, T_k$ generates a radical ideal equal to $(T_0, \ldots, T_n)$, because they have no common zero on $X$. Now there is an integer $q$ and homogenous ideals $F_{ij}$ that

$$T_{k+i}^q - \sum_{j=0}^k F_{ij}(T_0, \ldots, T_n)T_j \in I$$

so

$$q \log |x_{k+i}|_v \leq (q - 1) \max_{j \leq n} \log |x_j|_v + \max_{j \leq k} \log |x_j|_v + C_v$$

where $C_v = 0$ unless $v$ is Archimedean. Hence

$$\max_{j \leq n} \log |x_j|_v \leq \max_{j \leq k} \log |x_j|_v + C_v \Rightarrow h_\chi \leq h_\varphi + C.$$

**Prop. (13.2.4.19) [Weil Heights].** Let $X$ be a projective variety over a number field $K$, then for each element $\mathcal{L} \in \text{Pic}(X)$, we can assign a unique Weil height $h_\mathcal{L}$, determined up to equivalence, that

- $h_{\mathcal{L}_1 \oplus \mathcal{L}_2} \sim h_{\mathcal{L}_1} + h_{\mathcal{L}_2}$.
- If $X = \mathbb{P}^n$, then $h_{\mathcal{O}(1)}$ is the height defined in (13.2.4.3).
- For any $K$-morphism $\varphi : X \to Y$ and $L \in \text{Pic}(Y)$, $h_{\varphi^*(\mathcal{L})} \sim h_L \circ \varphi$.

**Proof:** The uniqueness follows from the fact that Pic($X$) is generated by very ample line bundles because $X$ is projective. For the existence, we may take item 3 as definition, extend it to all Pic($X$), and it is essential to verify item 1.

Let $L_1 = \varphi^*(\mathcal{O}(1)), L_2 = \psi^*(\mathcal{O}(1))$, where $\varphi : X \to \mathbb{P}^k, \psi : X \to \mathbb{P}^l$. Denote $\sigma : \mathbb{P}^k \times \mathbb{P}^l \to \mathbb{P}^{kl+k+l}$ the Segre embedding, then $L_1 \otimes L_2 \cong \chi^*(\mathcal{O}_{\mathbb{P}^{kl+k+l}}(1))$ where $\chi : X \xrightarrow{(\varphi, \psi)} \mathbb{P}^k \times \mathbb{P}^l \xrightarrow{\sigma} \mathbb{P}^{kl+k+l}$. And we check $h_\chi \sim h_\varphi + h_\psi$.

**Thm. (13.2.4.20) [Northcott].** Let $X$ be a projective variety over a global field $F$ and let $h_c$ be a height function associated to an ample class $\mathcal{L} \in \text{Pic}(X)$, then the set

$$\{P \in X(K) | h_\mathcal{L}(P) \leq C, [K(P) : K] \leq d\}$$

is finite for any constant $C, d$. 
Proof: There is a $m > 0$ that $mc$ is very ample. Because $mh_L$ is the height function associated to $mL$, we can assume that $L$ is very ample, thus reducing to $X = \mathbb{P}^n$ and $L = \mathcal{O}(1)$ by (13.2.4.19). This follows from (13.2.4.7).

**Prop. (13.2.4.21).** Let $X$ be a projective smooth variety over $F$ and $c \in \text{Pic}(X)$ an ample line bundle, $c' \in \text{Pic}^0(X)$, then

$$h_{c'} = O(|h_c|^{1/2} + 1).$$

Proof: By base change of fields, we may assume $X$ has a rational point $P_0$. Consider the double Picard map $\varphi : X \to \text{Pic}^0(X) = \hat{A}$. Viewing $c'$ as a rational point of $A$, consider $c'' = (p_A)c' \in \text{Pic}(A)$, then $\varphi^*(c'') = (id \times \varphi)^*(p_A)|_{c'} = (p_X)c' = c'$. Thus $h_{c'} \sim h_{c''}$.

Let $\hat{c}$ be an even ample line bundle on $\hat{A}(13.5.1.27)$, then for for some $n$ large, $nc - \varphi^*(\hat{c})$ is base-point-free, thus by (13.2.4.19), $h_{\hat{c}} \circ \varphi = O(|h_c| + 1)$. Thus it suffices to prove for $c', c$ changed to $c'', \hat{c}$, which is true by (13.5.12.11).

**Prop. (13.2.4.22) [Weil Heights in Intersection Theory].** Cf. [B-G06]P44?

**Bounded Sets**

**Def. (13.2.4.23) [Bounded Sets].** Let $K$ be a field and $\cdot | $ a valuation on its alg.closure $\overline{K}$, $X$ be a variety over $K$. Then:

- If $X$ is an affine variety, then a subset $E \subset X(\overline{K})$ is called **bounded** if for any $f \in K[X]$, $|f|$ is bounded on $E$.
- If $X$ is arbitrary, then a subset $E \subset X(\overline{K})$ is called **bounded** if there is a finite open affine covering $U_i$ of $X$ and sets $E_i \subset U_i(\overline{K})$ that $E_i$ is bounded in $U_i$ and $E = \cup E_i$.

**Prop. (13.2.4.24) [Properties of Bounded Sets].**

- For a bounded set $E$ in $X$ and any finite open affine covering $U_i$ of $X$, there is a division of $E$:

$$E = \cup E_i, \ E_i \subset U_i(\overline{K})$$

and $E_i$ being bounded in $U_i$.
- If $E$ is bounded in $X$ and $Y$ is a closed subscheme of $X$, then $E \cap Y(\overline{K})$ is bounded in $Y$.
- The image of a bounded set under a morphism is also bounded.
- $\mathbb{P}^n(\overline{K})$ is bounded in $\mathbb{P}^n$.
- The inverse image of bounded set under a proper morphism is bounded. In particular, if $X$ is a complete variety over a field $K$, then $X(\overline{K})$ is bounded in $X$.

Proof: 1: Because $X$ is separated, it suffices to prove for $X$ affine. And we can also take a refinement of the covering, thus assuming $U_i = X_{h_i}$. Suppose $\sum g_i h_i = 1$, and let $E_i = \{P \in E||h_i(P)| = \max_k |h_k(P)|\}$, then $E_i \subset U_i(\overline{K})$. To show $E_i$ is bounded in $U_i$, it suffices to show $|1/h_i|$ is bounded in $E_i$. But this is clear, because $|g_i|$ is bounded on $E$.

2: Use local coordinates.

4: Use the affine open covering $X_i = \{x_i \neq 0\}$, and let $E_i = \{|x_i| = \max_{j=0,...,n} |x_j|\}$, then clearly $E_i$ is bounded in $X_i$.

5: Cf. [Diophantine Geometry, P55], may use Chow’s lemma?.
Prop. (13.2.4.25) [M-Bounded]. We can define the notion of M-boundedness similar to that of (13.2.4.23), where M is a set of places on K that for any α ≠ 0 ∈ K, only f.m. of M have nontrivial valuation. Then (E^u) is said to be M-bounded in an affine variety X if for any f ∈ K[X],

\[ C_v(f) = \sup_{u \in M; u|v} \sup_{P \in E^u} |f(P)|_u \]

is finite for any v ∈ M_K and C_v(f) > 1 for only f.m. v.

Then similar properties as in (13.2.4.24) hold for M-bounded sets.

Def. (13.2.4.26). A real function f on X(\overline{K}) is called locally bounded if f(E) is bounded for every bounded set E in X.

Distance Functions

Def. (13.2.4.27) [Distance Function]. Let C be a complete curve over a valued field K = \overline{K}, let for P, Q ∈ C(K), the v-adic distance function \( d_v(P; Q) \) be defined to be \( d_v(P; Q) = \min(|t_Q(P)|^{1/e}_v, 1) \), where \( t_Q \) is a function with only one zero of order e at Q.

To understand this definition, it is just same as the pullback of the local height via \( t_Q \). It is a special case of local heights.

Prop. (13.2.4.28). Let C be a complete curve over a valued field K and F ∈ K(C), then

\[ \lim_{P \in C(K), d_v(P, Q) \to 0} \frac{\log |F(P)|_v}{\log d_v(P; Q)} = \text{ord}_Q(F). \]

Proof: In taking limit, scaling \( t_Q \) by a constant doesn’t matter, so If we change \( h_{\mathcal{O}(-Q)} \) to \( h_{\mathcal{O}(-kQ)}^{1/k} \), the limit won’t change, so we will do so and assume k is large enough s.t. there is a function that has only zeros at P of order k, so \( f^*\mathcal{O}(1) = O(-kP) \), and thus we may change O(kP) to \( f^*\mathcal{O}(1) \) and then we see \( f^{\text{ord}_Q(F)}/F^k \) is regular and non-vanishing at Q, thus we can easily get the desired result.

Prop. (13.2.4.29). If \( \varphi : C_1 \to C_2 \) is a non-constant map of curves over a valued field K, then for \( Q \in C_1 \),

\[ \lim_{P \in C(K), d_v(P, Q) \to 0} \frac{\log d_v(\varphi(P), \varphi(Q))}{\log d_v(P; Q)} = e_Q(\varphi). \]

Proof: Similar as that of (13.2.4.28). In fact (13.2.4.28) can be derived from this one.

Metricized Line Bundles

Chevalley-Weil Theorem

Prop. (13.2.4.30) [Local Chevalley-Weil]. Let K be a non-Archimedean valued field. Let \( \varphi : Y \to X \) be a finite unramified morphism of K-varieties and E a bounded set in X(\overline{K}). Then there is an \( \alpha \neq 0 \in \mathcal{O}_K \) that \( \alpha \in \delta_{P/Q} \) whenever \( P \in Y(\overline{K}) \) and \( Q = \varphi(P) \in E \).

Proof: An unramified map is locally of the form a closed embedding of a standard étale morphism \( ?, \) thus there are f.m. \( U_i, V_i \) covering \( X, Y \) respectively that \( V_i \to U_i \) is closed embedding \( V_i \to W_i \) of a standard étale morphism \( W_i \to U_i \). Because \( \varphi \) is finite hence proper, \( \varphi^{-1}(E) \) is
bounded by (13.2.4.24), thus there is a decomposition of $\varphi^{-1}(E)$ into bounded sets $E_i' \subset V_i$. Then it suffices to prove for standard étale morphisms, because we can then multiply them.

The image of $E_i$ in $W_i$ is also bounded. Let $W_i \to U_i : \text{Spec}(A[t]/f) \to \text{Spec} A$, where

$$f = t^d + a_1 t^{d-1} + \ldots + a_d, \quad a_i \in A.$$ 

By boundedness, there is an $a \neq 0 \in R$ that

$$\max_{i=1,\ldots,d} \sup_{P\in E_i'} |a_i(\varphi(P))| \leq |a|^{-1}.$$ 

Then $\xi = at_P$ is a root of the polynomial

$$g_Q(t) = t^d + aa_1(Q)t^{d-1} + \ldots + a^d a_d(Q),$$

and it is easily verified that $|\xi| \leq 1$ thus $\xi \in R_P$. Now let $g_\xi$ be the minimal polynomial of $\xi$ over $\overline{K}(Q)$, then $g_\xi = g_\xi h$, $h \in \overline{K}(Q)[t]$. By Gauss lemma in fact $g_\xi h \in \hat{R}_Q[t]$.

Now the elements $1, \xi, \ldots, \xi^{d-1}$ form a basis of $\overline{K}(P)/\overline{K}(Q)$, so the discriminant $D_{g_\xi} \in \overline{\delta_{K(P)/\overline{K}(Q)}}$. By ?? and (4.2.7.33), $|D_{g_\xi}| = |N_{K(P)/\overline{K}(Q)}(g'_\xi(\xi))| = |g'_\xi(\hat{\xi})|$. But

$$g'_\xi(\xi)h(\xi) = g'_\xi(\xi) = a^{-d-1}f'_\xi(\xi) = a^{-d-1}f'_\xi(t_P) = a^{-d-1}f'(P).$$

Because $f'$ is unit, we have $|D_{g_\xi}|$ is bounded on $E'$. So there is an $\alpha \neq 0 \in R$ that $|D_{g_\xi}| \geq |\alpha|$, independent of $P$. Then we are done, as $D_{g_\xi} \in \delta_{\overline{K(P)/\overline{K}(Q)}}$.

Lemma (13.2.4.31) [Global Chevalley-Weil]. Let $\Sigma$ be a set of discrete valuations of a field $F$ that any element $\alpha$ has only f.m. nonzero valuations, $\varphi : Y \to X$ be an unramified finite $F$-morphism of complete $K$-varieties, and $(E^u)_{u \in \Sigma}$ is an $\Sigma$-bounded family in $X$ (13.2.4.25), then for every $v \in \Sigma$ there is a nonzero $\alpha_v \in \mathcal{O}_{F,v}$ that $\alpha_v \in \overline{\delta_{P/Q}}$ whenever $u|v$ and $P \in \overline{Y(K)}$ with $\varphi(P) = Q \in E^u$. Moreover, $\alpha_v = 1$ for a.e. $v \in \Sigma$.

Proof: The proof is exactly the same as that of (13.2.4.30), noticing that $a, \alpha$ depend only on $v$ but not $u|v$, and also $a = \alpha = 1$ for a.e. $v$. □

Lemma (13.2.4.32) [Global Chevalley-Weil Theorem for Discrete Valuations]. Let $\Sigma_K$ be a set of discrete valuations of a field $K$ that any element $\alpha \in K^*$ has only f.m. nonzero valuations, $\varphi : Y \to X$ be an unramified finite $K$-morphism of complete $K$-varieties, then there are a finite set $S \subset M_K$ and for any $v \in S$ a nonzero element $\alpha_v \in \mathfrak{m}_v$ s.t. for any $P \in \overline{Y(K)}, Q = \varphi(P)$ and any place $w_0|v$ of $K(Q), K(P)/K(Q)$ is unramified outside $S$ and if $v \in S$, $\alpha_v \in \overline{\delta_{P/Q}}$.

Proof: We may assume $\varphi$ is surjective because it is closed (finite is proper). Notice $X(\overline{K})$ is $M$-bounded in $X$ (13.2.4.24), where $M$ is the set of valuations of $\overline{K}$ extending that of $M_K$. Then we can use global Chevalley-Weil theorem (13.2.4.31) to find elements $\alpha_v$ for $v \in M_K$. Now notice

$$\overline{\delta_{P/Q}} = \prod_{w|w_0} (\overline{\delta_{P/Q}} \cap \mathcal{O}_{Q,v})$$

by (4.2.7.36), and the number of $w \in M_K(P), w|w_0$ is bounded by $[K(P) : K(Q)]$, which is further bounded by $\deg(f)$ as in (13.2.4.30). Hence we can take $\alpha_v = \alpha_v^{\deg(f)}$ to finish the proof. □
\textbf{Prop. (13.2.4.33).} Let $F$ be a global field or the function field of a non-singular curve over a field $k$, and let $\phi : Y \to X$ be a finite unramified morphism of $F$-varieties. If $X$ is complete, then there is an $\alpha \neq 0 \in \mathcal{O}_F$ that for any $P \in X(F)$ that $Q = \phi(P)$, the discriminant $\delta_{P/Q}$ contains $\alpha$.

\textit{Proof:} By (5.11.1.14), we can use the above lemma (13.2.4.32) to $\Sigma = \Sigma_F$. Notice because $\delta_{P/Q} = \prod_{v \in \Sigma_E} (\delta_{P/Q} \cap \mathcal{O}_X,Q)$, we can assume $\alpha_v \in \mathcal{O}_X,Q$, then take $\alpha = \prod_{v \in \Sigma} \alpha_v$. \hfill \Box

\textbf{Thm. (13.2.4.34) [Chevalley-Weil].} Let $F$ be a global field or the function field of a non-singular curve over a field $k$, $\phi : Y \to X$ be a finite unramified morphisms of $F$-varieties. If $X$ is complete, then there is a finite extension $L/K$ that $P \in Y(L)$ for any $P \in Y(K)$ that $\varphi(P) \in X(K)$.

\textit{Proof:} By Chevalley-Weil theorem (13.2.4.33), there is an $\alpha \in \mathcal{O}_F$ that $\alpha \in \delta_{P/Q}$ for any $P \in Y(F^\text{}\text{a})$ that $\varphi(P) \in X(K)$, thus $K(P)/K(Q)$ is unramified outside $S(\alpha)$. But then (12.2.4.21) shows there are only f.m. possibilities of $k(P)$. Thus we are done. \hfill \Box

5 Diophantine Approximations

\textbf{Thm. (13.2.5.1) [Roth].} Let $K$ be a number field with a set $S$ of f.m. places including all the Archimedean ones, and for each $v \in S$ a $K$-algebraic number $\alpha_v \in K_v$. Then for any $\varepsilon > 0$, there are only f.m. $\beta \in K$ that

$$\prod_{v \in S} \min(1,|\beta - \alpha_v|_v) \leq H(\beta)^{-2+\varepsilon}$$

Moreover, $\alpha_v$ can be $\infty$ as well, in the sense that $|\beta - \alpha_v|_v = |\beta|_v^{-1}$.

\textbf{Remark (13.2.5.2).} This theorem is ineffective in the sense it doesn’t give a maximal bound on $H(\beta)$ for a solution $\beta$, but it is effective in the sense it gives a bound for the number of solutions.

\textbf{Remark (13.2.5.3).} This is not true for function fields, as if we choose $K$ to be the splitting field of the separable polynomial $x^q - x + t$ over $\mathbb{F}_p(t)$, then there is a valuation $w$ over the valuation $v$ corresponding to $(t)$ s.t. $K_w = \mathbb{F}_p((t))$, and $\alpha = t + t^q + t^{q^2} + \ldots$. Take $\beta_k = t + t^q + \ldots + t^{q^k}$, then $|\beta_k - \alpha|_v = c^{-q^{k+1}}$ with $H(\beta_k) = c^{q^k} = H(\beta)^{-q}$, thus cannot have a Roth’s theorem.

\textit{Proof:} \hfill \Box

\textbf{Cor. (13.2.5.4) [Classical Roth’s Theorem].} For any $\alpha \in \mathbb{Q}$ and $\varepsilon > 0$, there are only f.m. $p/q \in \mathbb{Q}$ s.t. $|p/q - \alpha| \leq |q|^{-2-\varepsilon}$.

\textit{Proof:} Take $K = \mathbb{Q}$, $S = \{\infty\}$ and $\alpha_{\infty} = \alpha$, then use Roth’s theorem (13.2.5.1). \hfill \Box

\textbf{Cor. (13.2.5.5).} For an element $\alpha \in \mathbb{Q}_p$ and $\varepsilon > 0$, there are only f.m. $n \in \mathbb{Z}$ s.t. $|n - \alpha|_p \leq |n|^{-1+\varepsilon}$.

\textit{Proof:} Take $K = \mathbb{Q}$, $S = \{\infty, p\}$ and $\alpha_{\infty} = \infty$, $\alpha_p = \alpha$, then use Roth’s theorem (13.2.5.1). \hfill \Box

\textbf{Cor. (13.2.5.6) [Thue’s Equation].} Let $F(x,y) \in \mathbb{Z}[x,y]$ be a homogenous polynomial that has at least three different linear factors in $\mathbb{Q}[x,y]$, then for any $m \in \mathbb{Z}^\times$, there are only f.m. solutions of $F(x,y) = m$ in $\mathbb{Z}^2$.

\textit{Proof:} Let $F_1, \ldots, F_r$ be non-isomorphic irreducible polynomials in $\mathbb{Z}[x,y]$ dividing $F$, suppose there are i.m. solutions to $F(x,y) = m$, then there are i.m. rational points $x_n/y_n$ converging but not equal to a root of $F_i$ for each $i$. Thus $r = 1$, and $\deg F_1 \geq 3$ by hypothesis. And we easily get that $|x_n/y_n - \alpha| \leq C|y_n|^{-3}$ for all $n$ and some constant $C$, contradicting Roth’s theorem (13.2.5.4). \hfill \Box
Cor. (13.2.5.7) [Another Interpretation]. Let $K$ be a global field and $v$ a valuation of $K$, $C$ be a complete curve over $K$ and $Q \in C(K)$, then for $f \in K(C)^*$,

$$
\lim_{P \in C(K), d_v(P) \to 0} \frac{\log d_v(P; Q)}{\log H_K(f(P))} \geq -2.
$$

Proof: Replacing $f$ by $1/f$ if necessary, we can assume $f(Q) \neq \infty$. Let $f - f(Q)$ has order $e$ at $Q$, then by (13.2.4.28),

$$
\lim_{P \in C(K), d_v(P) \to 0} \frac{\log |f(P) - f(Q)|_v}{\log d_v(P, Q)} = e.
$$

And Roth’s theorem implies

$$
H_K(f(P))^{2+\varepsilon}|f(P) - f(Q)|_v \geq 1
$$

for a.e. $P$. Thus by taking limit and varying $\varepsilon$, the conclusion follows. \(\square\)

Prop. (13.2.5.8) [Dirichlet]. Let $\alpha \in \mathbb{R}\setminus\mathbb{Q}$, then there are infinitely many $p/q \in \mathbb{Q}$ s.t. $|p/q - \alpha| \leq 1/q^2$.

Proof: For $N > 0$, consider the sets $\{\{q\alpha\}\ | q = 0, \ldots, N\}$, where $\{\beta\}$ are the fractional part of $\beta$. Then by pigeonhole principle gives two $0 \leq q_1 < q_2 \leq N$ s.t. $|(q_1 - q_2)\alpha - p| \leq 1/N \leq (q_2 - q_1)$. Let $q = q_2 - q_1$, then $|p/q - \alpha| \leq 1/q^2$. \(\square\)

Remark (13.2.5.9) [Hurewitz]. In fact $1/q^2$ can be changed to $1/\sqrt{5}q^2$, and this bound is the best possible.

Proof: [G. H. Hardy and E. M. Wright. An introduction to the theory of numbers] Thm194. \(\square\)

Prop. (13.2.5.10) [Liouville]. Let $\alpha \in \overline{\mathbb{Q}}$ have degree $d \geq 2$ over $\mathbb{Q}$, then there is a constant $C > 0$ s.t. for all $p/q \in \mathbb{Q}$, $|p/q - \alpha| \geq C/q^d$. Notice only the $d = 2$ case is not covered by Roth’s theorem (13.2.5.4).

Proof: We can assume $\alpha \in \mathbb{R}$, because otherwise $C = \text{Im} \alpha$ works. Let $f(T) \in \mathbb{Z}[T]$ be a minimal polynomial of $\alpha$ over $\mathbb{Q}$, then $f$ has no roots in $\mathbb{Q}$. Suppose $C_1$ is the maximum of $|f(t)|$ for $t \in [\alpha - 1, \alpha + 1]$. Suppose $|p/q - \alpha| \leq 1$, then $|f(p/q)| = |f(p/q) - f(\alpha)| \leq C_1|p/q - \alpha|$, and also $q^df(p/q) \in \mathbb{Z}$ thus $|q^df(p/q)| \geq 1$. Thus we get $|p/q - \alpha| \geq 1/C_1q^d$. Thus for general $p/q$, $C = \min(C_1^{-1}, 1)$ works. \(\square\)

Warning’s Problem

Def. (13.2.5.11) [Warning’s Problem]. For $k \geq 1$, let $g(k)$ be the smallest number s.t. every positive integer is a sum of at most $g(k)$ positive $k$-th powers.

Prop. (13.2.5.12). $g(k) \geq \lceil \frac{k^2}{2} \rceil + \lceil \frac{3k}{2} \rceil - 2$.

Proof: This is because the number $\lceil \frac{3k}{2} \rceil 2^k - 1$ requires $\lceil \frac{3k}{2} \rceil$ powers $2^k$ and $2^k - 1$ powers $1^k$. \(\square\)

Prop. (13.2.5.13) [Dickson-Niven-Pillai-Rubugunday].

$$
g(k) = \begin{cases} 2^k + \lceil \frac{3k}{2} \rceil - 2, & \text{if } \lceil \frac{3k}{2} \rceil - \lceil \frac{3k}{2} \rceil \geq \lceil \frac{3k}{2} \rceil \ 0 \ \text{otherwise} \end{cases}
$$

In particular, $g(1) = 1, g(2) = 4, g(3) = 9, g(4) = 19.$
Cor. (13.2.5.14) [Hilbert]. \( g(k) < \infty \) for any \( k \in \mathbb{Z}_+ \).

Cor. (13.2.5.15) [Mahler]. \( g(k) = 2^k + \lceil (\frac{3}{2})^k \rceil - 2 \) a.e. \( k \).

Proof: Apply Roth’s theorem (13.2.5.1) with \( K = \mathbb{Q} \), \( S = \{ \infty, 2, 3 \} \) with \( \alpha_\infty = 1, \alpha_2 = \infty, \alpha_3 = 0 \), and \( \beta_k = 3^k/n2^k \) with \( n = \lceil (\frac{3}{2})^k \rceil \). Then \( |\beta - \alpha_2|_2 \leq 2^{-k}, |\beta - \alpha_3|_3 \leq 3^{-k}|n|_3^{-1} \), and \( H(\beta_k) = 3^k|n|_3 \). Thus Roth’s theorem says for any \( \varepsilon > 0 \),

\[
|1 - 3^k/n2^k|_\infty \leq 2^k3^k|n|_3(3^k|n|_3)^{-2-\varepsilon}
\]

holds for only f.m. \( k \). Which implies that \( \lceil (\frac{3}{2})^k \rceil - (\frac{3}{2})^k \geq 3^{-\varepsilon k} \) holds for a.e. \( k \). Thus we can apply (13.2.5.13).

Remark (13.2.5.16). Notice it is not known for how large \( k \) this is true, due to the ineffectiveness of the proof of Roth’s theorem (13.2.5.1).

6 Rational Points

Prop. (13.2.6.1) [Esnault]. Let \( p \in \mathbb{P}, q \in p^{\mathbb{Z}}, X \in \text{SmProjVar} / \mathbb{F}_q \) s.t. \( \text{CH}_0(X_{\overline{\mathbb{F}_q}}) = \mathbb{Z} \), then \( \#X(\mathbb{F}_q) \equiv 1(\text{mod } q) \). In particular, \( X \) has a rational point.

Proof: Cf. [Weil 1 Proof].

Cor. (13.2.6.2). Any rationally chain connected varieties over a finite field \( k = \mathbb{F}_q \) s.t. \( \text{CH}_0(X_{\overline{\mathbb{F}_q}}) = \mathbb{Z} \), then \( X(K) \equiv 1 \mod q \). In particular, \( X \) has a rational point.

Cor. (13.2.6.3) [Manin-Lang]. If \( X/\mathbb{F}_q \) is a smooth projective Fano variety, then \( X(K) \equiv 1 \mod q \).

Proof: This is because by (5.10.4.4), any Fano variety is rationally chain connected.

Hilbert’s 10-th Problem

Conj. (13.2.6.4) [Hilbert’s 10-th Problem]. Let \( K \) be a global number field, \( X \) be a projective scheme over \( \mathcal{O}_K \), it there an algorithm to determine in a finite number of operations whether this curve has a \( K \)-rational point.

Proof:

Remark (13.2.6.5) [Mazur-Rubin]. If the BSD conjecture holds for all elliptic curves over any number fields, then Hilbert’s 10-th problem has a negative answer for any number field.

Proof:
7 Geometry of Numbers

Minkowski’s Second Theorem

Cf.[B-G06].

Prop. (13.2.7.1)[Minkowski’s Second Theorem]. Let $F$ be a global number field of degree $d$, $V$ a f.d. $F$-vector space of dimension $n$, and $\Lambda$ a lattice in $V$. For any $v \mid \infty$, let $S_v$ be a non-empty open convex symmetric bounded subset $S_v$ of $V_v$. For $\lambda > 0 \in \mathbb{R}$, denote $\lambda S = \prod_{v \mid \infty} \lambda S_v \times \prod_{v \nmid \infty} \lambda \Lambda_v$. For $n \geq 1$, denote the $n$-th successive minimum of $S$ to be

$$\lambda_n = \inf \{ t > 0 | tS \text{ contains } n \text{ linearly independent vectors of } \Lambda \text{ over } K \}.$$ 

Then

$$\left( \prod_{i=1}^{n} \lambda_i \right) \text{Vol}(S)^{1/d} \leq 2^N,$$

where the volume is calculated w.r.t. the Adele measure given by (12.2.6.5).

Moreover, if $S_v$ are totally symmetric, then

$$\frac{2^{dn} \pi^{sn}}{(n!)^s ((2n)!)^s} N(\delta_{K/Q})^{n/2} \leq \left( \prod_{i} \lambda_i \right)^d \text{Vol}(S).$$

Proof: Cf.[B-G06]P611. \qed
13.3 Arithmetic of Algebraic Groups

Main references are [Algebraic Groups and Number Theory], [Mil17b].

1 over $p$-adic Number Fields

Notations (13.3.1.1).
- Let $K$ be a $p$-adic number field with ring of integers $\mathcal{O}_K$ and residue field $k$.

Prop. (13.3.1.2). For $G \in \text{Sch}^{ft}/\mathcal{O}_F$, then $G(\mathcal{O}_F)$ is compact.

Prop. (13.3.1.3). If $G$ is a reductive group over $K$, then $G(\mathcal{O}_K)$ is a maximal compact subgroup of $G(K)$.

Proof:

Prop. (13.3.1.4) [Reductive Groups are Unimodular]. If $G/K$ is a reductive group, then $G(K)$ is unimodular.

Proof:

Cor. (13.3.1.5). $GL(n, \mathcal{O}_F)$ is a maximal compact subgroup of $GL(n, F)$, and any compact subgroup of $GL(n, F)$ is conjugate to $GL(n, \mathcal{O}_F)$.

Proof: $GL(n, \mathcal{O}_F)$ is compact by (13.3.1.2).

For maximality, for any compact subgroup $\Gamma$, consider the standard representation of $GL(n)$, it suffices to find an $\mathcal{O}_L$-lattice that is stable under $\Gamma$-action. Notice $\rho(\Gamma) \cap GL(n, \mathcal{O}_L)$ is open in $\rho(\Gamma)$, thus is of finite index, so $\Gamma(\mathcal{O}_L^n)$ is a lattice that is stable under $\Gamma(12.2.3.29)$.

Prop. (13.3.1.6). $SL(n, \mathbb{Q}_p)$ has two maximal subgroups

$$SL(n, \mathbb{Z}_p), \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}^{-1} SL(n, \mathbb{Z}_p) \begin{bmatrix} p & 0 \\ 0 & 1 \end{bmatrix}$$

up to conjugacy.

Proof:

2 Over Global Fields

Def. (13.3.2.1) [Groups of Non-Compact Types]. Let $G \in \text{AlgGrp}/\mathbb{Q}$ be semisimple, then $G$ is said to be a group of compact type if $G(\mathbb{R})$ is compact, and said to be a group of non-compact type if it doesn’t contain a non-trivial normal subgroup of compact type.

Prop. (13.3.2.2) [Real Approximation]. If $G \in \text{AlgGrp}/\mathbb{Q}$ satisfies each connected components of $G$ contains a rational point, then $G(\mathbb{Q})$ is dense in $G(\mathbb{R})$.


Prop. (13.3.2.3).
Congruence Subgroups

**Def.(13.3.2.4) [Congruence Subgroups]**. Let $G \in \text{AlgGrp}/\mathbb{Q}$ with an embedding $G \to \text{GL}(n)_\mathbb{Q}$, for $N \in \mathbb{Z}_+$, define $\Gamma(N) = G(\mathbb{Q}) \cap \{g \in \text{GL}(n,\mathbb{Z})|g \equiv 1 \mod N\}$, and a **congruence subgroup** of $G(\mathbb{Q})$ is any subgroup of $G(\mathbb{Q})$ that contains some $\Gamma(N)$ as a finite index subgroup.

The notion is compatible with that defined in $(13.3.3.13)$. In particular, the set of congruence subgroups of $G$ doesn’t depend on the embedding.

**Prop.(13.3.2.5)[Congruence Subgroup Problem]**. Let $G$ be a reductive group over $\mathbb{Q}$,
- If $G$ is split simply connected other than $\text{SL}(2)$, then every arithmetic subgroup of $G$ is a congruence subgroup.
- If $G = \text{SL}(2)$ or non-simply connected, there are many arithmetic subgroups of $G$ that is not congruence subgroups.


**Prop.(13.3.2.6).** The image of a congruence subgroup may not be a congruence subgroup.

*Proof:*

---

3 over Adeles

**Notations(13.3.3.1).**
- In this subsection, let $F \in \text{GField}$ and $G \in \text{AlgGrp}/F$.

**Def.(13.3.3.2)[Adele Groups]**. Let $G \subset \text{GL}(V) \in \text{AlgGrp}/F$, where $V \in \text{Vect}_F$, $G(A_F)$ is called the **group of Adele points of** $G$. Let $\Lambda$ be a $\mathbb{O}_F$-lattice of $V$, for any place $v \in \Sigma_F$, let $K_v$ be the stabilizer of $\Lambda_v = \Lambda \otimes_{\mathbb{O}_F} \mathcal{O}_v$ in $G(F_v)$, then $K_v$ are compact open subgroups of $G(F_v)$. Define the **adelic group of** $G$

$$G(A_F) = \prod_v (G(F_v)_v, K_v),$$

which is a locally compact topological group. These $K_v$ are called **hyperspecial compact subgroups**, and they are maximal subgroups of $G(K_v)$ for a.e. $v$ if $G$ is reductive $(13.3.1.3)$. We can modify the remaining $v$ s.t. $K_v$ are special maximal compact subgroups, and denote

$$K = K_f K_\infty, \quad K_f = \prod_{v \in \Sigma_F^{\text{fin}}} K_v, \quad K_\infty = \prod_{v \in \Sigma_F^{\text{inf}}} K_v.$$

*Proof:* To show $G(A_F)$ is independent of $\Lambda$, notice $|G(A_F)|$ is clearly invariant, and if $\Lambda'$ is another lattice, then $d^{-1} \Lambda \subset \Lambda' \subset d \Lambda$ for some $d \in \mathbb{Z}_+$, so $K_v$ are the same for $v \nmid d$.

$K_v$ are compact open subgroups of $G(F_v)$ because they are the intersection of $GL(\Lambda_v) \cong GL(n, \mathcal{O}_v)$ with $G(F_v)$. To show they are maximal, for any other compact subgroup $K$ of $G(K_v)$, as $K_v \cap K$ is open, $K/K \cap K_v$ is a finite set, thus $\Box$

**Cor.(13.3.3.3).** $G(A_F) = G(A_S) \times G(A_S)$. 

13.3. ARITHMETIC OF ALGEBRAIC GROUPS 1217
Prop. (13.3.3.4). For a closed embedding of algebraic groups $G \subset G' \in \text{AlgGrp}/F$, the inclusion $G(A_F) \subset G'(A_F)$ is a closed embedding. But for open immersions, the induced inclusion may not be immersions. For example, the embedding $G_m \subset \mathbb{A}^1$ doesn’t induce immersion $I_F \subset A_F$.

Proof: 

Example (13.3.3.5). Fix the following compact subgroup of $GL(n, A)$:

$$K = \prod K_v, \quad K_v = \begin{cases} O(n) & v \text{ real} \\ U(n) & v \text{ complex} \\ GL(n, \mathcal{O}_v) & v \text{ non-Archimedean} \end{cases}.$$ 

then $K$ is the maximal compact subgroup of $GL(n, A)$ in the sense that any compact subgroup can conjugate into $K$.

Let $K_\infty = \prod_{v \in S_\infty} K_v$, and $g_\infty = \prod_{v \in S_\infty} gl(n, F_v)$, then we can define $(g_\infty, F_\infty)$-modules.

Prop. (13.3.3.6). $GL(F)$ is discrete in $GL(A_F)$.

Proof: 

Prop. (13.3.3.7) [Fundamental Domain]. $GL(F) \backslash GL(A_F)$ has a fundamental domain which can be covered by a sufficiently large Siegel sets $G_{c,d}$.

Proof: 

Prop. (13.3.3.8). $GL(F) \backslash GL(A_F)$ has finite volume if $G$ is semisimple, and it is compact if $G$ is anisotropic.

Proof: 

Def. (13.3.3.9) [Strong Approximation Property]. Let $S$ be a finite set of places containing $\Sigma^\infty_F$, a group $G$ is said to satisfy the strong approximation for $S$ if the image of $G(F)$ is dense in $G(A^S)$, or equivalently, for any compact open subgroup $U^S \subset G(A^S)$,

$$G(A) = G(F)G(A_S)U^S.$$ 

In particular,

$$\Gamma \backslash G(A_S) \cong G(F) \backslash G(A)/U^S.$$ 

where $\Gamma$ is the image of $G(F) \cap (G(A_S) \times U^S)$ in $G(A_S)$.

Thm. (13.3.3.10) [Strong Approximation]. Assume $G$ is a simply-connected semisimple group (7.3.2.1) and $G(A_S)$ is non-compact for some finite subset $\Sigma^\infty_F \subset S \subset \Sigma_F$, then $G$ satisfies strong approximation for $S$.

Proof: Cf. [Algebraic Groups and Number Theory, P427].

Remark (13.3.3.11). This is not true for non-semisimple or non-simply connected: for $G_m, \mathbb{Q}^\times$ is not dense in $\mathbb{A}^\times_{Q,f}$.

For $\text{PGL}(2)$, the determinant of $\text{PGL}(2, \mathbb{Q})$ is $\mathbb{Q}^\times/(\mathbb{Q}^\times)^2$ and the determinant of $\text{PGL}(2, \mathbb{A}_{Q,f})$ is $\mathbb{A}^\times_{Q,f}/(\mathbb{A}^\times_{Q,f})^2$, which is not dense.
Cor. (13.3.3.12) [Strong Approximation for $SL(n)$]. Let $F \in \mathbb{NField}$, then

- $SL(n)_F$ satisfies strong approximation for $\Sigma^\infty_F$.
- Let $K_0$ be an open compact subgroup of $GL(n, A_F^\infty)$, then

$$GL(n, F)GL(n, A_\infty)K_0T_1(A) = GL(n, A).$$

- Let $K_0$ be an open compact subgroup of $GL(n, A_F^\infty)$ that the image of $K_0$ under the determinant map is $\prod_{v \in \Sigma^0_F} \mathcal{O}_v^*$, then

$$\det : GL(n, F)GL(n, A_\infty) \backslash GL(n, A_F) / K_0 \to F^\times \mathcal{O}^{\times}_{F, \infty} / \prod_{v \in \Sigma^0_F} \mathcal{O}_v^* = \text{Cl}_1(F)$$

is an isomorphism.

**Proof:**

1 is a direct consequence of (13.3.3.10).

2 is a direct consequence of 1.

3: $\det$ is clearly surjective. To show it is injective, if $\det(a) = \det(b) \in \text{Cl}_1(F)$, then $\det(a) = \det(g_1g_\infty b_k0)$ where $g_1 \in GL(n, F), g_\infty \in GL(n, A_\infty^F), k_0 \in GL(n, A_F^\infty)$ by hypothesis. Then $g_1g_\infty bka^{-1} \in SL(n, A_F)$, and by item 1 it is of the form $h_1h_\infty k_0$ where $h_1 \in SL(n, F), h_\infty \in SL(n, A_\infty^F), k_1 \in a(K_0 \cap SL(n, A_F^\infty))a^{-1}$. Then the assertion follows. \(\square\)

Prop. (13.3.3.13) [Passage From Archimedean to Adele via Congruence Subgroups]. If $F \in \mathbb{NField}$, $U_\Gamma \subset G(A_F^\infty)$ a compact open subgroup and $\Gamma$ the image of $G(F) \cap (G(A_\infty^F) \times U_\Gamma)$ in $G(A_\infty)$, called a **congruence subgroup** of $G$. If $G$ satisfies strong approximation for $S = \Sigma^\infty_F$ (13.3.3.9), then

$$\Gamma \backslash G(A_\infty) \cong G(F) \backslash G(A) / U_\Gamma.$$  

In general, for any open compact subgroup $U \subset G(A_f)$,

$$\# G(F) \backslash G(A) / G(A_\infty) U < \infty.$$  

Thus if $\{g_i\} \subset G(A_f)$ is a set of double coset representatives,

$$G(F) \backslash G(A) / U = \prod_i \Gamma_i \backslash G(A_\infty)$$

where $\Gamma_i$ is the image of $(g_iUg_i^{-1} \times G(A_\infty^F)) \cap G(F)$ in $G(A_\infty)$. Thus the passage from Archimedean to adele is not seriously affected by the lack of strong approximation.

**Proof:** The double coset is finite because for any $(g_v) \in G(A_F^\infty)$, by strong approximation for $G_\infty$, we can choose a $g \in G(F)$ s.t. $g^{-1}g_v \in K_v$ for any $v \in \Sigma^\text{fin}_F$, then the image is finite as $U$ is compact open and $\prod_v K_v$ is compact. \(\square\)
### 13.4 Arithmetic Subgroups

Main references are [Mor15] and [V. Platonov and A. Rapinchuk: Algebraic Groups and Number Theory.]

**Def. (13.4.0.1)**[Arithmetic Subgroups]. For \( G \in \text{Alg}_{\text{grp}}/\mathbb{Q} \), an arithmetic subgroup \( \Gamma \leq G(\mathbb{Q}) \) is a subgroup that is commensurable with \( G(\mathbb{Q}) \cap \text{GL}(n,\mathbb{Z}) \) for some embedding \( G \hookrightarrow \text{GL}(n)_{\mathbb{Q}} \). This notion is independent of the embedding chosen.


**Prop.(13.4.0.2).** If \( \rho : G \to G' \in \text{Alg}_{\text{grp}}/\mathbb{Q} \) is surjective, then \( \rho \) maps an arithmetic subgroup to an arithmetic subgroup.

### 1 Arithmetical Subgroup of Lie Groups

**Def. (13.4.1.1)**[Arithmetic Subgroups]. Let \( H \) be a connected real Lie group, then an arithmetic subgroup \( \Gamma \subset H \) is a subgroup s.t. there exists an algebraic group \( G \in \text{Alg}_{\text{grp}}/\mathbb{Q} \), a surjective homomorphism \( G(\mathbb{R})^0 \to H \) with compact kernel, and \( \Gamma_0 \subset G(\mathbb{Q}) \) an arithmetic subgroup s.t. \( \Gamma_0 \cap G(\mathbb{R})^0 \) maps to \( \Gamma \).

**Prop.(13.4.1.2).** Let \( H \) be a semisimple real Lie group that admits a faithful f.d. representation, then every arithmetic subgroup of \( H \) is discrete of finite covolume, and contains a torsion-free subgroup of finite index.

*Proof:* Cf.[Mil17b]P34. \( \square \)

**Prop.(13.4.1.3).** In any connected real Lie group there are only countably many arithmetic subgroups up to conjugacy.

*Proof:* Cf.[Mor15]5.1.20. \( \square \)

**Thm.(13.4.1.4)**[Margulis]. Every discrete subgroup of finite volume in a non-compact simple real Lie group \( H \) is arithmetic unless \( H \) is isogenous to \( SO(1,n) \) or \( SU(1,n) \).

Note that \( SL(2,\mathbb{R}) \) is isogenous to \( SO(1,2) \), so the theorem doesn’t apply to it.

*Proof:* Cf.[Mor15]5.2. \( \square \)
13.5 Arithmetic of Abelian Varieties

Main references are [Sta], [Abelian Varieties notes Conrad], [Mil08], [B-G06], [Abelian Variety van der Geer], [BLR90]. See [Bhatt’s notes] for everything done in the relative setting. A history of Abelian varieties can be found in [Mil08]P125.

1 Basics

Def.(13.5.1.1) [Abelian Schemes]. An Abelian variety $A$ over a field $k$ is a group variety over $k$ that is a complete variety over $k$.

For $S \in \mathcal{S}$, an Abelian scheme over $S$ is a proper smooth group scheme $A \in \mathcal{S} \leftarrow S$ s.t. all the fibers $A_s$ are Abelian varieties over the resp. residue field $\kappa(s)$. Denote $\text{AbVar} \leftarrow S$ the subcategory of $\text{AlgGp} \leftarrow S$ consisting of Abelian schemes over $S$.

Being an Abelian scheme is stable under base change of fields, by (5.10.1.3).

Prop.(13.5.1.2). If $X$ is an Abelian variety, any global tangent vector on a group variety is left invariant.

Proof: Because $\Gamma(X, \mathcal{O}_X) = k(5.10.1.12)$, so by (7.1.4.35), $\Gamma(X, \mathcal{O}_X \otimes T_{X,e}) = T_{X,e}$ are all generated by left invariant vectors (left and right translation commutes).

Prop.(13.5.1.3) [Abelian Varieties are Projective, Weil]. Abelian varieties are projective, by (7.1.4.8) and (5.4.5.3).

Prop.(13.5.1.4) [Rigidity Theorem]. Let $f : X \to Y$ be a morphism of an Abelian varieties to a group variety, then it is a group homomorphism followed by a translation $t_{f(x)}$.

Proof: Set $y = i_Y(f(x))$ and consider $h = t_y \circ f$, then $h(e_X) = e_Y$, and consider the morphism:

$$g : X \times X \to Y : (x, x') \mapsto h(xx')(h(x)h(x'))^{-1}.$$  

then $g(e_X, X) = g(X, e_X) = e_Y$, so the rigidity lemma (5.10.1.20) shows $g$ is constant with value $e_Y$. Thus $h \circ m_X = m_Y \circ (h \times h)$, thus a group homomorphism.

Cor.(13.5.1.5) [Abelian Varieties are Commutative].

- Let $X$ be a variety over $k$, then there is at most one one structure of Abelian variety on $X$.
- The group law of an Abelian variety is commutative, justifying the name.

Remark(13.5.1.6). The completeness of $X$ is essential for the proof. In fact, there are many non-commutative group varieties, like $\text{GL}(n)$.

From now, use the additive notation for Abelian varieties.

Proof: 1: If there are two structure $(m, i), (n, j)$, then consider $X \times X \to X \to X : (x, y) \mapsto m(x, y)(n(x, y)^{-1})$, then it is constant on $e_X \times X$ and $X \times e_X$, thus it is constant, so $m = n$. And $i = j$ is also clear by the associativity.

2: The inverse $i$ is a group homomorphism by (13.5.1.4), thus it is Commutative.

Prop.(13.5.1.7) [Rigidity of Morphism from Smooth Varieties]. If $X$ is an Abelian variety over a field $K$, then any rational map from a smooth $K$-variety $Y$ extends to a morphism $Y \to X$. 


Proof: By (7.1.4.34), $V$ is regular, thus by (5.4.5.15), a rational map is defined on a set whose complement has codimension $\geq 2$, but then (7.1.1.20) shows it must be defined on all of $X$. □

Cor. (13.5.1.8) [Quotient by Finite Subgroups]. Quotients of an Abelian variety $A$ are also an Abelian varieties.

Proof: It is a group variety of dimension 1 with a rational point by (7.1.5.29). And it is complete by (5.4.5.3). □

Remark (13.5.1.9). WARNING: it is not true that the quotient of an Abelian variety by any finite group of automorphisms is an Abelian variety, as the quotient by the hyperelliptic involution (i.e. $-1$) is just $\mathbb{P}^1$.

Cor. (13.5.1.10) [Even Functions]. Let $E$ be an elliptic curve, then $f \in K(E)$ is even iff $f \in K(x)$.

Proof: Write $f(x, y) = g(x) + h(x)y$, then the condition says $(2y + a_1x + a_3)h(x) = 0$ for any $(x, y) \in E(K)$. Thus $h(x) = 0$, otherwise $E$ is degenerate, which is not possible. □

Pseudo-Abelian Varieties

Def. (13.5.1.11) [Pseudo-Abelian varieties]. A pseudo-Abelian variety is a group variety with no non-trivial affine normal group subvarieties.

Prop. (13.5.1.12). Abelian varieties are pseudo-Abelian varieties.

Proof: Every normal group subvariety is closed thus complete, hence if it is affine, it equals $e$. □

Prop. (13.5.1.13). Being a pseudo-Abelian variety is stable under separable base change of fields.

Proof: Cf. [Mil17] P149. □

Prop. (13.5.1.14). Let $G$ be a group variety over $k$, then there exists a unique affine normal group subvariety $N$ s.t. $G/N$ is a pseudo-Abelian variety. And this $N$ is stable under base change.

Proof: This follows from (7.1.4.34) and (7.1.5.30) (7.1.5.29). □

Prop. (13.5.1.15) [Barsotti-Chevalley]. Let $k$ be perfect, then any pseudo-Abelian variety over $k$ is complete hence is an Abelian variety.


Cor. (13.5.1.16). If $G$ is a group variety over a perfect field $k$, then unique affine normal group subvariety $N$ s.t. $G/N$ is an Abelian variety, by (13.5.1.14).

Prop. (13.5.1.17) [Algebraic Groups are Extensions of Abelian Varieties]. Let $G$ be a connected algebraic group over a field $k$, then there is a connected affine normal algebraic subgroup $N$ (not necessarily smooth) s.t. $G/N$ is is an Abelian variety.


Cor. (13.5.1.18). Every pseudo-Abelian variety $G$ is commutative.

Proof: As $G$ is smooth and connected, so is $[G, G]$ (7.1.4.27), so it is a group variety (7.1.4.34). Let $N$ be given by (13.5.1.17), then because $G/N$ is an Abelian variety, $[G, G] \subset N$. Thus $[G, G]$ is affine, which implies $[G, G] = e$. □

Prop. (13.5.1.19) [Totaro(2013)]. Any pseudo-Abelian variety is an extension of a connected unipotent group variety $U$ by an Abelian variety $A$ in a unique way.

Proof:
13.5. ARITHMETIC OF ABELIAN VARIETIES

**Line Bundles**

**Remark (13.5.1.20).** As Abelian varieties are regular, $\text{Cl}(X) \cong \text{Pic}(X)$, by (5.5.3.15).

**Prop. (13.5.1.21) [Theorem of the Cube].** If $X$ is an Abelian variety, and $L$ is a line bundle over $X$, then

$$\Theta(L) = \text{pr}_{123}^* L \otimes \text{pr}_{12}^* (L^{-1}) \otimes \text{pr}_{13}^* (L^{-1}) \otimes \text{pr}_1^* (L) \otimes \text{pr}_2^* (L) \otimes \text{pr}_3^* (L)$$

is trivial.

**Proof:** This is trivial on $0 \times X \times X, X \times 0 \times X, X \times X \times 0$, so it is trivial, by (5.10.1.23). \hfill $\square$

**Cor. (13.5.1.22).** There is a form of morphisms from a scheme to $X$, just by considering $(f, g, h) : Y \times Y \times Y \to X \times X \times X$, i.e.

$$(f + g + h)^* L \otimes (f + g)^* L^{-1} \otimes (f + h)^* L^{-1} \otimes (g + h)^* L^{-1} \otimes f^* L \otimes g^* L \otimes h^* L$$

is trivial.

**Cor. (13.5.1.23) [Theorem of the Square].** Let $A$ be an Abelian variety that $L$ is a line bundle, then for any $x, y \in A$,

$$t_{x+y}^* L \otimes L \cong t_x^* L \otimes t_y^* L \in \text{Pic}(A_{k(k(x)k(y)})).$$

Notice this isomorphism is defined under the field generated by the residue fields of $x$ and $y$.

**Proof:** Apply the theorem of the cube (13.5.1.22) for $f = \text{id}_X$ and $g, h$ the function with constant value $x, y$. \hfill $\square$

**Cor. (13.5.1.24).** For a line bundle $L$ on an Abelian variety $X$, then the map $\varphi_L : X \to \text{Pic}(X) : x \mapsto [t_x^* L \otimes L^{-1}]$ is a homomorphism.

**Cor. (13.5.1.25).** For any line bundle $L$, 

$$[n]^* L \cong L^{n(n+1)/2} \otimes [-1]^* L^{n(n-1)/2}.$$ 

**Proof:** Use (13.5.1.22) in case $f = [n], g = [1], h = [-1]$, then we have:

$$n^* L^2 \otimes (n + 1)^* L^{-1} \otimes (n - 1)^* L^{-1} \cong (L \otimes [-1]^* L)^{-1}.$$ 

So we can use induction. \hfill $\square$

**Def. (13.5.1.26) [Even Line Bundle].** Consider the involution $[-1]$ of $X$ and its action on the line bundles, then a **even/odd line bundle** is defined to be a line bundle $L$ that $[-1]^* L \cong L$ (resp. $L^{-1}$).

**Prop. (13.5.1.27).** On an Abelian Variety, there is an even very ample line bundle.

**Proof:** Abelian variety is projective by (13.5.1.3), thus there is a very ample line bundle $L$, and $[-1]^* L$ is also very ample, so $L \otimes [-1]^* L$ is even and very ample, by (5.5.4.21). \hfill $\square$

**Prop. (13.5.1.28).** For an Abelian variety over a number field $K$ and any line bundle $c \in \text{Pic}(X)$, there are an odd line bundle $c^-$ and an even line bundle $c^+$ that $c = c_- + c_+$. 
Proof: Consider \( 2c = (c + [-1]^*c) + (c - [-1]^*c) \). \( c - [-1]^*c \) is odd thus is in \( \text{Pic}^0(X) \) by (13.5.4.8), thus by (13.5.6.14), there is a \( c^* \in \text{Pic}^0(X) \) that \( 2c^* = c - [-1]^*c \). Then \( c = (c-c^*)+c^* \) satisfies the requirement. \( \square \)

Lemma (13.5.1.29). Let \( A \) be an Abelian variety over \( K \) and \( \text{pr}_i : A \times A \to A \) be the projections and \( m \) be the multiplication, then the following are equivalent:

- \( m^*(c) \cong \text{pr}_1^*(c) + \text{pr}_2^*(c) \).
- \( \tau_a^*(c) \cong c \) for \( a \in A \).

And if these are satisfied, \( c \) is even.

Proof: The equivalence is a consequence of the formula \( (m^*(c) - \text{pr}_1^*(c) - \text{pr}_2^*(c))|_{A \times \{a\}} = \tau_a^*(c) - c \) and the see-saw principle (5.10.1.22). The last assertion is a consequence of the first equation pulled back via the morphism \( A \to A \times A : a \mapsto (a, -a) \). \( \square \)

Prop. (13.5.1.30) [Projective Embeddings]. No Abelian varieties of dimension \( g \) can be embedded into \( \mathbb{P}^{2g-1} \). No Abelian variety except for elliptic curves and Abelian surfaces of degree 10 in \( \mathbb{P}^4 \) can be embedded into \( \mathbb{P}^{2g} \).

Proof: Cf. [Van de Geer P26], where algebraic topologies are used. \( \square \)

2 Formal Groups

Def. (13.5.2.1) [Formal Group Law of Abelian Varieties]. Given an Abelian variety \( A \) over a field \( K \), the group structure on \( A \) induces a homomorphism \( \mathcal{O}_{A,e} \to (\mathcal{O}_{A,e} \times \mathcal{O}_{A,e})_{e \times e} \), whose completion is a formal group law of dimension \( n \).

3 over Alg. Closed Fields

All Abelian variety \( X \) in this subsection is over an alg. closed field \( k \).

Prop. (13.5.3.1). There is a closed pt \( 0 \) in \( X \) that corresponds to 0 in the group \( X(k) \), if we denote \( \Omega_0 \) the cotangent space at 0, it is the stalk of the differential \( \Omega_{X/k} \) at 0 (5.5.5.6).

Def. (13.5.3.2) [Fields of Moduli]. Let \( k \) be a field, the field of moduli of an Abelian variety \( A \) over \( \overline{k} \) is the fixed field of \( \{ \sigma \in \text{Gal}(\overline{k}/k) | A^\sigma \cong A \} \).

Def. (13.5.3.3) [Fields of Definition]. Let \( k \) be a field, the field of moduli of an Abelian variety \( A \) over \( \overline{k} \) is the minimal field \( \overline{k} \supset k' \supset k \) s.t. \( A \) is defined over \( k' \).

Remark (13.5.3.4). Generally, the field of definition is bigger than the field of moduli.

Prop. (13.5.3.5). For any Abelian variety \( A \) over a field \( k = \overline{k} \) of dimension \( g \), \( \dim_k H^1(A, \mathcal{O}_A) \leq g \). In fact, equality holds by (13.5.4.12).

Proof: This follows from Borel’s classification of Hopf-algebras (2.9.1.15). Cf. [Van de Geer P94] or [Conrad Notes, P45]. \( \square \)
**Prop. (13.5.3.6)**. For \( k \in \text{Field}, \text{char} \, k = p, A \in \text{AbVar}/k \), \( A(k^{\text{sep}}) \) is an Abelian group and its \( l^n \) torsion is isomorphic to \( (\mathbb{Z}/(p^n))^{2g} \) and its \( p^n \) torsion is isomorphic to \( (\mathbb{Z}/(p^n))^r \) for some \( r \geq 1 \).

**Prop. (13.5.3.7)**. There is an isomorphism

\[
H^m_i(\Lambda_{K^{\text{sep}}}, \mathbb{Q}_l) \cong \bigwedge^m(V_i(A))^*.
\]

Cf. [Grothendieck Monodromy theorem].

### 4. Dual Abelian Varieties

**Def. (13.5.4.1) [Dual Abelian Variety]**. For an Abelian variety \( A \), the **dual Abelian variety** \( \hat{A} \) is defined to be its Picard variety \( \text{Pic}^0_A/k \), which represents \( \text{Pic}^0_A/k \) and is a projective scheme by (7.7.3.33). We will see it is an Abelian variety in (13.5.4.12).

**Prop. (13.5.4.2) [\( A \to \hat{A} \) Induced by a Line Bundle]**. If \( A \) is an Abelian variety over \( k \), for any line bundle \( c \), there is a line bundle on \( A \times \hat{A} \) given by the **Mumford line bundle**

\[
\Lambda(c) = m^*c - \text{pr}_1^*c - \text{pr}_2^*c,
\]

where \( m : A \times A \to A \) is the product. It is in \( \text{Pic}^0(A) \) because \( \Lambda(c)|_{e \times A} = 0 \) and \( \Lambda(c)|_{A \times a} = \tau_a^*c - c \). Then by definition, this line bundle corresponds to a morphism \( \varphi_c : A \to \hat{A} \) over \( k \), and by (7.7.3.34) \( \varphi_c(a) = \tau_a^*c - c \in \hat{A}(k(a)) \). This is also a homomorphism of Abelian variety, by (13.5.1.4), as \( \varphi_c(e) = e \).

**Cor. (13.5.4.3) [\( \varphi \)-Construction]**. It is clear from the definition above that \( \mathcal{L} \mapsto \varphi_\mathcal{L} \) is a group homomorphism \( \text{Pic}(A) \to \text{Hom}(A, \hat{A}) \).

**Cor. (13.5.4.4)**. For \( x \in A(k) \), \( \varphi_{\tau_x^*\mathcal{L}} = \varphi_\mathcal{L} \).

*Proof:* This follows from see-saw lemma, by observing that stalks of the line bundles in (13.5.4.2) are \( \tau_{a+x}^*\mathcal{L} = \tau_x^*\mathcal{L} \) and \( \tau_a^*\mathcal{L} = \mathcal{L} \) resp.. \( \square \)

**Cor. (13.5.4.5)**. \( (1, \varphi_\mathcal{L})^*p_A = \mathcal{L} \otimes [-1]^*\mathcal{L} \).

*Proof:* \( (1, \varphi_\mathcal{L})^*p_A = (x \mapsto (x, -x))^*(1, -\varphi_\mathcal{L})^*p_A = (x \mapsto (x, -x))(-m^*\mathcal{L} + \text{pr}_1^*\mathcal{L} + \text{pr}_2^*\mathcal{L}) = \mathcal{L} \otimes [-1]^*\mathcal{L}. \) \( \square \)

**Prop. (13.5.4.6) [Poincaré Class is Even]**. Let \( p \in \text{Pic}(A \times \hat{A}) \) be the Poincaré class of \( A \), then \( p \) is even in \( \text{Pic}(A \times \hat{A}) \).

*Proof:* Let \( b \in \hat{A} \), then

\[
([-1]^*p)|_{A \times \{b\}} = [-1]^*p|_{A \times \{-b\}} = [-1]^*(-b) = b.
\]

and

\[
([-1]^*p)|_{\{0\} \times \hat{A}} = [-1]^*p|_{\{0\} \times \hat{A}} = 0.
\]

Thus \([-1]^*p \cong p\) by (7.7.3.34) and the see-saw principle (5.10.1.22). \( \square \)
**Lemma (13.5.4.7).** If $b \in \text{Pic}(A)$ that $\varphi_b = 0$, then for any ample $c \in \text{Pic}(A)$, there is some $a \in A(K)$ that $b = \tau_a^*(c) - c$.

**Proof:** [Mumford, P77].

**Prop. (13.5.4.8) [Characterizing $\hat{A}$].** For $c \in \text{Pic}(A)$, $[-1]^*c - c \in \text{Pic}^0(A)$, the following are equivalent:
1. $b \in \text{Pic}^0(A)$.
2. $\ker(\varphi_b) = A$.
3. For every ample line bundle $c$, there is an $a \in A$ that $b \cong \tau_a^*(c) - c$.
4. There is an ample line bundle $c$ and an $a \in A$ that $b \cong \tau_a^*(c) - c$.
5. $c$ is odd.
6. For any scheme $X$, the map $\text{Mor}(X, A) \to \text{Pic}(X) : \varphi \mapsto \varphi^*(c)$ is linear.

**Proof:** $2 \to 3$ is by the lemma (13.5.4.7). $4 \to 1$ is by (13.5.4.2).

$1 \to 2$: By (7.7.3.22), It suffices to prove for $K$ alg.closed. Firstly we shows there is a morphism underlying the map

$$\varphi : A \times \text{Pic}^0(A) \to \text{Pic}^0(A) : (a, b) \mapsto \tau_a^*(b).$$

For $T = A \times \text{Pic}^0(A)$, consider the line bundle $c = (m \times \text{id}_{\text{Pic}^0(A)})^*(p)$ on $A \times T$. Notice the restriction of $m \times \text{id}_{\text{Pic}^0(A)}$ on $A \times \{a\} \times \{b\}$ is given by $\tau_a$,

$$c|_{A \times \{a\} \times \{b\}} = \tau_a^*(b),$$

and also $c|_{\{0\} \times T} = p$, so the family $c - \text{pr}_2^*(p)$ of $\text{Pic}^0(A)$ parametrized by $T$ gives an morphism $T \to \text{Pic}^0(A)$ extending $\varphi$.

Next, because $\varphi(A \times \{0\}) = 0$, by rigidity lemma (5.10.1.20) we have $\tau_a^*(b) \cong b$ for any line bundle $b$.

$6 \to 5$ is trivial, and 6 is clearly equivalent to the assertion when $X = A$, and it is equivalent to 2 by (13.5.1.29).

We next prove $[-1]^*c - c \in \text{Pic}^0(A)$: because $[-1]\tau_a = \tau_{-a}[-1]$, we have

$$\tau_a^*([-1]^*c) - [-1]^*c = [-1](\tau_a^*(c) - c).$$

since $\tau_{-a}^*(c) - c \in \text{Pic}^0(X)$ by (13.5.4.2), the equation is equal to $c - \tau_{-a}^*(c)$ by implication $1 \to 2 \to 6$.

and this further equals $\tau_a^*(c) - c$ by the theorem of square (13.5.1.23). Then

$$\tau_a^*([-1]^*c) - (-1)^*c = 0.$$

Hence $[-1]^*c - c \in \text{Pic}^0(A)$ by the implication $2 \to 3 \to 4 \to 1$.

$5 \to 1$: Let $c$ be an odd element, then $-2c = [-1]^*c - c \in \text{Pic}^0(A)$ by what just proved, we have $c \in \text{Pic}^0(A)$. Then $\varphi_c$ has image in the kernel of $[2]$ on $\hat{A}$, by the implication $1 \to 2$, thus it has trivial image, by (13.5.6.14).

**Cor. (13.5.4.9).** $L \mapsto \varphi_L$ induces an injective map

$$\text{NS}(A_\mathbb{F}) = \text{Pic}(A_\mathbb{F})/\text{Pic}^0(A_\mathbb{F}) \hookrightarrow \text{Hom}_\mathbb{F}(A_\mathbb{F}, \hat{A}_\mathbb{F}).$$
Cor. (13.5.4.10) [Abelian Varieties are Finite Torsion-Free]. For an Abelian variety $A$, $\text{NS}(A_{\overline{k}})$ is a finite free $\mathbb{Z}$-module. (Although this is true for any complete variety).

Proof: This follows from (13.5.4.9) and (13.5.6.9).

Prop. (13.5.4.11) [Ample Implies Non-Degenerate]. A class $\mathcal{L} \in \text{Pic}(A)$ is ample iff $\ker \varphi_{\mathcal{L}}$ is finite and $H^0(A, nc) \neq 0$ for some $n > 0$.

In particular, an effective line bundle on $A$ is ample iff $\ker \varphi_{\mathcal{L}}$ is finite.

Proof: Cf. [Diophantine Geometry, P253] or [Conrad notes].

Cor. (13.5.4.12) [Dual Abelian Variety]. Let $k \in \text{Field}$ and $A \in \text{AbVar}_{/k}$, then

$$A^\vee = \text{Pic}^0_{X/S} = \text{Pic}^0_{X/S, \text{red}} = \text{Pic}^r_{X/S}$$

is also an Abelian variety, and $\dim A = \dim \hat{A} = \dim_k H^1(A, \mathcal{O}_A)$.

Proof: Take an ample line bundle $\mathcal{L}$ on $A$, then $\varphi_{\mathcal{L}} : A \to \hat{A}$ has finite kernel, thus $\dim \hat{A} \geq \dim A$, but by (13.5.3.5) and (7.7.3.24), $\dim_k H^1(A, \mathcal{O}_A) = T_e(\hat{A}) \leq \dim A$, thus it is regular by (4.3.5.17).

Def. (13.5.4.13) [Non-degenerate Line Bundles]. A non-degenerate line bundle on an Abelian variety is a line bundle $\mathcal{L}$ s.t. $K(\mathcal{L}) = \ker \varphi_{\mathcal{L}}$ is a finite group scheme, i.e. $\varphi_{\mathcal{L}}$ is an isogeny.

Prop. (13.5.4.14) [Ample Line Bundles induce Isogenies]. For any ample line bundle $\mathcal{L}$ on $A$, the morphism $\varphi_{\mathcal{L}} : A \to \hat{A}$ is an isogeny, because it is surjective by (7.1.5.14).

Lemma (13.5.4.15). For $k \in \text{Field}$ and $A \in \text{AbVar}_{/k}$, $\mathcal{L} \in \text{Pic}(A)$, consider the double Picard map (7.7.3.37) $\kappa_A : A \to \hat{A}$, then $\varphi_{\mathcal{L}} = \hat{\varphi}_{\mathcal{L}} \circ \kappa_A : A \to \hat{A}$.

Proof: Cf. [van Der Geer, P100].

Prop. (13.5.4.16) [Double Duality Theorem]. For $k \in \text{Field}$ and $A \in \text{AbVar}_{/k}$, the double Picard map (7.7.3.37) $A \to \hat{A}$ is an isomorphism.

Proof: Cf. [van Der Geer, P101].

5 Cohomology of Line Bundles

Prop. (13.5.5.1). $H^n(A \times A^\vee, p_A) = \delta_{n,g}$.

Proof: Cf. [Conrad, P62].

Prop. (13.5.5.2) [Riemann-Roch]. Let $A$ be an Abelian variety of dimension $g$, and $\mathcal{L} \in \text{Pic}(A)$, then $\chi(\mathcal{L}) = c_1(\mathcal{L})^g / g!$ and $\chi(\mathcal{L})^2 = \deg(\varphi_{\mathcal{L}})$.

Proof: Cf. [Van de Geer, P131].

Cor. (13.5.5.3). Let $f : X \to Y$ be an isogeny of Abelian varieties, then $\chi(f^* \mathcal{L}) = \deg(f) \chi(\mathcal{L})$.

Proof:
Prop. (13.5.5.4) [Index]. If $\mathcal{L}$ is a non-degenerate line bundle on an Abelian variety $A$ over a field $k$, then there is a unique integer $0 \leq i \leq g$ s.t. $H^i(X, \mathcal{L}) \neq 0$. Such an $i$ is called the index of $\mathcal{L}$. Notice index 0 just means it is effective.

Proof:

Thm. (13.5.5.5) [Kempf-Mumford-Ramanujam]. Let $\mathcal{L}$ be a line bundle on an Abelian variety $A$, and fix an ample line bundle $H$ on $A$, let $\Phi$ be the Hilbert polynomial of $\mathcal{L}$ w.r.t. $H$, then

- The multiplicity of 0 in $\Phi$ equals $\dim K(\mathcal{L})$.
- If $\mathcal{L}$ is non-degenerate, then all roots of $\Phi$ in $\mathbb{C}$ are real, and the number of positive roots equals $i(\mathcal{L})$.

Proof: Cf. [Van de Geer, P139,140].

Cor. (13.5.5.6). Let $\mathcal{L}$ be a non-degenerate line bundle on $A$ and $f : B \to A$ is an isogeny of Abelian varieties, then $i(\mathcal{L}) = i(f^*\mathcal{L})$.

Proof: This follows from the relation of Hilbert polynomial resulted from (13.5.5.3) and the above theorem (13.5.5.5).

6 Isogenies and Tate Modules

Isogenies

Prop. (13.5.6.1) [Isogenies of Abelian Varieties]. Let $k \in \text{Field}$ and $f : X \to Y \in \text{AbVar}/k$, the following are equivalent:

- $f$ is an isogeny.
- $f$ is surjective and $\dim X = \dim Y$.
- $\ker f$ is a finite group scheme and $\dim X = \dim Y$.
- $f$ is finite.

The set of isogenies from $X$ to $Y$ is denoted by $\text{Isog}(X,Y)$. $\text{Isog}(X,X) \cup \{0\}$ is denoted by $\text{Isog}(X)$.

Proof: This follows from the theory of algebraic groups.

Def. (13.5.6.2) [Isogenous Abelian Varieties]. For $k \in \text{Field}$ and $A,B \in \text{AbVar}/k$, write $A \sim B$ to mean that $A,B$ is isogenous. This is an equivalence relation.

Prop. (13.5.6.3) [Separable Isogenies]. Let $f : X \to Y$ be an isogeny of Abelian varieties over $k$, then

- For any $Q \in Y(\bar{k})$, $\#f^{-1}(Q)(\bar{k}) = \deg_s(f)$, and for any $P \in X$, $e_P(f) = \deg_s(f)$.
- The map: $X[f] \to \text{Gal}(K(X_{\bar{k}})/\varphi^*(K(Y_{\bar{k}}))) : P \mapsto \tau_{\varphi}^P$ is an isomorphism of groups.
- $f$ is unramified iff it is étale iff it is separable, and in this case, $K(X_{\bar{k}})/K(Y_{\bar{k}})$ is an Abelian Galois extension of degree $\deg(f)$.

Proof: 1: By (5.10.3.4), this holds for $Q$ in a dense open subset of $Y$, thus by homogeneity, it holds for all $Q$. The second assertion follows from the fact after shrinking $f$ is finite locally free of rank $\deg(f)$ by using homogeneity on $X$.

2: This is clearly a group homomorphism. By Galois theory, it suffices to show it is injective, which is clear.

3: This follows from (13.5.6.1) and generic unramifiedness (5.6.5.9).
Prop. (13.5.6.4) [Isogenous is an Equivalence Relation]. If \( k \in \text{Field}, X, Y \in \text{AbVar} / k \) and \( f \in \text{Isog}(X, Y) \), \( d = \text{deg}(f) \), then there exists \( g \in \text{Isog}(Y, X) \) s.t. \( g \circ f = [d]_X, f \circ g = [d]_Y \).

Proof: As \( \ker(f) \) is a finite group scheme of rank \( d \), \( [d] \ker(f) = 0 \), so \( [d] \) factors through \( f \) via \( g : Y \to X \), so \( g \circ f = [d]_X \). Then also \( [d]_Y \circ f = f \circ [d]_X = f \circ (g \circ f) = (f \circ g) \circ f \), thus \( [d]_Y = f \circ g \) as \( f \) is a quotient map. \( \square \)

Prop. (13.5.6.5) [Dual Isogenies]. Let \( A, A' \in \text{AbVar} / k \) and \( \varphi \in \text{Hom}(A, A') \), then we get a dual homomorphism \( \hat{\varphi} \in \text{Hom}(\hat{A'}, \hat{A}) \). Then:

- \( \hat{\varphi} = \varphi \).
- \( \text{deg}(\hat{\varphi}) = \text{deg}(\varphi) \).
- \( \hat{\varphi} + \psi = \hat{\varphi + \psi} \).
- \( [m]_E = [m]_{\hat{E}} \).

Proof: 1: This is formal.
2: [Conrad, P66].
3: This is clear from the modular description of \( \hat{A} \).
4: This follows from 3. \( \square \)

Hom\((X,Y)\)

Def. (13.5.6.6) [Simple Abelian Varieties]. A simple Abelian variety is an Abelian variety that has no non-trivial Abelian subvarieties.

Prop. (13.5.6.7) [Poincaré’s Complete Reducibility Theorem]. Let \( B \) be an Abelian subvariety of \( A \), then there exists an Abelian subvariety \( C \) of \( A \) that the addition gives an isogeny 

\[ B \times C \to A. \]

Proof: Choose an ample line bundle \( c \) on \( A \), let \( \iota : B \to A \) be the inclusion and \( \hat{\iota} : \hat{A} \to \hat{B} \) the dual map, then 

\[ (\hat{\iota} \circ \varphi_c)|_B = \varphi_{\iota^*(c)}. \]

Since \( \iota^*(c) \) is also ample, \( \varphi_{\iota^*(c)} \) is an isogeny, thus has finite kernel. Let \( C = \ker(\iota \circ \varphi_c) \), then we have \( C \cap B \) is finite, whence \( B \times C \to A \) has finite kernel. The dimension theorem (7.1.4.36) applied to \( \iota \circ \varphi_c \) shows

\[ \dim C + \dim \hat{B} = \dim \hat{A}. \]

and this together with (13.5.4.12) shows \( B \times C \to A \) is a surjection, because \( A \) is irreducible. Thus it is an isogeny. \( \square \)

Cor. (13.5.6.8). For \( k \in \text{Field}, A \in \text{AbVar} / k \), there are simple Abelian subvarieties \( B_1, \ldots, B_n \) of \( A \) that the inclusions give an isogeny 

\[ B_1 \times \ldots \times B_n \to A. \]

Prop. (13.5.6.9) [\( \text{Hom}(A, A') \) is Torsion-Free and F.g.]. Let \( k \) be a field and \( A, A' \in \text{AbVar} / k \), then \( \text{Hom}(A_1, A_2) \) w.r.t. the addition is a f.g. torsion-free Abelian group of rank at most \( 4g^2 \).

Proof: Assume \( [m] \circ \varphi = 0 \), then \( \varphi \circ [m] = 0 \), and use the fact \( [m] \) is surjective (13.5.6.14). The last assertion follows from (13.15.1.1). \( \square \)
Def. (13.5.6.10) [Quasi-Isogenies]. For $A, A' \in \text{AbVar} / k$, $\text{Hom}_Q(A, A') = \text{Hom}(A, A') \otimes Q$ is called the set of quasi-isogenies from $A$ to $A'$.

Define the category $\text{Isog} / k$ to be the category consisting of Abelian varieties over $k$ with morphisms $\text{Mor}(A, A') = \text{Hom}(A, A') \otimes Q$. Notice $f : A \to A' \in \text{AbVar} / k$ is an isogeny iff $f$ is an isomorphism in $\text{Isog} / k$, by (5.4.4.20).

Thus by (13.5.6.8), $\text{Isog} / k$ is a semisimple $Q$-linear Abelian category.

Prop. (13.5.6.11). For $A, A' \in \text{AbVar} / k$, if $A \sim A'$, then $\text{End}_Q(A) = \text{End}_Q(A')$. Moreover, $\text{End}_Q(A)$ is a semisimple $Q$-algebra, and it is simple iff $A$ is simple.

Proof: These follow from (13.5.6.8). \hfill \Box

Tate Modules

Prop. (13.5.6.12). Let $S \in \text{Sch}$ be locally Noetherian, and $A \in \text{AbVar}^g / S, n \in Z_+$, then $A[n]$ is a finite locally free $S$-group scheme of order $n^{2g}$.

Proof: \hfill ? \hfill \Box

Cor. (13.5.6.13). For an Abelian variety $X$ and any $n > 0$, the group of geometric points of order $n$ in $X$ is finite.

Prop. (13.5.6.14) [Multiplication Map, Weil]. Let $k \in \text{Field}^p, A \in \text{AbVar} / k$, and $n \in Z \cap k^\times$, then $[n] : A \to A$ is finite faithfully flat of degree $n^{2\dim_A}$. In particular it is an isogeny (13.5.6.11), and

- If $n \in Z \cap k^\times$, then $[n]$ is finite étale and $A[n] \cong (Z/nZ)^{2\dim_A}$.
- If $n = 0 \in k$, then $[n]$ is not separable.
- If $p > 0$, then $\ker([p]) \cong (Z/pZ)^r \times \alpha_p^{2g-2r} \times \mu_p^r$ for some $0 \leq r \leq g$. In particular, $A[p^f] = (Z/(p^e))^r$ for any $e \geq 0$. This $r$ is called the $p$-rank of $A$. It is invariant under isogenies.

Proof: 1, 2: Let $Z = \ker([n])$, then it is proper. By (13.5.1.25), choose an ample line bundle $\mathcal{L} = \mathcal{L}(D) \in \text{Pic}(A)$, then $\mathcal{O}_Z = \mathcal{L}_Z^{n+1/2} \otimes [-1]^* \mathcal{L}_Z^{n-1/2}$. As $\mathcal{L}_Z$ and $[-1]^* \mathcal{L}_Z$ are both ample, $\mathcal{O}_Z$ is ample. Now (5.4.4.20) shows $\mathcal{Z}$ is finite. Thus by dimension equation, $[n]$ is finite and faithfully flat.

The action of $[n]$ on the tangent space at the origin is given by multiplying by $n$ by (7.2.2.1), thus it is unramified at the origin iff $n \in Z \cap k^\times$ by (5.6.5.12), and also on any other closed points by homogeneity. Thus if $n \in Z \cap k^\times$, $[n]$ is finite étale, and otherwise $[n]$ is not separable, by (5.6.5.12), as it is not generically unramified.

To calculate $A[n]$ in the étale case, notice $[n]^*D = n^2D$, and the intersection number formula

$$n^{2g}(D \cdot D \cdot \ldots \cdot D) = ([n]^*D \cdot [n]^*D \cdot \ldots \cdot [n]^*D) = \deg([n])(D \cdot D \cdot \ldots \cdot D)$$

where the intersection is $g$-fold, thus $(D \cdot D \cdot \ldots \cdot D)$ equals the degree of the projection embedding of $X$ via $\mathcal{L}(D)$ thus positive, so we get $\deg([n]) = n^{2g} = \#A[n]$ as $[n]$ is finite étale. To see the structure of $A[n]$, notice this is true for any $m/n$.

3: Cf. [Conrad]. The last assertion follows from the fact the fact $[p]$ is surjective and the structure theory of Abelian groups. \hfill \Box
13.5. ARITHMETIC OF ABELIAN VARIETIES

**Def. (13.5.6.15) [Tate Modules].** Let \( k \in \text{Field}, A \in \text{AbVar} / k \). For \( \ell \in \mathbf{P} \setminus \text{char} \, k \), define \( T_\ell(A) = \varprojlim_{n \geq 0} A[\ell^n] \), called the **Tate module** of \( A \). Then it is naturally a \( \mathbb{Z}_\ell \)-module and isomorphic to \( \mathbb{Z}_\ell^{2g} \) by (13.5.6.14).

Thus we can define \( V_\ell(A) = T_\ell(A) \otimes_{\mathbb{Z}_\ell} \mathbb{Q}_\ell \). There are Galois actions on them, as \( \ell^n \) is étale and Galois preserves \( A[\ell^n] \) because \( O \) is Galois-invariant.

For \( \ell = \text{char} \, k = p > 0 \), we can also define \( T_p(A) \), which is isomorphic to \( \mathbb{Z}_p^{2g} \) for some \( 0 \leq r \leq g \) by (13.5.6.14), but there is not Galois action on it.

**Def. (13.5.6.16) [Adelic Tate Modules].** Situation as in (13.5.6.15), if \( \text{char} \, k = 0 \), define the **Adelic Tate module** to be

\[
T_f(A) = \prod_{\ell \in \mathbf{P}} T_\ell(A), \quad V_f(A) = \prod_{\ell \in \mathbf{P}} (V_\ell(A), T_\ell(A)).
\]

**Prop. (13.5.6.17) [Étale Cohomology and Tate Modules].** Let \( k = k^s \) and \( A \in \text{AbVar} / k \), and \( \ell \in \mathbf{P} \setminus \text{char} \, k \), then

- There is a canonical isomorphism \( H^1_{\text{ét}}(A, \mathbb{Z}_\ell) \cong \text{Hom}_{\mathbb{Z}_\ell} (T_\ell(A), \mathbb{Z}_\ell) \). Thus \( H^1_{\text{ét}}(A, \mathbb{Z}_\ell) \cong \mathbb{Z}_\ell^{2g} \) by (13.5.6.14).
- The cup product defines isomorphisms \( \wedge^r H^1_{\text{ét}}(A, \mathbb{Z}_\ell) \cong H^r(A, \mathbb{Z}_\ell) \) for any \( r > 0 \).

**Proof:** Cf.[Mil08]P55. \( \square \)

**Cor. (13.5.6.18).** There is a natural Galois-invariant pairing \( \wedge^r T_\ell(A) \times H^r_{\text{ét}}(A, \mathbb{Z}_\ell) \to \mathbb{Z}_\ell \).

**Prop. (13.5.6.19) [Semisimplicity].** Let \( F \in \text{Field}, \ell \in \mathbf{P} \setminus \text{char} \, F, A \in \text{AbVar} / F \), then the action of Gal\( F \) on \( V_\ell(A) \) is semisimple.

**Proof:**

\( \square \)

7 Polarizations and Weil Pairings

Polarizations and Rosati Involutions

**Def. (13.5.7.1) [Polarizations].** Let \( k \in \text{Field}, \) a **polarization** of an Abelian variety \( A \in \text{AbVar} / k \) is an isogeny \( \lambda : A \to \tilde{A} \) that \( \lambda^* = \varphi_L \) for some ample invertible sheaf \( L \in \text{Pic}(A_{\bar{k}}) \). A **principal polarization** of an Abelian variety is a polarization of degree 1.

The category of Abelian varieties over \( k \) of dimension \( g \) together with a polarization of degree \( d \) is denoted by \( \text{AbVar}^{\text{dim}=g, \text{polar} = d} / k \).

**Prop. (13.5.7.2) [Zariski’s Trick].** For any \( k \in \text{Field} \) and \( A \in \text{AbVar} / k \), \((A \times A^\vee)^4 \) is canonically principally polarized.

**Proof:** Cf.[Mil08]P60. \( \square \)

**Prop. (13.5.7.3) [Finitely Many Polarizations].** Let \( k \in \text{Field} \) and \( A \in \text{AbVar} / k \), then for any \( d \in \mathbb{Z}_+ \), there are only f.m. isomorphism classes of polarizations on \( A \) of degree \( d \).

**Proof:** Cf.[Mil08]P63. \( \square \)

**Def. (13.5.7.4) [Rosati Involution].**

**Prop. (13.5.7.5).** Let \( k \in \text{Field} \) and \((A, \lambda) \in \text{AbVar} / k \), then

- \( \# \text{Aut}((A, \lambda)) < \infty \).
- for any \( n \geq 3 \), any automorphism of \((A, \lambda)\) acting trivially on \( A[|n|] \) is the identity.
**Weil Pairings**

**Proposition (13.5.7.6) [Weil Pairing for Elliptic Curves].** Let \( E \in \mathcal{E}/k \), then for any \( m \in \mathbb{Z} \cap k^* \), there is a non-degenerate pairing \( e_m : E[m] \times E[m] \to \mu_m \) that is alternating, non-degenerate and \( \text{Gal}_k \)-invariant.

Moreover, \( e_{mm'}(S,T) = e_m([m']S,T) \) for \( S \in E[mm'] \) and \( S \in T[m] \). In particular, for \( \ell \in \mathbb{P} \setminus \text{char} \ k \), we can define a Weil pairing on the Tate module \( e : T_\ell(E) \times T_\ell(E) \to \mu_{\ell^\infty} \).

**Proof:** Let \( T \in E[m] \), then by (13.8.1.21), there exists some \( f \in \overline{K}(E)^* \) s.t. \( \text{div}(f) = m[E] - m[O] \).

Let \( T' \in E[m^2] \) s.t. \( mT' = T \), then there exists a function \( g \in \overline{K}(E)^* \) s.t.

\[
\text{div}(g) = [m]^*(T) - [m]^*(O) = \sum_{R \in E[m]} ([T' + R] - [R]).
\]

Notice \( f \circ [m] \) and \( g^m \) have the same divisor, so we may assume \( f \circ [m] = g^m \). Then for any \( S \in E[m] \) and \( X \in E \), \( g(S + X)^m = f(mX) = g(X)^m \), so \( E \to \mathbb{P}^1 : g(X + S)/g(X) \) is constant and has value in \( \mu_m \), denote it by \( e(T,S) \).

For bilinearity, Cf.[Sil16]P94?.

For alternating, Cf.[Sil16]P94?.

For non-degeneracy, if \( e_m(S,T) = 1 \) for any \( T \in E[m] \), then \( g \in E[m]-\text{invariant}, which implies \( g = h \circ [m] \) for some \( h \in \overline{K}(E)^* \) by (13.5.6.3) and the fact \( [m] \) is separable. Then \( (h \circ [m])^m = f \circ [m] \), so \( f = h^m \), and \( \text{div}(h) = [T] - [O] \), so \( T = O \).

Galois invariance is clear.

The last assertion follows by taking \( g' = g \circ [m'] \) and \( f' = f^{m'} \).

**Corollary (13.5.7.7) [Primitive Pairing].** Let \( E \in \mathcal{E}/k \), then for any \( m \in \mathbb{Z} \cap k^* \), \( \mu_m \subset K(E[m]) \), and there exists some \( S,T \in E[m] \) s.t. \( e_m(S,T) \) is a primitive \( m \)-th roots of unity.

**Proof:** If the subgroup generated by all \( e_m(S,T) \) is \( \mu_d \), then \( e_m([d]S,T) = 1 \) for any \( S,T \in E[m] \), so \( [d]S = 0 \) by non-degeneracy, so \( d = m \) because \#\( E[m] = (\mathbb{Z}/(m))^2 \). Then the \( \text{Gal}_k \)-invariance of \( e \) shows \( \mu_m \subset K(E[m]) \).

**Proposition (13.5.7.8) [Duality with Isogenies].** Let \( \varphi : E_1 \to E_2 \) be an isogeny between elliptic curves over a field \( k \), \( m \in \mathbb{Z} \cap k^* \), then for \( S \in E_1[m], T \in E_2[m] \),

\[
e_m(S,\hat{\varphi}(T)) = e_m(\varphi(S),T).
\]

In particular, for \( S \in T_\ell(E_1) \) and \( T \in T_\ell(E_2) \), \( e(S,\hat{\varphi}(T)) = e(\varphi(S),T) \).

**Proof:** Cf.[Sil16]P97?.

**Proposition (13.5.7.9).** Let \( E \in \mathcal{E}/k \) and \( \varphi \in \text{End}(E), \varphi \in \text{End}(E), \ell \in \mathbb{P} \setminus \text{char} \ k \), then \( \det(\varphi_\ell) = \deg(\varphi), \text{tr}(\varphi_\ell) = 1 + \deg(\varphi) - \deg(1 - \varphi) \).

**Proof:** For any \( v, v' \in T_\ell(E) \), use the Weil pairing:

\[
e(v,v')^{\deg(\varphi)} = e([\deg(\varphi)]v, v') = e(\varphi_\ell v, \varphi_\ell v') = e(v, v')^{\det(\varphi_\ell)},
\]

thus \( \deg(\varphi) = \det(\varphi_\ell) \). The latter equality follows from the identity \( \text{tr}(A) = 1 + \det(A) - \det(1 - A) \) for any \( A \in M_2(R) \).
8 Over Archimedean Local Fields

Prop. (13.5.8.1) [Complex Abelian Varieties and Complex Tori]. By (11.8.5.9) and GAGA (11.7.6.17), the category of Abelian varieties over $\mathbb{C}$ is the same as the category of complex tori $V/\Lambda$ with a Riemann form $\omega$.

Such a complex tori $V/\Lambda$ with a Riemann form $\omega$ is called a polarizable integral Hodge structure.

Prop. (13.5.8.2) [Rosati Involutions are Positive]. Let $X = V/\Lambda \in \text{AbVar}/\mathbb{C}$, then for any $\alpha \in \text{End}_{\mathbb{Q}}(X)$, there exists $\alpha' \in \text{End}_{\mathbb{Q}}(X)$ s.t.

$$\omega(\alpha x, y) = \omega(x, \alpha'y).$$

And this determines an involution on $\text{End}_{\mathbb{Q}}(X)$, called the Rosati involution. Notice this is compatible with that defined in (13.5.7.4), by using (11.8.5.10).

Then this is a positive involution on $\text{End}_{\mathbb{Q}}(X)$.

Proof: Notice the form $\omega_J : (x,y) \mapsto \omega(x,Jy)$ is symmetric and positive, and

$$\omega_J(\alpha x, y) = \omega(x, J\alpha'y) = \omega(x, J\alpha'y) = \omega_J(x, \alpha'y).$$

So this involution is positive by (13.9.2.19).

Thm. (13.5.8.3) [Frobenius-Lefschetz-Poincaré-Riemann-Weierstrass]. The functor $\mathbf{A} \mapsto H^1(A, \mathbb{Z})$ defines an equivalence from $\text{AbVar}/\mathbb{C}$ to the category of polarizable integral Hodge structures of type $\{(−1,0), (0,−1)\}$.

Proof: ?

Elliptic Curve Case

Prop. (13.5.8.4) [Complex Tori as Elliptic Curves]. Let $\Lambda$ be a complete real lattice of $\mathbb{C}$, then we can make $\mathbb{C}/\Lambda$ into a Riemannian surface as the quotient space of $\mathbb{C}$. Then it is positive by??t is a smooth curve of genus 1 with the origin as the rational point, which means it is an elliptic curve.

Prop. (13.5.8.5) [Elliptic Curve as Complex Tori]. For an elliptic curve $\mathbb{C}/\Lambda$ over $\mathbb{C}$, by (10.5.7.7), the Weierstrass functions (10.5.7.5) $\Psi, \Psi'$ are just the rational functions in (13.8.1.6), so the map

$$z \mapsto [\Psi(z), \Psi'(z), 1]$$

is biholomorphic from $\mathbb{C}/\Lambda$ to the elliptic curve defined by the Weierstrass equation $y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda)$ that $g_2^3 - 27g_3^2 \neq 0$. And it also preserves the group structure.

Proof: To show that the homomorphism preserves group structure, notice that if $z_1, z_2, z_3$ maps to three points that is colinear, then they satisfy a equation

$$f(z) = a\Psi(z) + b\Psi'(z) + c.$$

If $b \neq 0$, then this is a meromorphic function with three poles, thus three zeros, which is exactly $z_1, z_2, z_3$, so by (10.5.7.2), $z_1 + z_2 + z_3 \equiv 0 \mod \Lambda$. If $b = 0$, then $z_3 = 0$, which corresponds to the point $(1,0,0) \in \mathbb{P}^2$, then the same argument shows $z_1 + z_2 + 0 \equiv 0 \mod \Lambda$. □
Lemma (13.5.8.6) [Isogenies and Homogeneities]. If $E_1, E_2$ are elliptic curves in $\mathbb{P}^2$ corresponding to $\Lambda_1, \Lambda_2$ via (13.5.8.5) resp., then the natural map

$$\{\text{isogenies } E_1 \to E_2\} \to \{\text{non-constant holomorphic maps } \varphi : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2, \varphi(0) = 0\}$$

is a bijection.

Proof: By (11.8.5.2), it suffices to show for any lattices $\Lambda_1, \Lambda_2$ and $\alpha \in \mathbb{C}^*$ that $\alpha \Lambda_1 \subset \Lambda_2$, the map

$$[\Psi(z, \Lambda_1), \Psi'(z, \Lambda_1), 1] \to [\Psi(\alpha z, \Lambda_2), \Psi'(\alpha z, \Lambda_2), 1]$$

is a morphism. For this, notice $\Psi(\alpha z, \Lambda_2)$ is an elliptic function for $\Lambda_1$, thus by (10.5.7.7), it is a rational function of $\Psi(z, \Lambda_1)$ and $\Psi'(z, \Lambda_1)$.

Lemma (13.5.8.7). Let $E \in \mathbb{C}$ be an elliptic curve in $\mathbb{P}^2$ defined by a Weierstrass equation, then there exists a lattice $\Lambda \subset \mathbb{C}$, unique up to homothety, that the embedding given in (13.5.8.5) induces an isomorphism $\mathbb{C}/\Lambda \cong E(\mathbb{C})$.

Proof: This is a consequence of (10.5.7.8) and (13.8.1.13).

Prop. (13.5.8.8) [Elliptic Curves and Complex Tori]. The following categories are equivalent:

- Category of elliptic curves over $\mathbb{C}$ with morphisms given by isogenies.
- Category of complex tori with morphisms homomorphisms preserving 0.
- Category of lattices in $\mathbb{C}$ with homotheties as morphisms.

Proof: This is a consequence of (13.5.8.5)(13.5.8.6) and (11.8.5.2).

Prop. (13.5.8.9) [Complex Multiplication]. Let $E/\mathbb{C}$ be an elliptic curve, and let $\omega_1, \omega_2$ be a generator of the lattice $\Lambda$ corresponding to $E(13.5.8.8)$, then one of the following is true:

- $\text{End}(E) \cong \mathbb{Z}$.
- $\mathbb{Q}(\omega_2/\omega_1)$ is an imaginary quadratic extension of $\mathbb{Q}$ and $\text{End}(E)$ is isomorphic to an order of $\mathbb{Q}(\omega_2/\omega_1)$.

Proof: Cf.[Sil16]P176.?

Prop. (13.5.8.10). Let $E/\mathbb{C}$ be an elliptic curve and $\Lambda$ a lattice in $\mathbb{C}$ that $E(\mathbb{C}) \cong \mathbb{C}/\Lambda$, then

- there is a natural isomorphism $H_1(E(\mathbb{C}), \mathbb{Z}) \cong \Lambda : \gamma \mapsto \int_{\gamma} dz$.
- There is a natural isomorphism $H_1(E(\mathbb{C}), \mathbb{Z}/(m)) \cong E[m]$.

Proof: Cf.[Sil16]P176.

Over $\mathbb{R}$

Prop. (13.5.8.11). Let $E \in \mathbb{E}ll/\mathbb{R}$, then there exists a unique $\tau$ in the set

$$\mathcal{C} = \{it | t \geq 1\} \cup \{e^{i\theta}|\pi/3 \leq \pi/2\} \cup \{1/2 + it | t \geq \sqrt{3}/2\}.$$

s.t. $j(\tau) = j(E)$. And by (13.8.6.3), each $\tau \in \mathcal{C}$ corresponds to exactly two isomorphism classes of elliptic curves over $\mathbb{R}$.
Proof: Firstly these $\tau$ satisfies $j(\tau) \in \mathbb{R}$ because by the power expansions of $j(\tau)(15.11.5.10)$, for $\tau = it$ or $1/2 + it$, $q \in \mathbb{R}$, thus $j(\tau) \in \mathbb{R}$. For $\tau = e^{i\theta}$, $j(e^{i\theta}) = j(-e^{-i\theta}) = j(e^{i\theta})$ as $j \in M_0(\Gamma(1))$.

Next it can be proven $j(i\infty) = +\infty$ and $j(1/2+i\infty) = -\infty$, and $j$ is injective on $\mathbb{C}$ by (15.11.5.10). Thus the assertion follows by continuity. □

Remark (13.5.8.12). Notice by action of $\alpha = \begin{bmatrix} 0 & -1 \\ 1 & -1 \end{bmatrix} \in \text{SL}(2, \mathbb{Z})$ on $\{e^{i\theta}|\pi/2 \leq \pi/3\}$, we can also replace $\mathbb{C}$ by $\mathbb{C}' = \{it|t \geq 1\} \cup \{1/2 + it|t > 1\}$. 9 char $k > 0$ Case

Prop.(13.5.9.1). If $k \in \text{Field}, \#k < \infty$, then for any $g, d > 0$, $\#_{\text{AbVar}}^{\text{dim}=g, \text{polar}=d^2}/k < \infty$.

Proof: Cf.[Mil08]P54. □

Prop.(13.5.9.2). Let $p \in \mathbb{P}, q \in p^{\mathbb{Z}}$, and $(A, \lambda) \in \text{AbVar}^{\text{polar}}/\mathbb{F}_q$ with Rosati involution $\dagger \in \text{End}(A)_{\mathbb{Q}}$, then $\text{Frob}_{q,A}^\dagger \circ \text{Frob}_{q,A} = [q]$.

Proof: Cf.[Mil08]P76. □

Honda-Tate Theory

Prop.(13.5.9.3)[Weil Conjecture for Abelian Varieties]. For $p \in \mathbb{P}$, $r \in \mathbb{Z}_+, q = p^r, \ell \in \mathbb{P}\setminus\ell$, and $A \in \text{AbVar}^g/\mathbb{F}_q$, let $\varphi_A = \varphi^r$ be the Frobenius of $A$, and let $P_{\varphi}(X)$ be the characteristic polynomial of the action of $\varphi_A$ on $T_\ell(A)$, then

- $P_{A,\ell}(X) \in \mathbb{Z}[X]$, and is invariant of $\ell$ chosen. Thus we omit $\ell$ from now on.
- $P_{A,\ell}(X) = \prod_{i=1}^{2g}(X - \alpha_i)$, where $\alpha_i \in \mathbb{C}$ and $|\alpha_i| = q^{1/2}$.
- $\#A(\mathbb{F}_q^m) = \prod_{i=1}^{2g}(1 - \alpha_i^m)$.

In particular,

$$|\#A(\mathbb{F}_q^m) - q^{mg}| \leq 2gq^{m - 1/2} + (4^g - 2g - 1)q^m(g - 1).$$

Proof: These follow from (13.5.6.17) and Weil conjecture (13.12.2.6)(16.1.1.4). □

Thm.(13.5.9.4)[Honda-Tate].

10 Reductions

over DVRs

Prop.(13.5.10.1)[Good Reductions]. Let $(R, K, k)$ be a DVR and $A \in \text{AbVar}/K$, then $A$ has good reduction over $R(13.7.1.2)$ iff there exists $\tilde{A} \in \text{AbVar}/R$ with generic fiber $A$. In this case, $A(K) \cong \tilde{A}(R) \to \tilde{A}(k)$ is a surjective map of Abelian groups.

It will be shown in (13.5.15.7) that a good reduction is unique if it exists.
Def. (13.5.10.2) [Conductor]. Let $E$ be an elliptic curve over $F$, then the **conductor of $E$** is defined in [Si99]P380.

If $F = \mathbb{Q}$, then the conductor $N_E = \prod_{p \in \mathcal{P}} p^{f_p}$, where

$$f_p = \begin{cases} 0, & E \text{ has good reduction at } p \\ 1, & E \text{ has multiplicative reduction at } p \\ 2, & E \text{ has additive reduction at } p & \& p \neq 2, 3 \\ 2 + \delta_p, & E \text{ has additive reduction at } p & \& p = 2, 3 \end{cases}$$

where $0 \leq \delta_2 \leq 6, 0 \leq \delta_2 \leq 3$.

**Proof:**

Prop. (13.5.10.3) [Semistable Reduction Theorem].

- If $K'/K$ is a finite extension, and $E$ has stable or semistable reduction, then the reduction type of $E_{K'}$ is the same as that of $E$.
- If $K'/K$ is a finite unramified extension, then the reduction type of $E_{K'}$ is the same as that of $E$.
- There exists a finite extension $K'/K$ s.t. $E_{K'}$ is of stable or split semistable reduction type.

**Proof:**

1: For these two cases, $c_4$ and $\Delta$ cannot be reduced anymore to another minimal Weierstrass equation by (13.8.4.4).

2: It suffices to consider the additive reduction case: ? The short Weierstrass equation case is clear, for the general case, use Tate’s algorithm.

3: Use the Legendre or Deuring form (13.8.1.16)(13.8.1.17) to analyze $\Delta$ and $c_4$.

Thm. (13.5.10.4) [Néron-Ogg-Shafarevich Criterion]. Let $(R, K, k)$ be a DVR and $A \in \text{AbVar}/K, \ell \in \mathcal{P}\setminus \text{char } k$, then the following are equivalent:

- $A$ has good reduction.
- The module $|A[m]|$ is unramified as a $\text{Gal}_K$-module, for all $m \in \mathbb{Z} \setminus \text{char } k$.
- The Tate module $T_{\ell}(A)$ is unramified for all(some) primes $\ell \in \mathcal{P}\setminus \text{char } k$.
- The module $A[m]$ is unramified for infinitely many $m \in \mathbb{Z} \setminus \text{char } k$.

**Proof:**

2 $\rightarrow$ 3 $\rightarrow$ 4 are obvious.


1 $\rightarrow$ 2: Let $K'$ be the finite extension of $K$ generated by $E[m]$, then (13.5.10.3) implies $E_{K'}$ has the same reduction type as $E$. Then by (13.8.4.20), $E[m] \rightarrow E_{K'}(k')$ is an injection. So clearly $I_v$ acts trivially on $E[m]$.

4 $\rightarrow$ 1: Let $m \in \mathbb{Z} \setminus \text{char } k$ s.t. $E[m]$ is unramified and $m > \#E(K^{ur})/E_0(K^{ur})$, where $\#E(K^{ur})/E_0(K^{ur}) < \infty$ by (13.8.4.16). Then because $E[m] \cong (\mathbb{Z}/(m))^2 \subset E(K^{ur})$, $E_0(K^{ur})$ contains some subgroup isomorphic to $(\mathbb{Z}/(\ell))^2$ for some $\ell \in \mathcal{P}\setminus \text{char } k$, thus by (13.8.4.20), $E_{\text{sm}}(E)$ contains some subgroup isomorphic to $(\mathbb{Z}/(\ell))^2$. But by (13.8.1.15), this is possible only when $E_{\text{sm}} = E$. Thus $E_{K^{ur}}$ has good reduction, so $E$ also has good reduction by (13.5.10.3).

Cor. (13.5.10.5). If $0 \rightarrow A' \rightarrow A \rightarrow A'' \rightarrow 0$ are exact sequences of Abelian varieties over $K$ and $A$ has good reduction, then $A'$, $A''$ also have good reductions.
Cor. (13.5.10.6) [Isogeny and Good Reductions]. Let \((R, K, k)\) be a DVR and \(A \rightarrow A' \in \text{AbVar}/K\) is an isogeny, then \(A\) has good reduction iff \(A'\) does.

Proof: Use (13.5.10.4) and the fact if \(\ell \in \mathcal{P}\) is prime to char \(k\) and deg \(\varphi\), then \(\varphi_\ell : T_\ell(A) \rightarrow T_\ell(A')\) is an isomorphism of \(\text{Gal}_K\)-modules.

Prop. (13.5.10.7). If \(K \in p\text{-Fields}, \ell \in \mathcal{P} \setminus p\) and \(A \in \text{AbVar}/K\) satisfies \(\rho_{\ell,A}(\text{Gal}_K)\) has finite image, then \(A\) has potential good reduction.

Proof: It follows from class field theory that the image of \(I_K\) is a quotient of \(\mathcal{O}_K^*\), which contains a pro-\(p\)-group of finite index, and \(\text{End}(T_\ell(A))\) contains a pro-\(\ell\)-group of finite index, so the image is finite. Then \(A\) has potential good reduction by (13.5.10.4).

Thm. (13.5.10.8) [Néron-Ogg-Shafarevich Criterion for Elliptic Curves]. Let \(K\) be a CDVR, \(\ell \in \mathcal{P} \setminus \text{char } k\) and \(A \in \text{AbVar}/K\), then
- \(A\) has good reduction iff \(T_\ell(A)\) is an unramified \(\text{Gal}_K\)-module.
- \(A\) has good or semistable reduction iff \(I_K\) acts unipotently on \(T_\ell(A)\).
- \(A\) has potential good reduction iff \(T_\ell(E)\) is potentially unramified, i.e. \(\rho_{\ell,A}(I_K)\) is finite.

Proof: 1 follows from (13.5.10.4).

2: We only prove for \(\dim A = 1\) case?: As \(I_K\) acts trivially on \(\det(T_\ell(E))\) by (14.1.6.3), it acts unipotently on \(T_\ell(E)\) if it has a fixed vector. If it has a fixed vector, then \(\tilde{E}_{\text{sm}}(\overline{K})\) contains a subgroup isomorphic to \(\mathbb{Z}/(\ell)\), which is possible only if \(E\) has semistable or good reduction, by (13.8.1.15) and (13.5.10.3). The converse is proved the same way as that of (13.5.10.4).

3 follows from (2.2.5.11).

Cor. (13.5.10.9). If \(K\) is a CDVR with residue characteristic \(p\) and \(\varphi : E \rightarrow E'\) is an isogeny of degree \(p\) of elliptic curves over \(K\), then \(E\) has good reduction of ordinary type/supersingular type iff \(E'\) does.

Proof: By (13.5.10.6) we can assume both \(E, E'\) have good reductions, then their minimal Weierstrass equations are their Néron models, thus by definition \(\varphi\) extends to a map \(\tilde{\varphi} : \tilde{E} \rightarrow \tilde{E}'\). Let \(\psi = \tilde{\varphi}\), then we also have \(\tilde{\psi} : \tilde{E}' \rightarrow \tilde{E}\) s.t. \(\tilde{\varphi} \circ \tilde{\psi} = [p]_{\tilde{E}}\), and \(\tilde{\varphi} \circ \tilde{\psi} = [p]_{\tilde{E}'}\). Thus \([p]_{\tilde{E}} \circ \tilde{\varphi} = \tilde{\varphi} \circ [p]_{\tilde{E}}\), which implies \(\deg_{\ast}([p]_{\tilde{E}}) = \deg_{\ast}([p]_{\tilde{E}'})\), thus we are done by (13.8.3.4).

Prop. (13.5.10.10) [Isogeny and Semistability]. If \(A, B \in \text{AbVar}/k\) are isogenous, then \(A\) is semistable iff \(B\) is semistable.

Proof: ?

over Dedekind Domains

Def. (13.5.10.11) [Conductor]. For an elliptic curve \(E\) over a global field \(K\), the conductor of \(E\) is defined to be the integral ideal of \(K\) given by

\[ N_{E/K} = \prod_{v \in \Sigma_K^0} p_v^{f_v} \]

where \(f_v\) is the local conductors (13.5.10.2).
**Conj.** (13.5.10.12) [Szpiro]. For any $\varepsilon > 0$, there exists $C_\varepsilon > 0$ s.t.

$$|N_{K/Q}(\Delta_E)| \leq C_\varepsilon |N_{K/Q}(N_E)|^{6+\varepsilon}$$

for any $E \in \mathfrak{ell}/\mathbb{Q}$, where $N_E$ is the conductor of $E$.

**Proof:** \hfill \Box

**Prop.** (13.5.10.13) [No Everywhere Good Reduction over $\mathbb{Q}$]. There are no elliptic curve $E$ over $\mathbb{Q}$ with everywhere good reductions. There are 24 elliptic curves over $\mathbb{Q}$ with good reductions away from 2, and 784 elliptic curves over $\mathbb{Q}$ with good reduction away from 2, 3.

**Proof:** Let $E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$ be an elliptic curve over $\mathbb{Q}$ with $a_i \in \mathbb{Z}$ and $\Delta = \pm 1$, then $a_1$ must be odd, otherwise $\Delta \equiv 5 b_0^2 = \pm 1 \mod 8$ is impossible. Thus $c_4 = b_2^2 - 24 b_4 \equiv 1 \mod 8$. And $c_3^2 - c_2^3 = (\pm 12)^3$ shows that $c_4 \pm 12$ is a square or 3 times a square, which are both impossible by modulo 8.

For good reduction away from 2, 3? \hfill \Box

**Prop.** (13.5.10.14). Let $F$ be a number field and $A, B \in \mathrm{AbVar}/F$, and $S \subset \Sigma_F$ is a finite set of places of $F$ containing $\Sigma_F^0$ and all places s.t. $A$ or $B$ has bad reduction, then for any $\ell \in \mathbb{P} \ s.t. \ S(\ell) \cap S = \emptyset$, there exists a finite set $T = T(S, \ell, g) \subset \Sigma_\infty$ s.t. $T \cap (S \cup S(\ell)) = \emptyset$, and

$$P_\ell(\tilde{A}, t) = P_\ell(\tilde{B}, t) \Rightarrow A \sim B$$

**Proof:** Cf.[Mil08]P142. \hfill \Box

**Prop.** (13.5.10.15) [Reduction Theorem]. For any number field $F$ and $A \in \mathrm{AbVar}/F$, there exists a finite extension $L/F$ s.t. $A_L$ is semistable.

**Proof:** ? \hfill \Box

11 Galois Cohomologies

**Prop.** (13.5.11.1) [Fundamental Exact Sequence]. Let $\varphi : X \to X'$ be an étale isogeny between Abelian varieties over a field $k$, then there is an exact sequence

$$0 \to \ker(\varphi)(k^s) \to X(k^s) \to X'(k^s) \to 0$$

by (7.1.5.5), thus taking Galois cohomology, there is an exact sequence

$$0 \to X'(k)/\varphi(X(k)) \xrightarrow{\delta} H^1(G_k, X[\varphi]) \to H^1(G_k, X)[\varphi] \to 0.$$

**Cor.** (13.5.11.2). By (13.5.6.14), if $n \neq 0 \in \mathbb{Z} \cap K$, then there is an exact sequence

$$0 \to X(k^s)/n X(k^s) \xrightarrow{\delta} H^1(G_k, X[n]) \to H^1(G_k, X)[n] \to 0.$$  

And the first map is described as follows: for $P \in X(k^s)$, let $[n]Q = P$ where $Q \in K(k^s)$, then $P$ is mapped to the 1-cocycle $f(\sigma) = \sigma(Q) - Q$.  

**Prop. (13.5.11.3)**. Let $F$ be a global field or the function field of a non-singular smooth curve over an alg.closed field $k$, $\varphi : X \to X'$ an étale isogeny of Abelian varieties over $F$, then by restriction (10.1.1.10), there is an exact sequence

\[
0 \to X'(K)/\varphi(X(K)) \to H^1(G_K, X[\varphi]) \to H^1(G_K, X)[\varphi] \to 0.
\]

Where $v$ are extended to $K^s$ arbitrarily.

**Def. (13.5.11.4) [Selmer Groups]**. Let $F$ be a global field or the function field of a non-singular smooth curve over an alg.closed field $k$, $\varphi : A \to A'$ an étale isogeny of Abelian varieties over $F$, the $\varphi$-Selmer group of $A/F$ is a subgroup of $H^1(\text{Gal}_F, A[\varphi])$ defined by

\[
\text{Sel}^\varphi(A/F) = \ker(H^1(\text{Gal}_K, A[\varphi]) \to \prod_{v \in \Sigma_F} H^1(\text{Gal}_{K_v}, A)).
\]

Notice the kernel is independent of the extension of $v$ to $K^s$, because any two such extensions induces conjugate groups $G_{K_v}$ in $G_K$ and use (10.1.1.12).

**Def. (13.5.11.5) [Shafarevich-Tate Group]**. The Shafarevich-Tate group of $A/F$ is the subgroup of $H^1(G_F, A[\varphi])$ defined by

\[
\Pi(A/F) = \ker \left( H^1(G_F, A) \to \prod_{v \in \Sigma_F} H^1(\text{Gal}_{K_v}, A) \right).
\]

Notice the kernel is independent of the extension of $v$ to $K$, because any two such extensions induces conjugate $G_{K_v}$ in $G_K$ and use (10.1.1.12).

For a homomorphism of Abelian varieties in $\text{AbVar}/F$, there is a natural map $\Pi(A/F) \to \Pi(B/F)$.

**Prop. (13.5.11.6) [Selmer Groups and Shafarevich-Tate Groups]**. Let $C$ be a proper Dedekind scheme or a non-singular curve over a field $k$ with fraction field $F$, $\varphi : A \to A'$ an étale isogeny of Abelian varieties over $F$, then there is an exact sequence

\[
0 \to A'(K)/\varphi(A(K)) \to \text{Sel}^\varphi(A/K) \to \Pi(A/K)[\varphi] \to 0.
\]

**Proof**: The exact sequence is a consequence of (13.5.11.3) and (13.5.11.4)(13.5.11.5). 

**Remark (13.5.11.7) [Computability]**. It is difficult to characterize $A'(K)/\varphi(A(K)) \subset \text{Sel}^\varphi(A/K)$.

**Prop. (13.5.11.8) [Sel$^\varphi(A)$ is Finite]**. Let $F$ be a global field or the function field of a non-singular smooth curve over an alg.closed field $k$, $\varphi : A \to A'$ an étale isogeny of Abelian varieties over $F$, then if $S$ is a finite set of places of $F$ containing all the places dividing $\deg(\varphi)$, and the places that $A$ has bad reductions, then any element in $\text{Sel}^\varphi(A/F)$ is unramified at all finite places outside $S$. In particular, $\text{Sel}^\varphi(A/F)$ is finite, by (10.1.3.11).
Proof: By definition of $\text{Sel}^\varphi$ and (13.5.11.3), if $\xi \in \text{Sel}^\varphi(A/F)$, then for any $v \in \Sigma^\varphi_F$, there is some $P \in A(F_v^\varphi)$ s.t. $\xi_\sigma = \sigma(P) - P \in A[\varphi]$ for any $\sigma \in G_v$. But if $A$ has good reduction at $v$ and $\sigma \in I_v$, then $\sigma(P) - P$ maps to $\hat{O} \in \hat{A}_v$. But notice $A[\varphi] \subset A[m]$ which maps injectively into $\hat{A}_v(k_v)$ by (13.8.4.20) if $v$ is not dividing $\deg(\varphi)$. Thus in this case, $\xi_\sigma = 0$ for any $\sigma \in I_v$. \qed

Cor. (13.5.11.9) [$\ell^\infty$-Selmer Rank]. If $\ell \in \mathbf{P} \setminus \text{char } F$, then the $\ell$-primary part $\text{III}(A/F)[\ell^\infty] = \lim_{n \to \infty} \text{III}(A/F)[\ell^n]$ is isomorphic to $(\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{\delta_\ell} \times \text{II}_\ell$ for some $\delta_\ell \in \mathbb{N}$ and finite group $\text{II}_\ell$, and also

$$\text{Sel}^{\ell^\infty}(A/F) = \lim_{n \to \infty} \text{Sel}^{\ell^n}(A/F),$$

called the $\ell^\infty$-Selmer group. Then by taking limits of the exact sequence in (13.5.11.6), there is an exact sequence

$$0 \to A(F) \otimes \mathbb{Q}_\ell/\mathbb{Z}_\ell \to \text{Sel}^{\ell^\infty}(A/F) \to \text{III}(A/F)[\ell^\infty] \to 0.$$  

If we define the $\ell^\infty$-Selmer rank $\text{rank}_\ell(A/F) = \text{rank}(A/F) + \delta_\ell$, then

$$\text{Sel}^{\ell^\infty}(A/F) = (\mathbb{Q}_\ell/\mathbb{Z}_\ell)^{\text{rank}_\ell(A/F)} \cdot \text{III}(A/F)[\ell^\infty],$$

where $\#\text{III}(A/F)[\ell^\infty] < \infty$. Notice $\text{rank}_\ell(A/F)$ is a cohomological number.

Conj. (13.5.11.10) [Tate-Shafarevich]. For $A \in \text{AbVar}/F$, $\#\text{III}(A/F) < \infty$.

Proof: \qed

Prop. (13.5.11.11) [Cassels-Tate Pairing]. Let $A \in \text{AbVar}/F$ and $\hat{A}$ its dual, then there is a bilinear Cassels-Tate pairing $\text{III}(A/K) \times \text{III}(\hat{A}/K) \to \mathbb{Q}/\mathbb{Z}$ and the kernel on both sides are the set of divisible elements.

Proof: Cf. [Birch and Swinnerton-Dyer Conjecture, P10]. \qed

Cor. (13.5.11.12) [Principally Polarized Case]. If $K \in \text{AbVar}/F$ has a principal polarization $\lambda$ that comes from a rational divisor $D$, then the pullback pairing $\text{III}(A/K) \times \text{III}(\hat{A}/K) \to \mathbb{Q}/\mathbb{Z}$ is alternating. In particular, if $\#\text{III}(A/F) < \infty$, then it is a perfect square, by (2.1.4.17).

In particular, if $E \in \text{Ell}/F$ and $\#\text{III}(E/F) < \infty$, then it is a perfect square.

Proof: \qed

Remark (13.5.11.13). This is not right for general Abelian varieties.

The discussion of Selmer groups and ranks are continued in BSD Conjecture 16.8.

12 Néron-Tate Heights

Prop. (13.5.12.1) [Néron-Tate Heights]. Let $X$ be an Abelian variety over a global field $K$, $\mathcal{L} \in \text{Pic}(X)$, then there are uniquely defined bilinear form $b_\mathcal{L}$, additive homomorphism $l_\mathcal{L}$ on $X(\bar{K})$ s.t.

$$\tilde{h}_\mathcal{L}(x) = \frac{1}{2} b_\mathcal{L}(x, x) + l_\mathcal{L}(x) \sim h_\mathcal{L}(x),$$

called the Néron-Tate height of $\mathcal{L}$. 

Proof: We want to use (2.1.4.13) for the Weil height (13.2.4.19) \( h_\mathcal{L} \) on \( X(\mathbb{K}) \): apply the theorem of the cube (13.5.1.21) to the projections \( \pi_i : X \times X \times X \to X \) and pullback to \( X \) via the diagonal map, then taking the Weil heights, we will get the desired relation

\[
h_\mathcal{L}(\sum_{i=1}^{3} x_i) - \sum_{1 \leq i < j \leq 3} h_\mathcal{L}(x_i + x_j) + \sum_{i=1}^{3} h_\mathcal{L}(x_i) \sim 0.
\]

\[\square\]

Cor. (13.5.12.2). The Néron-Tate height is a refinement of Weil heights (13.2.4.19) made for Abelian varieties:

- The map \( \hat{h} : \text{Pic}(X) \to \mathbb{R}^{X(\mathbb{K})} : \mathcal{L} \mapsto \hat{h}_\mathcal{L} \) is an additive homomorphism.
- (Symmetry) If \( \varphi : A \to B \) is a homomorphism of Abelian varieties, then \( \hat{h}_{\varphi^*(\mathcal{L})} = \hat{h}_\mathcal{L} \circ \varphi \).
- (Positivity) Let \( \mathcal{L} \in \text{Pic}(X) \) be even. If \( \mathcal{L} \) is base-free or ample, then \( \hat{h}_\mathcal{L} \geq 0 \).
- (Boundedness) Let \( \mathcal{L} \in \text{Pic}(X) \) be even and ample (such an \( \mathcal{L} \) exists by (13.5.1.27)), then \( \hat{h}_\mathcal{L} \) induces a symmetric bilinear form on \( X(K) \) satisfying \( \{ x \in X(\mathbb{K}) | \deg(x) \leq d, (x, x) < C \} \) is finite for all \( C > 0 \).

Proof: 1, 2 follow from the corresponding property of Weil heights (13.2.4.19) and the uniqueness in (2.1.4.13).

3: Notice that the fact \( \mathcal{L} \) is even implies \( \hat{h}_\mathcal{L} = \frac{1}{2} b(x, x) \). The ample case reduces to the base-free case, because there is a multiple \( m\mathcal{L} \) that is very ample, and then \( \hat{h}_{m\mathcal{L}} = m\hat{h}_\mathcal{L} \). For the base-free case, \( c \) is the pullback of \( O(1) \) for some morphism \( X \to \mathbb{P}^n \), thus \( h_\mathcal{L} \) is non-negative by (13.2.4.3), and \( h_\mathcal{L} \sim \hat{h}_\mathcal{L} \), thus \( \hat{h}_\mathcal{L} \) must also be non-negative.

4 follows from Northcott’s theorem (13.2.4.20).

\[\square\]

Cor. (13.5.12.3) [Positive Definiteness]. For any ample line bundle \( \mathcal{L} \in \text{Pic}(A) \), \( b_\mathcal{L} \) induces a positive definite symmetric bilinear form on \( A(\mathbb{K}) \otimes_\mathbb{Z} \mathbb{R} \)

Proof: We want to use (2.1.4.14). Notice \( b_\mathcal{L} \) is just \( 2\hat{h}_{\mathcal{L},[-1]!*\mathcal{L}} \), thus satisfies the conditions by (13.5.12.2).

\[\square\]

Prop. (13.5.12.4) [Tate’s Limiting argument].

Proof: Cf. [Diophantine Geometry, P285].

\[\square\]

Cor. (13.5.12.5). Tate’s limiting argument gives another way of constructing Néron-Tate heights. More generally, for any projective variety \( X \) over a global field \( K \), if \( \varphi : X \to X \) a morphism over \( K \), \( \mathcal{L} \) a line bundle on \( X \) and \( k, l \in \mathbb{Z}, |k| > |l| \) that

\( l\varphi^*(\mathcal{L}) = k\mathcal{L}, \)

then there is a unique function \( \hat{h}_{\varphi,\mathcal{L}} \) in the equivalent class of \( h_\mathcal{L} \) that

\( \hat{h}_{\varphi,\mathcal{L}}(\varphi(x)) = k\hat{h}_{\varphi,\mathcal{L}}(x). \)

In particular, the Néron-Tate heights on an Abelian variety for an even or odd line bundle is obtained by taking \( \varphi = [m] \) for some \( m \geq 2 \).
Proof: Assume $l \neq 0$, consider the subgroup $\mathcal{N} = \{\lambda^r | r \in \mathbb{N}\}$, where $\lambda = k/l$, and $\mathcal{N}$ acts on $X(\overline{K})$ by $\lambda^r \cdot x = \varphi^r(x)$, then $\hat{h}_\mathcal{L}$ is quasi-homogenous of degree 1, so Tate’s limiting argument (13.5.12.4) shows

$$\hat{h}_{\varphi,\mathcal{L}}(x) = \lim_{r \to \infty} \lambda^{-r}h_\mathcal{L}(\varphi^r(x))$$

satisfies the requirement. And similarly, it is non-negative if $c$ is ample or base-free. \qed

Prop. (13.5.12.6) [Zero of Heights and Torsion]. If $F$ is a global field, $A \in \text{AbVar}/F$ and $\mathcal{L}$ is ample, then $\hat{h}_{\varphi,\mathcal{L}}(x) = 0$ iff $x$ is preperiodic, i.e. the sequence $\{x, \varphi(x), \varphi^2(x), \ldots\}$ is finite.

In particular, $\hat{h}_\mathcal{L}(x) = 0$ iff $x$ is torsion.

Proof: Assume $l \neq 0$. If $x$ is preperiodic, then clearly $\hat{h}_{\varphi,\mathcal{L}}(x) = \lim_{r \to \infty} \lambda^{-r}h_\mathcal{L}(\varphi^r(x)) = 0$. Conversely, if $\hat{h}_{\varphi,\mathcal{L}}(x) = 0$, then $\hat{h}_{\varphi,\mathcal{L}}(\varphi^r(x)) = 0$ for any $r$, then $|h_\mathcal{L}(\varphi^r(x))| \leq |\hat{h}_{\varphi,\mathcal{L}}(\varphi(x))| + C(\varphi, \mathcal{L}) = C(\varphi, \mathcal{L})$ is bounded and also $\varphi^r(x) \in X(k(x))$, thus has bounded degree. So by Northcott’s theorem (13.2.4.20), there are only f.m. such points. \qed

Cor. (13.5.12.7) [Kronecker]. The height (13.2.4.5) of a $\zeta \in \overline{Q}$ equals 0 iff it is a root of unity.

Proof: This is a special case of (13.5.12.6), where $\varphi : \mathbb{P} \to \mathbb{P} : [x, y] \mapsto [x^n, y^n]$ and $\mathcal{L} = \mathcal{O}(1)$, thus the preperiodic points are just $0, \infty$ and all the roots of unity. \qed

Prop. (13.5.12.8) [Néron-Tate Pairings]. Let $K$ be a number field and $A \in \text{AbVar}/K$, then $A \times \hat{A}$ is also an Abelian variety with the even Poincaré class $p(13.5.4.6)$, thus generating a function:

$$\hat{h}_{A \times \hat{A}, p} : A(\overline{K}) \times \hat{A}(\overline{K}) \to \mathbb{R}.$$ 

Then in fact this pairing is bilinear, called the Néron-Tate pairing $\langle \cdot, \cdot \rangle_{A,K}$.

The Weil-Tate pairing satisfies the functoriality property: If $f : A \to B$ is a homomorphism of Abelian varieties, then $\langle f(a), b \rangle_{B,K} = \langle a, f(b) \rangle_{A,K}$.

Proof: Use functoriality of heights for $A \to \hat{A}$, then $\hat{h}_{A \times \hat{A}, p}((a, 0)) = \hat{h}_{A,0}(a) = 0$. Similarly, $\langle 0, a \rangle_{A,K} = 0$. Thus $\hat{h}_{A \times \hat{A}, p}$ is bilinear by (2.1.4.8).

The last assertion follows from (7.7.3.36). \qed

Prop. (13.5.12.9). Let $\mathcal{L} \in \text{Pic}(A)$ and $\varphi_\mathcal{L} : A \to \hat{A}$ the associated homomorphism (13.5.4.2), then for any $a, a' \in A(\overline{K})$,

- $\hat{h}_{\varphi_\mathcal{L}}(a) = \hat{h}_\mathcal{L}(a) + b(a, a')$.
- $\hat{h}_\mathcal{L}(a) = \langle a, \mathcal{L} \rangle_{A,K}$.
- $b_\mathcal{L}(a, a') = \langle a, \varphi_\mathcal{L}(a') \rangle_{A,K} = \hat{h}_{\varphi_\mathcal{L}}(a')(a)$.

Proof: 1: $b_\mathcal{L}(a, a') = \hat{h}_\mathcal{L}(a + a') - \hat{h}_\mathcal{L}(a) - \hat{h}_\mathcal{L}(a') = \hat{h}_\mathcal{L}(\tau_{a'} \cdot a) - \hat{h}_\mathcal{L}(a) - \hat{h}_\mathcal{L}(a')$. Then $b(\cdot, a') + \hat{h}_\mathcal{L}$ is a representative in the class $h_{\tau_{a'}(\mathcal{L})}$ by functoriality. And it is a quadratic function, thus by uniqueness, we are done.

2: Because the pullback of $p$ to $A \times \{\mathcal{L}\}$ is $\mathcal{L}$ by (7.7.3.34), and thus this follows from functoriality and (13.5.12.8).

3: By (13.5.4.2) and item1, $b(a, a') = \hat{h}_{\varphi_\mathcal{L}}(a')(a)$. Thus we are done by item2. \qed

Cor. (13.5.12.10) [Regulator]. The Néron-Tate pairing induces a non-degenerate pairing $A(\overline{K})/A(\overline{K})_{\text{tor}} \times \hat{A}(\overline{K})/\hat{A}(\overline{K})_{\text{tor}} \to \mathbb{R}$. The discriminant of this pairing is called the regulator of $A$, denoted by $R(A/K)$. 


Proof: Let \( \mathcal{L} \in \text{Pic}(A) \) be ample, then \( \varphi_{\mathcal{L}} : A \to \hat{A} \) is an isogeny, thus \( \varphi_{\mathcal{L}} : A(K)/A(K)_{\text{tor}} \to \hat{A}(K)/\hat{A}(K)_{\text{tor}} \) is injective, and by (13.13.1.7), the image is a subgroup of \( \hat{A}(K)/\hat{A}(K)_{\text{tor}} \) of the same rank, thus we are done by (13.5.12.9) item3 and (13.5.12.3). \( \square \)

Cor. (13.5.12.11). Let \( A \) be an Abelian variety, \( c \in \text{Pic}(A) \) an even ample class, \( c' \in \text{Pic}(A) \), then

\[ \hat{h}_c = O(\hat{h}_{c'}^{1/2}). \]

Proof: By (13.5.14), \( \varphi_c \) is isogeny thus surjective, thus we can assume \( c' = \varphi_c(a') \) for some \( a' \in A(K) \). Then by (13.5.12.9), \( \hat{h}_c(a) = b_c(a, a') \). Because \( b_c \) is positive semi-definite by (13.5.12.2), by Cauchy-Schwartz (2.1.4.7), \( |\hat{h}_{c'}(a)|^2 \leq b(a, a)b(a', a') = 4\hat{h}_c(a)\hat{h}_c(a') \). \( \square \)

Hilbert's Irreducibility Theorem

Prop. (13.5.12.12)[Runge's Theorem].

Prop. (13.5.12.13)[Hilbert's Irreducibility Theorem]. Let \( C \) be a smooth irreducible projective curve over a number field \( K \) and let \( f : C \to \mathbb{P}^1 \) be a surjective rational function on \( C \) over \( K \), then for all \( n \in \mathbb{N} \) except for a set of natural density 0, the divisor \( f^*[n] \) is a prime divisor over \( K \).

Proof: Cf.[Diophantine Geometry, P319]. \( \square \)

Local Height Pairings

Cf.[Sil99]Chap6 or [Local Heights on Curves, Gross, in Arithmetic Geometry] and [B-G06] or [Introduction to Diophantine Geometry, Lang].

13 Jacobians of Curves

Prop. (13.5.13.1)[Picard Schemes of Curves]. Let \( C \) be a smooth complete precurve over a field \( k \) of genus \( g \) with a rational point, then

- \( \text{Pic}_{C/k} \) is representable by a disjoint union of smooth complete varieties \( \text{Pic}_{C/k}^d, d \in \mathbb{Z} \) where \( \text{Pic}_{C/k}^d \) corresponds to relative line bundles of degree \( d \).
- \( \text{Pic}_{C/k}^0 \) is an Abelian variety over \( k \).
- for \( d \geq 0 \), the Abel map \( \text{Div}_{C/k}^d \to \text{Pic}_{C/k}^d \) is surjective for \( d \geq g \) and smooth for \( d \geq 2g - 1 \).
- The morphism \( \text{Div}_{C/k}^g \to \text{Pic}_{C/k}^g \) is birational.

Proof: Cf.[Sta]0BA0 or [Neron Models] or (13.5.13.2)? item1 follows from (6.1.12.5) \( \square \)

Prop. (13.5.13.2)[Picard Scheme of Relative Curves]. If \( X/S \) is locally projective, flat with fibers all curves, \( m \in \mathbb{Z} \), let \( \text{Pic}_{X/S}^m \) denote the subfunctor of \( \text{Pic}_{X/S} \) representing invertible sheaves \( \mathcal{L} \) with \( \text{deg}(\mathcal{L}) = m \), then

- \( \text{Pic}_{X/S}^m \) are clopen subschemes of \( \text{Pic}_{X/S} \) of f.t. and form a disjoint cover of it, and forming it commutes with base change.
- \( \text{Pic}^{(0)}_{X/S} = \text{Pic}^0_{X/S} = \text{Pic}^r_{X/S} \), and each \( \text{Pic}^m_{X/S} \) is a fppf-torsor under \( \text{Pic}^0_{X/S} \).
- If \( X/S \) is projective and \( S \) is Noetherian, then each \( \text{Pic}^m_{X/S} \) is quasi-projective over \( S \).

Proof: Cf.[Kle05]P60.? \( \square \)
Def. (13.5.13.3) [Jacobians of Curves]. For a smooth complete precurve over a field $k$, its Jacobian variety $\text{Jac}(C)$ is just its Picard variety $\text{Pic}^0_{C/k}$.

Cor. (13.5.13.4). For a smooth complete precurve $C$ over a field with a rational point, $x \in \text{Pic}_C/k$ is in $\text{Jac}(C)$ iff the corresponding line bundle $x$ on $C_{k(x)}$ has degree 0, by (13.5.13.1).

Prop. (13.5.13.5). If $C$ is a smooth complete curve of dimension $g$, then $\text{Jac}(C)$ has dimension $g$, by (7.7.3.24) and (7.7.3.22).

Def. (13.5.13.6) [Symmetric Product]. Let $C$ be a smooth curve, then the symmetric product $C^{(r)} = C^r/S_r$ is a smooth variety of dimension $r$ by considering the symmetric functions.

Prop. (13.5.13.7) [Generic Riemann-Roch].

Prop. (13.5.13.8) [Polarization of Jacobians].

Prop. (13.5.13.9) [Push and Pull]. For a non-constant morphism $\varphi : C_1 \to C_2$ of pointed smooth curves over $k$, the push and pull induce maps

$$\varphi_* : J\text{ac}(C_1) \to J\text{ac}(C_2), \quad \varphi^* : J\text{ac}(C_2) \to J\text{ac}(C_1).$$

s.t. $\varphi_* \circ \varphi^* = \deg(\varphi)$.

Proof: \hfill $\square$

Prop. (13.5.13.10) [Abel-Jacobi]. Let $X$ be a smooth curve over $\mathbb{C}$ with a rational point $x_0$, then $\text{Jac}(C)$ is isomorphic to $\Omega^1_{\text{hol}}(X)^\vee / H_1(X, \mathbb{Z})$ as complex manifolds via

$$L(\sum_x n_xx) \mapsto \sum_x n_x \int_{x_0}^x.$$

Proof: \hfill $\square$

Prop. (13.5.13.11). Let $k \in \text{Field}, C$ be a smooth complete curve over $k$, $P \in C(k)$, then for any $\ell \in \mathbb{P}$, the map $f_P : C \to \text{Jac}(C)$ induce isomorphisms

$$H^1(\text{Jac}(C), \mathcal{O}_{\text{Jac}(C)}) \cong H^1(C, \mathcal{O}_C), \quad H^1(\text{Jac}(C), \mathbb{Z}_\ell) \cong H^1(C, \mathbb{Z}_\ell).$$

Proof: Cf. [Mil08]P114. \hfill $\square$

Prop. (13.5.13.12) [Surjection by Jacobians]. Let $k \in \text{Field}$ and $A \in \text{AbVar}/k$, there exists a smooth complete curve $C$ over $k$ and a surjection $\text{Jac}(C) \to A$.

Proof: We only prove for $\#k = \infty$. For $k$ finite, Cf. [Gabber, On space filling curves and Albanese varieties], [Poonen, Bjorn, Bertini theorems over finite fields. Ann. of Math].

Since elliptic curves are their own Jacobians, we can assume that dim $A > 1$. Choose a projective embedding $A \to \mathbb{P}^n_k$, then by Bertini and the fact $\#k = \infty$, there is a hyperplane cut $A \cap H$ that is also a smooth complete $k$-variety. By repeating dim $A - 1$ times, we get a $k$-curve $C$ on $A$. This curve gives a map $\text{Jac}(C) \to A$ by (13.5.13.8) and double duality (13.5.4.16). The image is an Abelian subvariety of $A$. If it is not the whole of $A$, then by Poincaré’s reducibility theorem (13.5.6.7), there
exists another Abelian subvariety $A_2 \subset A$ s.t. $\text{Jac}(C) \times A_2 \to A$ is an isogeny. In particular, $\text{Jac}(C) \cap A_2$ is finite.

Using the embedding $C \subset \text{Jac}(C)$, $C$ is regarded as a subscheme of $\text{Jac}(C)$. Take $n \in \mathbb{Z} \cap k^*$ large, the composition $\text{Jac}(C) \times A_2 \xrightarrow{(1,n)} \text{Jac}(C) \times A_2 \to A$ is finite, and the inverse image of $C$ projects to $[n]^{-1}(A_1 \cap A_2) \subset A_2$, which is finite and disconnected. So the inverse image of $C$ is not connected, which contradicts the fact it is an ample divisor by (5.5.12.4) and (5.8.6.25).

\[\square\]

**Conj. (13.5.13.13) [Resolution Conjecture]**. Let $k \in \text{Field}, k = \overline{k}$, and $A \in \text{AbVar}/k$, we can find a surjective homomorphism $J_1 \to A$ where $J_1$ is a Jacobian of a curve by (13.5.13.12). Then the identity component of the kernel is also an Abelian variety. Then we can do the same process again.

is it possible to choose the Jacobians s.t. the process terminate after finite steps?

**Proof:**

\[\square\]

**Thm. (13.5.13.14) [Tonelli]**. Let $k \in \text{Field}$ and $k = \overline{k}$, and $(C, P), (C', P')$ be pointed complete smooth curves over $k$. Let $f : C \to \text{Jac}(C)$ and $f' : C' \to \text{Jac}(C')$ be the maps corresponding to $P, P'$. Then if $\beta : (\text{Jac}(C), ) \cong (\text{Jac}(C'), )$ is an isomorphism of polarized Jacobians, then

- There exists an isomorphism $\alpha : C \to C'$ s.t. $f' \circ \alpha = \pm \beta \circ f + c$ for some $c \in \text{Jac}(C)(k)$.

- If $g(C) \geq 2$ and $C$ is non-hyperelliptic, then $\alpha, \pm 1, c$ are determined by $\beta, P, P'$. And if $g(C) \geq 2$, then $\pm 1$ can be arbitrary, and $\alpha, c$ is determined by $\beta, \pm 1, P, P'$.

**Proof:** Cf.[Mil08]P120.

\[\square\]

**Cor. (13.5.13.15).**

- If $k \in \text{Field}, C, C'$ are complete smooth curves over $k$ with rational points s.t. their polarized Jacobians are isomorphic, then $C, C'$ are isomorphic over $k$.

- If $k \in \text{Field}$ is perfect, $C, C'$ are complete smooth curves of genus $\geq 2$ over $k$, then if their polarized Jacobians are isomorphic, then $C, C'$ are also isomorphic over $k$.

**Proof:** Let $\beta : (\text{Jac}(C), ) \cong (\text{Jac}(C'), )$ is an isomorphism, for any $P \in C(\overline{k}), P' \in C'(\overline{k})$, there is a unique isomorphism $\alpha : C_{\overline{k}} \cong C'_{\overline{k}}$ s.t. $f'^{P'} \circ \alpha = \pm \beta \circ f^P + c$, and if $C$ is hyperelliptic, take $\pm = +$. Then if $Q, Q'$ are different points, $f'^{P} = f'^{Q} + d, f'^{Q'} = f'^{P'} + e$ for some $d \in \text{Jac}(C)(\overline{k}), e \in \text{Jac}(C')(\overline{k})$. So $\alpha$ is invariant of the points $P, P'$ chosen. In particular, $f'^{(P')} \circ \alpha = \sigma(f'^P) \circ \alpha = \pm \beta \circ \sigma(f^P) + \sigma(c) = \pm \beta f'^{(P)} + \sigma(c)$.

for any $\sigma \in \text{Gal}_k$. So $\alpha$ is invariant under $\text{Gal}_k$, which means $C, C'$ are isomorphic over $k$.

\[\square\]

**Arithmetics**

**Prop. (13.5.13.16).** If $F$ is a global field and $C$ is a complete smooth curve over $F$ with good reduction at a place $P$ of $F$, then $\text{Jac}(C)$ has good reduction at $P$.

**Proof:** The hypothesis implies $C$ extends to a smooth proper curve $\tilde{C}$ over $\text{Spec } R_P$. Then the Picard scheme $\mathcal{J}$ of $C/\text{Spec } R_P(13.5.13.2)$ has generic fiber $\text{Jac}(C)$, which implies $\text{Jac}(C)$ has good reduction at $P$. 

\[\square\]
14 Abelian Schemes

Prop. (13.5.14.1) [Rigidity Lemma].

Proof: □

Cor. (13.5.14.2). Any morphism of Abelian schemes in $\text{AbVar}/S$ preserving the zero section is a homomorphism. Thus the group structure is determined by the zero section, and any Abelian scheme is commutative.

Prop. (13.5.14.3) [Dual Abelian Schemes]. If $X/S$ is a projective Abelian scheme, then

- $\text{Pic}^0_X/S = \text{Pic}^0_{X/S}$ is a projective Abelian scheme over $S$, called the dual Abelian scheme of $X/S$.
- the double Picard map $(7.7.3.37) A \to A^\vee$ is an isomorphism.

Proof: By reducing to the fiber, these reduces to the case that $S$ is a field, and this case follows from (13.5.4.12) and (13.5.4.12). □

15 Néron Models

Main references are [Serre/Tate, Good Reduction of Abelian Varieties], [BLR90] and http://virtualmath1.stanford.edu/~conrad/mordellsem/Notes/L11.pdf.

Def. (13.5.15.1) [Néron Models]. Let $(R, K)$ be a DVR and $X \in \text{Sch}^{\text{sm}, \text{sep}, \text{ft}} / K$, then a Néron model for $X/K$ is a scheme $\mathcal{X} \in \text{Sch}^{\text{sm}, \text{sep}, \text{ft}}$, satisfying the following universal property: For any smooth scheme $\mathcal{Y}$ over $R$ and any morphism $f : \mathcal{Y}_K \to X$, there exists a unique morphism $\mathcal{Y} \to \mathcal{X}$ extending $f$.

In particular, the natural map $\mathcal{X}(R) \to X(K)$ is a bijection.

Prop. (13.5.15.2) [Étale Valuation Criterion for Group Schemes]. Let $(R, K)$ be a DVR and $X \in \text{Sch}^{\text{sm}, \text{sep}, \text{ft}} / K$, then if $\mathcal{X}/R$ is a Néron model for $X$, then $\mathcal{X}$ satisfies valuation criterion for any $R'$ that is the integral closure of $R$ in an unramified field extension $K'/K$.

Conversely, if $X$ is a group scheme over $K$, then the converse is also true: If $\mathcal{G}$ is a smooth $R$-group scheme of f.t., then $\mathcal{G}$ is a Néron model of its generic fiber iff the natural map $\mathcal{G}(R^{\text{sh}}) \to \mathcal{G}(K^{\text{sh}})$ is an isomorphism.

Proof: Cf.[BLR90]Prop. 7.1.1. □

Prop. (13.5.15.3) [Unramified Base Change]. Let $(R, K)$ be a DVR and $X \in \text{Sch}^{\text{sm}, \text{sep}, \text{ft}} / K$, $K'/K$ an unramified field extension, $R'$ the integral closure of $R$ in $K'$, then if $\mathcal{X}$ is a Néron model for $X$, then $\mathcal{X}_{R'}$ is a Néron-model for $X_{K'}$.

Proof: Because $R'/R$ is smooth(by(5.6.4.6) and the definition of unramifiedness(12.2.2.4)), for any $\mathcal{Y}'/R'$ smooth,

$$\text{Mor}_{R'}(\mathcal{Y}', \mathcal{X}_{R'}) = \text{Mor}_R(\mathcal{Y}', \mathcal{X}) = \text{Mor}_K(\mathcal{Y}'_{K'}, X) = \text{Mor}_{K'}(\mathcal{Y}'_{K'}, X_{K'}).$$

□

Prop. (13.5.15.4) [Étale Descent]. Let $(R, K) \subset (R', K') \subset (R^{\text{sh}}, K^{\text{sh}})$ be DVRs. If $G$ is a smooth $K$-group scheme of f.t. over $K$ s.t. $G_{K'}$ has a Néron model $\mathcal{G}' / R'$, then $\mathcal{G}'$ descends to a Néron model $\mathcal{G}/R$ of $G$. 
Proof: Cf.[BLR90]Prop. 6.5.4. □

Cor. (13.5.15.5). Let \((R, K) \subset (R', K')\) be an unramified extension of DVRs, and \(G\) is a smooth \(K\)-group scheme of f.t. over \(K\), then \(G\) has a Néron model iff \(G_{K'}\) has a Néron model.

Proof: Cf.[BLR90]Prop. 6.5.4. □

Prop. (13.5.15.6) [Néron Model of Abelian Varieties]. Let \((R, K, k)\) be a DVR and \(A \in \text{AbVar}/K\) with Néron model \(A/R\), then \(A\) is a \(R\)-group scheme by universal property. The relative identity component \(A_0\) of \(A\) is defined to be the open subgroup of \(A\) deleting all non-identity components of \(A_k\).

Prop. (13.5.15.7) [Good Reduction of Abelian Varieties]. Let \((R, K)\) be a DVR, \(A \in \text{AbVar}/K\) and \(A \in \text{Sch}/R\) is proper smooth with generic fiber \(A\), then the group structure extends to \(A\), making it the Néron model of \(A\).

In particular, the good reduction of \(A\) is unique if it exists.

Proof: Cf.[BLR90]Prop. 7.2.1 of [Milne, CM, P49].

To show the group structure extends, Cf.[Koizumi, On specializations of the Albanese and Picard Varieties] or might be somewhere in [BLR90]. □

Cor. (13.5.15.8). Let \((R, K, k)\) be a DVR, \(A \in \text{AbVar}/K\) with Néron model \(A/R\), then the following are equivalent:

- \(A\) is an Abelian scheme.
- \(A\) has good reduction over \(R\).
- The identity component \(A^0_k\) of \(A_k\) is proper hence an Abelian variety over \(k\).

Proof: 1 \(\rightarrow\) 2, 1 \(\rightarrow\) 3 is clear. 2 \(\rightarrow\) 1 follows from the proposition. 3 \(\rightarrow\) 1: By (5.10.5.3) \(A_0\) is an Abelian scheme, so \(A_0 = A\) is the Néron model by the proposition. □

Prop. (13.5.15.9) [Exactness]. Let \((R, K)\) be a DVR with mixed characteristic \((0, p)\) and ramification index \(e < p - 1\). If \(0 \rightarrow A' \rightarrow A \rightarrow A'' \rightarrow 0\) is an exact sequence in \(\text{AbVar}/K\), and \(A\) has good reduction, then so does \(A'\) and \(A''\) by (13.5.10.4). Then the Néron models

\[
0 \rightarrow A' \rightarrow A \rightarrow A'' \rightarrow 0
\]

for an exact sequence.

Proof: Cf.[BLR90]Prop7.5.4.. □

Prop. (13.5.15.10) [Extending Polarizations]. Let \((R, K)\) be a DVR and \(A \in \text{AbVar}/K\) has good reduction over \(R\), then any polarization \(\lambda : A \rightarrow A^\vee\) extends to a polarization on \(A\).

Proof: See [Artin 1986, 4.4 in Arithmetic Geometry], and [Chai and Faltings 1990]. □

Existence of Néron Models

Prop. (13.5.15.11) [Néron Model for Abelian Varieties]. Let \(X\) be an Abelian variety over \(K\) and \(A\) be any ring of integers in the field \(K\), then there exists an open subset \(Y = \text{Spec} A_S \subset \text{Spec} A\), and a scheme \(\bar{X}\) projective over \(Y\), and morphisms \(\bar{m} : \bar{X} \times \bar{X} \rightarrow \bar{X}\) over \(Y\) and \(\bar{e} : Y \rightarrow X\) that:
• The fiber of $\tilde{X}$ over a generic point of $Y$ with the morphisms $\tilde{m}, \tilde{e}$ are Abelian varieties isomorphic to $X$.

• $\tilde{X}$ is a group scheme over $Y$, and its fiber over any closed point of $Y$ with the morphisms $\tilde{m}, \tilde{e}$ are Abelian varieties.

• The mapping in item 1 induces an isomorphism of groups $\tilde{X}(Y) \cong X(K)$.

Proof: 1: Consider for any qc scheme over a field $K$, it is glued together from f.m. affine schemes, and these gluing involves f.m. polynomials and rational transition functions, and the coefficients of them are contained in a subring $A_S \subset K$ of f.t. over $A$. Thus this variety can be seen as a variety over $A_S$ with the same equations, satisfying item 1. The situation is similar for morphisms between qc schemes, in particular $\tilde{m}$ and $\tilde{e}$, thus constructing $\tilde{X}$.

2: Cf.[Mumford, P265].

3: Cf.[Mumford, P265].

Cor. (13.5.15.12). Let $x \in \tilde{X}(Y)$, consider $x$ as a closed subscheme of $\tilde{X}$ and denote $n^{-1}(x)$ the closed subscheme in $\tilde{X}$ the inverse image of $x$ under the morphism $[n]_Y$. Then the natural projection $n^{-1}(x) \to Y$ is étale over all points $y \in Y$ that $\text{char } k(y) \nmid n$.

Proof: [Mumford, P265].

Thm. (13.5.15.13)[Existence of Néron Models]. Let $(R, K)$ be a DVR and $A \in \text{AbVar } / K$, then $A$ admits a Néron model $A/R$.

Proof:

Def. (13.5.15.14)[Tamagawa Numbers]. Let $(R, K, k)$ be a DVR and $A \in \text{AbVar } / K$ with Néron model $A/R$, define the component group of $A$ to be $\pi_0(A_k)$, denoted by $\Phi(A)$. And $\#\Phi(A) < \infty$ is called the Tamagawa number of $A$.

Then $c(A)$ equals the number of geo.connected components of $A_k$. And if $k$ is finite, it also equals the connected components of $A_k$ with a rational point.

Proof: Cf.[Liu Qing, 10.2.21(a)].
13.6 Surfaces and Arithmetic Surfaces

Main references are [Sil99], [Liu Qing].

Notations (13.6.0.1).
- In this section, let $S \in \text{Sch}$ be a Dedekind scheme with generic point $\eta$ or a spectrum of a field, and $\eta = S$.

1 Over Fields

Main references are [Liu Qing, Algebraic Geometry and Arithmetic Curves].

Prop. (13.6.1.1) [27-Lines]. Any smooth cubic surface in $\mathbb{P}^3_k$ contains exactly 27 lines.

Proof: □

Prop. (13.6.1.2). Any birational transformation of non-singular surfaces will be factorized into f.m blowing-ups and blowing-downs of points.

Proof: □

Prop. (13.6.1.3). Any smooth surface over a field $k$ is projective.


Prop. (13.6.1.4) [Non-Projective Smooth Proper Threefold]. Cf. [Vak17] P671.

Proof: □

Resolution of Surfaces

Cf. [Sta] Chap 51.

Regular Surfaces

2 Fibered presurfaces

Def. (13.6.2.1) [fibered presurfaces]. Let $S \in \text{Sch}$ be Dedekind, a fibered presurface over $S$ is flat $S$-scheme integral of dimension 2.

Prop. (13.6.2.2). Let $S \in \text{Sch}$ be Dedekind, $X$ a fibered presurface over $S$, then $X_s$ has dimension 1 for any $s \in S$, and $X_\eta$ is a precurve.

Proof: Cf. [Qing Liu] P348. □

Example (13.6.2.3). Let $q \in \mathbb{Z_+}$ be a square-free integer, then $\mathcal{C} = \text{Proj}(\mathbb{Z}[X, Y, Z]/(X^q + Y^q + Z^q))$ is a normal fibered presurface over $\text{Spec} \, \mathbb{Z}$.

Proof: Cf. [Qing Liu] P455. □

Prop. (13.6.2.4) [Horizontal and Vertical Divisors]. Let $S \in \text{Sch}$ be Dedekind, $X$ a fibered presurface over $S$, then
• If $x$ is a closed point of $X_\eta$, then $\overline{\{x\}}$ is an integral closed subscheme of $X$ that is finite surjective over $S$, called a **horizontal divisor**.

• If $D \subset X$ is a prime Weil divisor, then $D$ is either a horizontal divisor, or an integral component of a special fiber, called a **vertical divisor**.

• If $x_0 \in X$ is closed, then $\dim \mathcal{O}_{X,x_0} = 2$.

Moreover, call a Weil divisor $D$ on $X$ horizontal or vertical if it consists of horizontal or vertical prime divisors.

**Proof:** Cf.[Qing Liu]P349. □

**Prop.(13.6.2.5)**[Generically Smoothness]. Let $S \in \text{Sch}$ be Dedekind and $\pi : X \to S$ be a fibered presurface s.t. $X_\eta$ is smooth, then there is a dense open subscheme $V \subset S$ s.t. $\pi^{-1}(V) \to V$ is smooth.

**Proof:** Cf.[Qing Liu]P352. □

**Regular Fibered Presurfaces**

**Prop.(13.6.2.6)**[Regular Fibered Presurfaces are Projective]. Let $S$ be affine and $X/S$ be a flat morphism with fibers of dimension 1, then $X/S$ is projective. In particular, a regular fibered presurface is projective.

**Proof:** Cf.[Qing Liu]P353. □

**Prop.(13.6.2.7)**[Sections are Regular]. Let $\pi : C \to S$ be a regular fibered presurface and $s \in S$, then

- If $s \in S$ is closed and $x \in C_s$ is closed, then $C_s$ is regular at $x$ iff $\pi^s(p_s) \not\subseteq m_x^2$.

- If $P : U \to C$ is a rational section, then $C_p$ is smooth at $P(s)$ for $s \in U$.

**Proof:**

1: This is because $\mathcal{O}_{C_s,x} = \mathcal{O}_{C,x}/\pi^s(p_s)$, $m_{C_s,x} = m_{C,x}/\pi^s(p_s)$ and use the definition of regularity.

2: We show that $\pi^s(p_s) \not\subseteq m_x^2$: Suppose otherwise, then

$$p_s = (\pi \circ P)^s(p_s) \subset \pi^s(m_x^2) = \mathfrak{p}^2,$$

which is impossible. □

**Cor. (13.6.2.8).** Let $C/S$ be a regular fibered presurface, then $C(S) = C_{\text{sm}}(S)$. If moreover $C/S$ is proper, then $C(S) = C_{\text{sm}}(S) = C_\eta(K)$.

**Example (13.6.2.9).**

- $C \subset \mathbb{P}^2_Z$ defined by the equation $y^2 = x^3 + 2x^2 + 6$ is a regular fibered presurface over $\mathbb{Z}$ with 3 singular points.

- $C \subset \mathbb{P}^2_Z$ defined by the equation $y^2 = x^3 + 2x^2 + 6$ is not regular at $(x,y,2)$.

**Proof:**

1: The determinant $\Delta = -2^6 \cdot 3 \cdot 97$, so it has three singular fibers $C_2, C_3, C_{97}$:

$$C_2 : y^2 = x^3, \quad C_3 : y^2 = x^2(x + 2), \quad C_{97} : y^2 = (x + 66)^2(x + 64).$$

By (13.8.1.15), they are singular at a single point, and we check these points are regular in $C$:

For $C_2$, the singular point is defined by $(x,y,2)$, and has residue field $\mathbb{F}_2$. To show it is regular, it suffices to show that $(x,y,2)/(x,y,2)^2$ is generated by 2 elements $x, y$: $2 = 3^{-1}(y^2 - x^3 - 3x^2)$. The $C_3, C_{97}$ cases are similar. □
3 Arithmetic Surfaces

Def. (13.6.3.1) [Arithmetic Surfaces]. An arithmetic surface is a flat of f.t. over $S$ that is integral normal and excellent, such that its generic fiber is a non-singular projective curve, and its special fibers are unions of curves.

Prop. (13.6.3.2). Any arithmetic surface is regular in codimension 1.

Prop. (13.6.3.3) [Mordell-Weil for Function Fields]. Let $E \rightarrow C$ be an elliptic surface defined over a field $k$. Let $E^\otimes (C)$ be the generic fiber. If $k$ is a number field or $E^\otimes C$ is not split, then $E(K(C))$ is a f.g. Abelian group.


4 Intersection Theory

Def. (13.6.4.1) [Canonical Divisors]. $K_{X/S}$, Cf. [Qing Liu] P389.

Def. (13.6.4.2) [Vertically Nef]. Let $X^\otimes S$ be a regular fibered presurface, then $D \in \text{Cl}(X)$ is called vertically nef if $D \cdot C \geq 0$ for any vertical divisor $C$.

Prop. (13.6.4.3) [Factorization Theorem]. Any birational morphism of regular fibered presurfaces over $S$ is a finite composition of blowing-up along a single closed point.


Arithmetic Surfaces

Prop. (13.6.4.4) [Intersection between Vertical Divisors]. Let $X^\otimes S$ be an arithmetic surface and $s \in S$ a closed point, then for any $\Gamma \in \text{Div}_s(X)$, $\Gamma \cdot X_s = 0$. In particular, if $\Gamma_1, \ldots, \Gamma_r$ are irreducible components of $X_s$ of multiplicities $d_1, \ldots, d_r$, then

$$\Gamma_i^2 = -\frac{d_j}{d_i} \sum_{j \neq i} \Gamma_i \cdot \Gamma_j \leq 0.$$ 

5 Minimal Arithmetic Surfaces

Def. (13.6.5.1) [Exceptional Divisors]. Let $X/S$ be a regular fibered presurface, then an exceptional divisor or $(-1)$-curve $E \subset X$ is a prime divisor s.t. there is a morphism of regular fibered presurfaces $f : X \rightarrow Y$ s.t. $f(E)$ is a closed point. Notice an exceptional divisor must be a vertical divisor.

Prop. (13.6.5.2) [Castelnuovo’s criterion, Lichtenbaum/Shafarevich]. Let $X/S$ be a regular fibered presurface, $E \subset X_s$ a vertical prime divisor. Let $k' = H^0(E, \mathcal{O}_E)$, then $E$ is an exceptional divisor iff $E \cong \mathbb{P}^1_{k'}$. And this is the case if $E^2 = -[k' : k(s)]$.


Prop. (13.6.5.3) [Characterizing Exceptional Divisors]. Let $X/S$ be a regular fibered presurface, then for a vertical prime divisor $E$ on $X$,

- $E$ is exceptional iff $K_{X/S} \cdot E < 0$ (13.6.4.1) and $E^2 < 0$. And in this case, $K_{X/S} \cdot E = E^2$. 

• If \( \dim S = 0 \) and \( H^0(X, [\omega_{X/S}]^q) \neq 0 \) for some \( q \geq 1 \) or \( \dim S = 1 \) and \( p_a(X_\eta) > 0 \), then \( E \) is exceptional iff \( K_{X/S} \cdot E < 0 \).

Proof: Cf.[Qing Liu]P417.

Def.(13.6.5.4) [Minimal Surfaces]. A relatively minimal surface over \( S \) is a regular fibered presurface \( C/S \) s.t. for any other such regular fibered presurface \( C' \) and any birational morphism \( C \to C' \) is an isomorphism. Equivalently, \( C \) is a regular proper model that doesn’t contain an exceptional curve of the first kind, i.e. cannot be blown down by(13.6.4.3). Cf.[Sta]0C21.

A minimal surface over \( S \) is a regular fibered presurface \( C/S \) s.t. for any other such regular fibered presurface \( C' \) and any birational map \( C' \to C \) is a birational morphism. In particular, a minimal surface \( C/S \) is relatively minimal, and \( \text{Aut}_S(C) \cong \text{Aut}_K(C_\eta) \) is an isomorphism.

Cor.(13.6.5.5). If a relatively minimal arithmetic surface over \( S \) is birational to a minimal surface over \( S \), then they are isomorphic over \( S \).

Prop.(13.6.5.6) [Étale Descent]. Let \( X/S \) be an arithmetic surface with \( p_a(X_\eta) > 0 \), and \( S' \to S \) is an étale covering or \( S = \text{Spec} R \) where \( R \) is a DVR and \( S' = \text{Spec} \hat{R} \), then \( X/S \) is minimal iff \( X \times_S S'/S' \) is minimal.

Proof: Cf.[Qing Liu]P423.

Cor.(13.6.5.7). Let \( X/S \) be an arithmetic surface with \( p_a(X_\eta) > 0 \) and \( T \to S \) is a smooth morphism, then for any \( \xi \in T \) of codimension 1, \( X \times_S \mathcal{O}_{T,\xi} \) is a minimal regular surface over \( \mathcal{O}_{T,\xi} \).

Proof: Cf.[Qing Liu]P424.

Minimal Models

Prop.(13.6.5.8) [Minimal Models]. Let \( C/S \) be a normal fibered presurface, then a regular model for \( C/S \) is a regular fibered presurface \( C'/S \) with a birational map \( C' \to C \) over \( S \). Notice \( C'_\eta \to C_\eta \) is a birational map of regular projective precurve, thus an isomorphism.

A (relatively) minimal model for \( C/S \) is a regular model for \( C/S \) that is (relatively) minimal. Notice if a minimal model exists, it is unique up to a unique isomorphism.

Lemma(13.6.5.9). If \( X/S \) is an arithmetic surface, then there exists only f.m. fibers \( X_s \) containing an exceptional divisor.

Proof: Cf.[Qing Liu]P420.

Prop.(13.6.5.10) [Blowing Down to Relatively Minimal Surfaces]. If \( X/S \) is an arithmetic surface, then \( X \) is a finite blowing-up of relatively minimal arithmetic surface over \( S \).

Proof: The number of exceptional divisors decreases along contractions?

Prop.(13.6.5.11) [Lichtenbaum/Shafarevich]. Let \( X/S \) be an arithmetic surface with \( p_a(X_\eta) \geq 1 \), then \( X \) admits a unique minimal model over \( S \).

Proof: Cf.[Qing Liu]P422.

Remark(13.6.5.12). This is not true for \( p_a(X_\eta) = 0 \), Cf.[Qing Liu]P422.
Cor. (13.6.5.13) [Minimal and Relatively Minimal Surfaces]. If $X/S$ is an arithmetic surface s.t. $p_a(X_\eta) > 1$, then $X$ is minimal iff it is relatively minimal iff $K_{X/S}$ is vertically nef, by (13.6.5.5) and (13.6.5.4)(13.6.5.3). Why in the field case, why the hypothesis is satisfied?

Cor. (13.6.5.14). If $X/S$ is a smooth arithmetic surface, then $X/S$ is relatively minimal by (13.6.4.4) as in this case $X_s$ is a disjoint union of irreducible curves. And if $p(X_\eta) > 0$, then $X$ is minimal.
13.7 Reductions

1 Semistable Reductions

Def. (13.7.1.1) [Models]. Let $S$ be a Dedekind domain with function field $K$ and $X$ an algebraic $K$-scheme, a model over $S$ for $X$ is a proper flat f.t. $S$-scheme $\mathcal{X}$ s.t $\mathcal{X} \times_S K \cong X$.

Def. (13.7.1.2) [Good Reduction]. Let $(R,K,k)$ be a DVR and $X$ an algebraic $K$-scheme, $X$ is said to have good reduction over $R$ if there is a smooth model $\mathcal{X}$ for $X$. If this is the case, then $\tilde{X} = \mathcal{X}_k$ is a smooth scheme over $k$, called the reduction of $X$.

In this case, the reduction map $X(K) \cong \mathcal{X}(\mathcal{O}_R) \rightarrow \tilde{X}(k)$ is surjective, by valuation criterion and formal smoothness criterion.

2 Reduction of Curves

Main references are [Sta]Chap55 and [Qing Liu].

Def. (13.7.2.1) [Semistable and Stable Unions of Curves]. Let $k \in \text{Field}, k)$, $C$ an algebraic union of curves over $k$, then $C$ is called a semistable union of curves iff $C_k$ is reduced and the singular points of $C_k$ are all ordinary double points. $C$ is called a stable union of curves if moreover it satisfies:

- $C_k$ is connected and projective, with $p_a(C) \geq 2$.
- Let $\Gamma$ be an integral component of $C$ that is isomorphic to $\mathbb{P}^1_k$, then it meets other integral components at at least 3 points.

Minimal Models

Def. (13.7.2.2) [Minimal Models]. Let $R$ be a DVR with fraction field $K$. Let $C$ be a smooth projective curve over $K$, then a minimal model for $C$ is a regular proper model $\mathcal{C}$ for $C$ s.t. for any other such model $C'$, any birational map of models $C \rightarrow C'$ is an isomorphism.

Equivalently, $C$ is a regular proper model that doesn’t contain an exceptional curve of the first kind, i.e. cannot be blown down? Cf.[Sta]0C21.

Prop. (13.7.2.3) [Resolution of Singularities for Arithmetic Surfaces]. Let $(R,K)$ be a DVR, $C$ a smooth projective curve over $K$ of genus $g$. Then there exists a proper regular model for $C$.

Proof: Cf.[?] □

Prop. (13.7.2.4) [Minimal Model Theorem]. Let $(R,K)$ be a Dedekind domain and $C$ a smooth projective precurve over $K$, then of genus $\geq 1$, then there exists a minimal model for $C$.

Proof: Cf.[?] □

Prop. (13.7.2.5) [Semistable Reductions]. Let $(R,K)$ be a DVR, for a smooth complete curve $C$ over $K$, the following are equivalent:

- There exists a proper model of $C$ that is at-most-model of relative dimension 1 over $R$.
- There exists a minimal model of $C$ that is at-most-model of relative dimension 1 over $R$.
- Any minimal model of $C$ that is at-most-model of relative dimension 1 over $R$.

If this is the case, then $C$ is said to have semistable reduction.
Proof: Cf.[Sta]0CDG.

**Prop. (13.7.2.6)[Good Reductions]**. Let $R$ be a DVR with fraction field $K$, for a smooth projective curve $C$ over $K$, the following are equivalent:

- $C$ has good reduction over $R$.
- There exists a minimal model of $C$ that is smooth over $R$.
- Any minimal model of $C$ is smooth over $R$.

Proof: Cf.[Sta]0CDI.

**Good Reduction for Curves**

**Prop. (13.7.2.7)[Reduction of Morphisms]**. For any morphism $\varphi : C \to C'$ of smooth projective curves over $\mathbb{Q}$ with good reduction at $p$ and $g(C') > 0$, there exists a unique reduction morphism $\overline{\varphi} : \overline{C} \to \overline{C'}$ that commutes with the reduction map $(13.7.1.2)$. This defines a functor from the category of smooth projective curves of positive genus with good reduction to the category of smooth curves over $\mathbb{F}_p$.

Moreover, $\deg(\varphi) = \deg(\overline{\varphi})$, and by $(13.7.1.2)$, if $\varphi$ is surjective, $\overline{\varphi}$ is also surjective. And $\varphi$ is an isomorphism iff $\overline{\varphi}$ is an isomorphism.

Proof: Cf.[BLR90]Prop 9.5.1?

**Cor. (13.7.2.8)**. If $\varphi : E \to E'$ is an isogeny of elliptic curves over $\mathbb{Q}$ with good reduction at $p$, then the reduction morphism $\overline{\varphi} : \overline{E} \to \overline{E'}$ is also an isogeny.

Proof: Because it maps $\overline{O}_E$ to $\overline{O}_{E'}$ and is surjective, this follows from $(13.5.1.4)$.

**Prop. (13.7.2.9)[Pushforward of Divisors]**. Let $C$ be a smooth projective curve over $\mathbb{Q}$ with good reduction at $p$, then the reduction map $X(\overline{K}) \to \tilde{X}(\mathbb{F}_p)$ induces a map

$$\text{Div}^0(X) \to \text{Div}^0(\tilde{X})$$

that maps principal divisors to principal divisors, so inducing a map $\varphi_* : \text{Pic}^0(C) \to \text{Pic}^0(C')$, which is compatible with pushforward of divisors along morphisms of curves: if $h : C \to C'$ is a morphism of smooth projective curves over $\mathbb{Q}$ with good reductions at $p$, then the following digram is commutative:

$$\begin{array}{ccc}
\text{Pic}^0(C) & \xrightarrow{h_*} & \text{Pic}^0(C') \\
\downarrow & & \downarrow \\
\text{Pic}^0(\overline{C}) & \xrightarrow{\overline{h}_*} & \text{Pic}^0(\overline{C'})
\end{array}$$

Proof: Cf.[BLR90]Prop 9.5.1?

**Classification of Special Fibers of the Minimal Regular Models of Curves of Genus 2**

13.8 Arithmetic of Elliptic Curves

Main References are [Sil16] and [Sil99], [Sil11], http://www-personal.umich.edu/~asnowden/teaching/2013/679/index.html. Should add Snowden’s notes 5,6,7,9,11, 14, 15, 17-23.

Notations (13.8.0.1).
- Use notations defined in Arithmetic of Abelian Varieties.
- Use notations defined in Algebraic Number Theory.

1 Basics

Def. (13.8.1.1) [Elliptic Curves]. An elliptic curve $E$ is a complete non-singular curve of genus 1 over a field $k$, together with a specified rational pt $O$. In (13.8.1.9), we will see an elliptic curve is smooth.

Let $S \in \text{Sch}$, then an elliptic scheme over $S$ is a proper smooth scheme over $S$ with a section $e : S \to E$ s.t. all the fibers are elliptic curves over the resp. residue field $k(s)$ with the origin given by $e$. The category of elliptic schemes over $S$ is denoted by $\text{Ell} / S$.

Remark (13.8.1.2). Elliptic curves are Abelian varieties by (13.8.1.9). Thus the theory of Abelian varieties apply to elliptic curves.

Weierstrass Theory

Def. (13.8.1.3) [Weierstrass Equations]. A Weierstrass equations is an equation of the form

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6.$$  

Def. (13.8.1.4) [Important Identities]. Let $k \in \text{Field}, E \in \text{Ell} / k$, given any Weierstrass equation as in (13.8.1.3), we can define

- $b_2 = a_1^2 + 4a_2$, $b_4 = a_1a_3 + 2a_4$, $b_6 = a_3^2 + 4a_6$, $b_8 = a_1^2a_6 - a_1a_3a_4 + a_2a_3^2 + 4a_2a_6 - a_2^2$.
- $\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6$ the discriminant of $E$, to determine whether $E$ is singular.
- the quantity $c_4 = b_2^2 - 24b_4$, used in the singular case to determine if it has a node or cusp.
- the quantity $c_6 = -b_2^3 + 36b_2b_4 - 216b_6$, used to determine twisted elliptic curves.
- the $j$-invariant $j = c_4^3 / \Delta$, which is used to in the non-singular case to characterize $E$.

They satisfy the equations:

$$4b_8 = b_2b_6 - b_4^2, \quad 1728\Delta = c_4^3 - c_6^2.$$  

Prop. (13.8.1.5) [Reduced Weierstrass Equations]. Let $k \in \text{Field}, E \in \text{Ell} / k$, given any Weierstrass equation as in (13.8.1.3),

- If $\text{char} k \neq 2$, we can replace $(x, y)$ by $(x, y - (a_1x + a_3)/2)$ to eliminate $a_1, a_3$ to transform the original Weierstrass equation to

$$y^2 = x^3 + \frac{b_2x^2 + 2b_4x + b_6}{4}.$$  

- If $\text{char} k \neq 2, 3$, then we can further replace $(x, y)$ to $((x - 3b_2)/36, y/216)$ to eliminate $b_2$ to transform the Weierstrass equation to

$$y^2 = x^3 - 27c_4x - 54c_6.$$
In particular, $E$ has a Weierstrass equation of the form

$$y^2 = x^3 + a_4 x + a_6, \quad \Delta = -16(4a_4^3 + 27a_6^2), \quad j = 1728 \frac{4a_4^3}{4a_4^3 + 27a_6^2}$$

- If $\text{char } k = 3$, then $E$ has a Weierstrass equation of the form
  $$y^2 = x^3 + a_2 x^2 + a_6, \quad \Delta = -a_2^3 a_6, \quad j = a_2^3 / a_6,$$  or  $$y^2 = x^3 + a_4 x + a_6, \quad \Delta = -a_4^3, \quad j = 0$$
- If $\text{char } k = 2$, then $E$ has a Weierstrass equation of the form
  $$y^2 + y = x^3 + a_2 x^2 + a_6, \quad \Delta = a_6, \quad j = 1 / a_6,$$  or  $$y^2 + a_3 y = x^3 + a_4 x + a_6, \quad \Delta = a_3^4, \quad j = 0.$$

Prop. (13.8.1.6) [Explicit Embedding of Elliptic Curves]. Any $E \in \text{Ell}/k$ is isomorphic to the plane curve in $\mathbb{P}_k^2$ defined by an affine Weierstrass equation in $k[x, y]$.

And any isomorphism between elliptic curves defined by affine Weierstrass equations over $k$ and fixes $[0, 1, 0]$ are linear maps of the form

$$(X, Y) \mapsto (u^2 X + r, u^3 Y + s u^2 X + t), \quad u \in k^*, s, r \in k.$$

Proof: If $E$ is an elliptic curve over $k$, consider a rational point $O \in E(k)$, Riemann-Roch (5.11.2.9) tells $l(nP) = \deg(nP) = n$ for $n \geq 1$. Now $L(kP) = k$ by Riemann-Roch (5.11.2.9). So we choose a basis $1, x$ for $\mathcal{O}_X(2O)$, and extend it to a basis $1, x, y$ of $L(3P)$. Since $L(6O) = 6$, there is a linear relation between the seven elements $1, x, x^2, xy, y^2, x^3$. And $y^2, x^3$ must occur by observing the pole order at $P$. Thus by rescaling, we can write the relation as

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6.$$

So $x, y$ defines a rational map of $E$ to $\mathbb{P}^2 : a \mapsto (x(a), y(a), 1)$. This map extends to an embedding of $E$ into $\mathbb{P}^2$, by (5.11.1.15). Moreover, by the above proof, if $E'$ is another Weierstrass form, then $1, x'$ are basis for $\mathcal{O}_X(2O)$ and $1, x', y'$ are basis for $\mathcal{O}_X(3O)$. Thus we have the linear relation between $(X, Y)$ and $(X', Y')$.

To define an Abelian structure on $E$, first notice that

$$E(k) \to \text{Cl}^0(E) : Q \mapsto [Q] - [P]$$

is an isomorphism. Using Riemann-Roch, it is injective because $l(Q) = 1$ for $Q \in E(k)$, and for any divisor $A$ of degree $0$, $L(A + P) > 0$, so there exists an effective divisor that is equivalent to $A + P$, but this must be a rational point $Q \in E(k)$. Thus we can endow $E(k)$ with a group structure inherited from $\text{Cl}^0(E)$. By (13.8.1.8), there is a group variety structure prolonging this construction, so $E$ is a group scheme.

Remark (13.8.1.7). There is a more advanced way to prove that this is a group action, in [Qing Liu]P492.

Lemma (13.8.1.8) [Explicit Group Structure]. Let $E$ be an elliptic curve given by a Weierstrass equation

$$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6,$$

then the group addition on $E \setminus O$ is given by

- $-(x_0, y_0) = (x_0, -y_0 - a_1 x - a_3)$. 

• \((x_1, y_1) + (x_2, y_2) = O\) iff \(x_1 = x_2\) and \(y_1 + y_2 + a_1 x_2 + a_3 = 0\). Otherwise

\[(x_1, y_1) + (x_2, y_2) = (\lambda^2 + a_1 \lambda - a_2 - x_1 - x_2, -(\lambda + a_1)x_3 - \nu - a_3)\]

where

\[
\lambda = \begin{cases} \frac{y_1 - y_2}{x_1 - x_2}, & x_1 \neq x_2 \\ \frac{3x_2^2 + 2a_2x_1 + a_1y_1}{2y_1 + a_1x_1 + a_3}, & x_1 = x_2 \end{cases}
\]

\[
\nu = \begin{cases} \frac{y_2^2x_1 - y_1x_2}{x_1 - x_2}, & x_1 \neq x_2 \\ \frac{-x_1^2 + a_2x_1 + 2a_6 - a_3y_1}{2y_1 + a_1x_1 + a_3}, & x_1 = x_2 \end{cases}
\]

• (Doubling Formula) \(x([2]P) = \frac{x^4 - b_4x^2 - 2b_6x - b_8}{4x^3 - b_2x^2 + 2b_4x + b_6}\).

Thus the group actions defined in (13.8.1.6) are all morphisms. In particular, \(E\) is a group variety.

**Proof:** Cf. [Sil16]P53. \(\square\)

**Cor. (13.8.1.9) [Elliptic Curves and Abelian Varieties].** If \(X\) is an Abelian variety of dimension 1, then \(X\) is an elliptic curve. The converse is also true, by (13.8.1.6). In particular, the theory of Abelian varieties 13.5 applies to elliptic curves. And we will use notations for Abelian varieties.

**Proof:** By (7.1.4.35)(7.1.4.34), the tangent space \(T_{X/k}\) is trivial of rank 1, thus it is a curve of genus 1 by (5.11.1.24). it is also regular, by (5.6.4.16). \(\square\)

**Prop. (13.8.1.10) [Normalized Invariant Differential Form].** Let \(k \in \text{Field}, E \in \mathcal{E}l\ell/k\) defined by a Weierstrass equation \(W : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6\). Then the differential form given by

\[
\omega = \frac{dx}{2y + a_1x + a_3} = \frac{dy}{3x^2 + 2a_2x + a_4 - a_1y}
\]

is a non-zero section of \(\mathcal{K}_E\). It is normalized s.t. at the origin, with the uniformizer \(z = -x/y\), it has value 1.

Moreover, it is invariant under translation. It is called the **normalized invariant differential form** on \(E\) w.r.t \(W\).

**Proof:** Firstly we show \(\text{div}(\omega) = 0\): consider a finite point \(P_0 = (x_0, y_0)\), then it cannot have pole, otherwise \(P_0\) is singular. Because \(x - x_0 \in L(2O)\), \(\text{ord}_{P_0}(x - x_0) \leq 2\), and if \(\text{ord}_{P_0}(x - x_0) = 2\), \(\text{ord}_{P_0}(y - y_0) \geq 2\) also by inspecting the Weierstrass equation. Thus \(\text{ord}_{P_0}(\omega) = 0\). Also consider the situation at \(\infty\), \(\text{ord}_\infty(x) = -2\), \(\text{ord}_\infty(y) = -3\), thus \(\text{ord}_\infty(\frac{dx}{2y + a_1x + a_3}) = 0\) except possibly \(\text{char} K = 2\).

But the same calculation shows \(\text{ord}_\infty(\frac{dy}{3x^2 + 2a_2x + a_4 - a_1y}) = 0\) except possibly \(\text{char} K = 3\). Thus we are done.

Now any translation action induces a map \(\tau^*_x \omega = a(x)\omega\), where \(a \in K(C)^\times\). But \(a(x)\) has no pole and zeros, thus \(a(x) \in K^\times\). But then \(a(x)\) is rational function with no zero and poles, thus \(a(x) = a(O) = 1\). \(\square\)

**Cor. (13.8.1.11).** \(m^*_E \omega = pr_1^* \omega + pr_2^* \omega\).

**Proof:** It follows from this and the see-saw principal that \(m^*_E \mathcal{K}_E \cong pr_1^* \mathcal{K}_E \otimes pr_2^* \mathcal{K}_E\). \(\square\)

**Prop. (13.8.1.12) [Change of Variables].** A change of variables of the form \((x, y)\) replaced by \((u^2 + a, u^3 + y + bx + c)\) changes \(c_4\) to \(u^8 c_4\), \(c_6\) to \(u^6 c_6\), \(\Delta\) to \(u^{-12} \Delta\), and preserves \(j\).

**Proof:** This is just a equation of identities, so it suffices to prove for \(k\) of characteristic 0, then in this case, by (13.8.1.5), \(c_4, c_6\) is just the coefficients of the Weierstrass equation transformed into the reduced form(times a constant). So it suffices to prove for transformation between reduced Weierstrass equations. In this case, \(a = b = c = 0\), and the assertion is clear. \(\square\)
Prop. (13.8.1.13)[Characterizing Singularities]. Let $k \in \text{Field}$, then
- The plane cubic $E$ over $k$ defined by a Weierstrass formula $f$ is never singular at $O = [0, 1, 0]$, and it is a curve.
- $E$ is smooth iff its determinant $\Delta \neq 0$. And in this case it is an elliptic curve by genus formula.
- $E$ has a node iff $\Delta = 0$ and $c_4 \neq 0$.
- $E$ has a cusp iff $\Delta = c_4 = 0$.

For $E, E' \in \mathbb{E}ll/k$, $E_k \cong E'_k$ iff $j(E) = j(E')$. In fact, they are isomorphic over a separable field extension $k'/k$ of degree 24, and if $j \neq 0, 1728$, then they are isomorphic over a separable field extension $k'/k$ of degree 2.

Proof: 1: Firstly, $E$ is never singular at $[0, 1, 0]$: On $U(z)$, the curve is given by $z + a_1xz + a_3z^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3$, which is not singular at $(0, 0)$. Secondly, $E$ has genus 1. Finally it is a curve by(2.2.3.13) and checking $f$ doesn’t have a root $y \in \overline{k}(x)$: This is true by degree reasons using reduced Weierstrass equations(13.8.1.5).

2: (1): By(13.8.1.9), non-singular is equivalent to smoothness. So we may base change to $\overline{k}$. If $P$ is non-singular, linearly transform it to $(0, 0)$, then by Jacobian criterion, $\frac{\partial}{\partial x}f = \frac{\partial}{\partial y}f = 0$, so $a_3 = a_4 = a_6 = 0$, and it can be verified that $\Delta = 0$. Conversely, if $\Delta = 0$, then use the reduced Weierstrass equations and argue case by case, we can find a singular point.

(2), (3): In this case, assume $a_3 = a_4 = a_6 = 0$, then $c_4 = (a_1^2 + 4a_2)^2$, and $E : y^2 + a_1xy - a_2x^2 - x^3 = 0$, so the assertion is clear.

2: We use the reduced Weierstrass equations, derive an equation between their coefficients, and take a suitable change of variables. Details are omitted.

Prop. (13.8.1.14)[Fields of Moduli]. For any element $j_0 \in \overline{k}$, there exists an elliptic curve over $k(j_0)$ with $j$-invariant $j$. In particular, any elliptic curve over $k$ is defined over $k(j(E))$, by(13.8.1.13).

Proof: If $j_0 \neq 0, 1728$, then we can take the curve

$$E : y^2 + xy = x^3 - \frac{36}{j_0 - 1728}x - \frac{1}{j_0 - 1728}$$

with $\Delta(E) = \frac{j_0^3}{(j_0 - 1728)^2}$, $j(E) = j_0$.

If $j = 0$ or $1728$, we can take one of the curves

$$E : y^2 + y = x^3, \quad \Delta = -27, \quad j = 0$$

$$E : y^2 = x^3 + x, \quad \Delta = -64, \quad j = 1728.$$  

Notice for char $k = 2$ or $3$, $0 = 1728$, and at least one of these are elliptic curves.

Prop. (13.8.1.15)[Singular Weierstrass]. If $k \in \text{Field}$ is perfect or char $k \neq 2, 3$, $E \in \mathbb{P}^2_k$ is a plane cubic given by a Weierstrass equation $W$ is singular, then
- $E$ has a unique singular point, and it is a rational point.
- $E$ is birational to $\mathbb{P}^1_k$, i.e. its non-singular projective model is $\mathbb{P}^1(5.11.1.18)$.

$E_{\text{sm}}$ is a commutative $k$-group under the group action given in(13.8.1.8) with origin $O = [0, 1, 0]$, and $E_{\text{sm}} \cong G_m$ if $E$ has a split node, and $E_{\text{sm}} \cong G_a$ if $E$ has a cusp.
Prop. (13.8.1.16) [Legendre Forms]. Let \( \text{char} K \neq 2, 3 \), then
- every elliptic curve over \( K \) is isomorphic to an elliptic curve in **Legendre form**
  \[
  E_\lambda : y^2 = x(x-1)(x-\lambda), \quad \lambda \neq 0, 1 \in K.
  \]
- \( \Delta(E_\lambda) = 16\lambda^2(\lambda-1)^2, \quad j(E_\lambda) = \frac{2^8(\lambda^2-\lambda+1)^3}{\lambda^2(\lambda-1)^2}, \quad c_4 = 16(1-\lambda(1-\lambda)). \)
- If \( K \) is a valued field, we may take \( v(\lambda) \geq 0 \) as \( j(E_\lambda) = j(E_{\lambda^{-1}}) \).
- The map \( K \to \mathbb{K} : \lambda \mapsto j(E_\lambda) \) is 6 to 1 except above the points 0 and 1728, where for \( \text{char} K \neq 2, 3 \), \( \# j^{-1}(0) = 2 \), \( \# j^{-1}(1728) = 3 \), and for \( \text{char} K = 3 \), \( j^{-1}(0 = 1728) = 1 \).

Proof: 1: put the Weierstrass equation of \( E \) in the reduced form (13.8.1.5), then it is of the form
\[
y^2 = (x-e_1)(x-e_2)(x-e_3)
\]
in \( \mathbb{K}[x,y] \), and because \( \Delta = 16(e_1-e_2)^2(e_2-e_3)^2(e_3-e_1)^2 \neq 0 \), so \( e_1, e_2, e_3 \) are pairwise distinct. Thus the linear transform
\[
x \mapsto (e_2-e_1)x' + e_1
\]
makes the Weierstrass equation in the Legendre form with \( \lambda = \frac{e_3-e_1}{e_2-e_1} \).

2: Direct calculation.
3: Directly calculating the differential of \( j \).

Prop. (13.8.1.17) [Duering Normal Form]. Every elliptic curve over \( K \), except possibly \( \text{char} K = 3 \) and \( j(E) = 0 \), is isomorphic to an elliptic curve in **Deuring normal form**
\[
E_\alpha : y^2 + \alpha xy + y = x^3, \quad \alpha \in \mathbb{K}, \quad \Delta(E_\alpha) = \alpha^3 - 27 \neq 0, \quad j(E_\alpha) = \frac{\alpha^3(\alpha^3 - 24)^3}{\alpha^3 - 27}, \quad c_4 = \alpha(\alpha^3 - 24).
\]
And if \( K \) is a valued field, we can take \( v(\alpha) > 0 \).
Proposition 13.8.1.18 [Automorphism Group]. Let $E$ be an elliptic curve over a field $k$, then the automorphic group of $E$ is

$$\text{Aut}(E) \cong \begin{cases} \mu_2(k) & j(E) \neq 0, 1728 \\ \mu_4(k) & j(E) = 1728, \text{ char } k \neq 2, 3 \\ \mu_6(k) & j(E) = 0, \text{ char } k \neq 2, 3 \\ D_{12} & j(E) = 0 = 1728, \text{ char } k = 3, k=\overline{k} \\ C_3 \ltimes Q_8 & j(E) = 0 = 1728, \text{ char } k = 2, k=\overline{k} \end{cases}$$

Proof: Any automorphism of $E$ is defined by a linear map of the form

$$(X,Y) \mapsto (u^2X + r, u^3Y + su^2X + t), \quad u \in k^*, s, r \in K.$$ 

If char $k \neq 2, 3$, use the reduced Weierstrass form $E : y^2 = x^3 + Ax + B$, so it is of the form $(X,Y) \mapsto (u^2X, u^3Y)$, which is possible if $u^{-4}A = A, u^{-6}B = B$. Thus by arguing case by case, we are done.

The char $k = 2, 3$ cases are similar, use reduced Weierstrass forms (13.8.1.5) and argue case by case.

Proposition 13.8.1.19 [Dual Elliptic Curves]. An elliptic curve $E$ is canonically isomorphic to its dual $\hat{E}$, by the mapping $P \mapsto L(P - O)$.

Proof: This morphism is induced by the ample line bundle $L(O)(13.5.4.2)$, and it is an isomorphism because it has degree 1, by Riemann-Roch (13.5.5.2).

Corollary 13.8.1.20. For any $L \in \text{Pic}(E)$ of degree $d$, $\varphi_L = [d] : E \to E$ via the canonical duality, because $\text{Pic}^0(E)$ induces trivial maps by (13.5.4.8) and (6.1.12.5).

Corollary 13.8.1.21 [Characterizing Principal Divisors]. Let $E \in \text{Ell}/k$ and $D = \sum n_i [P_i] \in \text{Div}(E)$, where $P_i$ are rational points, then $D$ is a principal divisor iff $\sum n_i = 0$ and $\sum [n_i] P_i = O$.

Proof: Of course $\sum n_i = 0$. In this case, $\sum [n_i] P_i$ is mapped to the line bundle corresponding to $[D] \in \hat{E}$ via $E \to \hat{E}$, so $[D] = 0$ iff $\sum [n_i] P_i = O$.

Isogenies

Proposition 13.8.1.22. Let $\varphi, \varphi' : E' \to E$ be isogenies of elliptic curves over $k$, and let $\omega$ be an invariant differential on $E$, then by (13.8.1.11),

$$(\varphi + \varphi')^* \omega = \varphi^* \omega + (\varphi')^* \omega.$$ 

Corollary 13.8.1.23. $[m]^* \omega = m \omega$.

Corollary 13.8.1.24 [End$(E)$ is Commutative in Characteristic 0]. Let $E \in \text{Ell}/k$ with the normalized invariant differential form $\omega$, then there is a ring homomorphism

$$\text{End}(E) \to k : \varphi \mapsto a_\varphi, \text{ where } \varphi^* \omega = a_\varphi \omega.$$ 

And the kernel is the set of inseparable endomorphisms of $E$. In particular, if char $k = 0$, then $\text{End}(E)$ is commutative.
Proof:  Cf.[Sil16]P79.

Prop.(13.8.1.25) [Dual Isogenies]. Let $k \in \text{Field}$, $E, E' \in \text{Ell}/k$ and $\varphi \in \text{Hom}(E, E')$, then under
the canonical isomorphism(13.8.1.19), the dual map $\hat{\varphi}$ can be regarded as a map $\hat{\varphi} : E' \to E$. Then
$$\hat{\varphi} \circ \varphi = [\deg(\varphi)]_E, \varphi \circ \hat{\varphi} = [\deg(\varphi)]_{E'}.$$

End($E) \to \text{End}(E) : \varphi \mapsto \hat{\varphi}$ is additive, and defines an involution on End($E$).

Proof: Let $d = \deg(\varphi)$. By unwinding definition, $\hat{\varphi} \circ \varphi : E \to E' \to \tilde{E}' \to \tilde{E}$ is just $\varphi \varphi_* E(O)$. But for elliptic curves, $\varphi_L$ only depends on $\deg(L)$, thus $\varphi \varphi_* E(O) = \varphi_L(dO) = [d] \varphi_L(O)$. The second assertion follows by noticing $\varphi = \hat{\varphi}$ and $\deg(\varphi) = \deg(\hat{\varphi})$(13.5.6.5).

Cor.(13.8.1.26) [End($E$)]. Let $k$ be a field and $E \in \text{Ell}/k$, then End($E$) $\otimes Q$ is a division ring.

Prop.(13.8.1.27) [Classification of End($E$)]. Let $k \in \text{Field}, E \in \text{Ell}/k$, then End($E$) has the
following three possibilities:

- $\mathbb{Z}$,
- an order in an imaginary quadratic extension over $Q$.
- an order in a definite quaternion algebra over $Q$.

And the third case won’t happen in characteristic 0, by (13.8.1.24).

Proof: This follows from (2.4.5.1).

2 Formal Groups of Elliptic Curves

In this subsection, the formal group structure of an elliptic is studied.

In this subsection, $E$ is an elliptic curve over a field $K$ given by Weierstrass equation $y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$.

Prop.(13.8.2.1) [Calculation of Formal Group Law]. Make a change of variable $z = -x/y, w = -1/y$ to the Weierstrass equation of $E$, the equation becomes
$$w = z^3 + (a_1z + a_2z^2)w + (a_3 + a_4z)w^2 + a_6w^3 = f(z, w).$$

Then

- $\hat{\mathcal{O}}_{E,O} \cong K[[z]]$.
- There is a unique power series $w(z) \in \mathbb{Z}[a_1, \ldots, a_6][[z]]$ satisfying $w(0) = 0$ and $w(z) = f(z, w(z))$.
- $w(z) = z^3(1 + A_1z + A_2z^2 + \ldots)$, where $A_n$ is a homogenous polynomial in $a_1, \ldots, a_6$, where $a_i$ has weight $i$.
- $x(z) = z/w(z) = z^{-2} - a_1z^{-1} - a_2 - a_5z - (a_4 + a_1a_3)z^2 + \ldots \in \mathbb{Z}[a_1, \ldots, a_6][[z]]$
- $y(z) = -1/w(z) = -z^{-3} + a_1z^{-2} + a_2z^{-1} + a_3 + (a_4 + a_1a_3)z + \ldots \in \mathbb{Z}[a_1, \ldots, a_6][[z]]$
- The formal group law of $E$(13.5.2.1) is given by
$$F(z_1, z_2) = z_1 + z_2 - a_1z_1z_2 - a_2(z_1^2z_2 + z_1z_2^2) + (-2a_3z_1^3z_2 + (a_1a_2 - 3a_3)z_1^2z_2^2 - 2a_3z_1z_2^3) + \ldots \in \mathbb{Z}[a_1, \ldots, a_6][[z_1, z_2]].$$
The normalized invariant differential form (13.8.1.10)
\[
\omega(z) = \frac{dx(z)}{2y(z) + a_1x(z) + a_3} = [1 + a_1z + (a_1^2 + a_2)z^2 + (a_1^3 + 2a_1a_2 + 2a_3)z^3 + (a_1^4 + 3a_1^2a_2 + 6a_1a_3 + a_3^2 + 2a_4)z^4 + \ldots]dz \in \mathbb{Z}[a_1, \ldots, a_6][[z]]dz
\]

In particular, this formal group law is defined over \( \mathbb{Z}[a_1, \ldots, a_6] \).

Proof: \( \omega(z) \in \mathbb{Z}[a_1, \ldots, a_6][[z]]dz \) by (7.5.3.16).

For \( F(z_1, z_2) \): ?

\( \square \)

Prop. (13.8.2.2) [Inseparable Degree and Heights]. Let \( K \) be a field of characteristic \( p > 0 \) and \( E_1/K, E_2/K \) be two elliptic curves, and \( \varphi : E_1 \to E_2 \) a non-zero isogeny of elliptic curves over \( K \), and let \( \hat{\varphi} : \hat{E}_1 \to \hat{E}_2 \) be the homomorphism of formal group schemes, then
\[
\deg_\alpha(\varphi) = p^{ht(\hat{\varphi})}.
\]

Proof: Cf. [Sil16]P134. ?

\( \square \)

Cor. (13.8.2.3). Let \( K \) be a field of characteristic \( p > 0 \), then \( \text{ht}(\hat{E}) = 1 \) or \( 2 \), because \( \deg([p]_E) = p^2(13.5.6.14) \).

3 char \( k > 0 \) Case

In this subsection, \( E \) is an elliptic curve over a field \( k \) of characteristic \( p \) given by Weierstrass equation \( y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \).

Prop. (13.8.3.1). Let \( k = \mathbb{F}_q \), \( \#E(k) \equiv 0 \mod 4 \).

Proof: There are two involutions on \( E \): \( (x, y, z) \mapsto (x, -y, z) \), \( (x, y, z) \mapsto (z, y/x, x) \). The fixed points of these elements contain
\[
(0, 1, 0), \quad (0, 0, 1), \quad (\varepsilon_1, \varepsilon_2\sqrt{2\varepsilon_1}, 0), \quad (\varepsilon_3\sqrt{-1}, 0, 1).
\]
Considering either cases s.t. \( -1 \in \mathbb{F}_q^2 \) or \( 2 \in \mathbb{F}_q^2 \), the number of these points are divisible by 4, thus we are done.

\( \square \)

Prop. (13.8.3.2) [Hasse-Weil]. Let \( p \in \mathbb{P}, q = p^r, k = \mathbb{F}_q \) and \( E \in \mathcal{E}/k \), then
- If \( a = 1 + q - \#E(\mathbb{F}_q) \), \( \alpha, \beta \) be the two roots of \( T^2 - aT + q = 0 \), then \( \#E(\mathbb{F}_q^n) = 1 + q^n - \alpha^n - \beta^n \).
- \( \#E(\mathbb{F}_q) - 1 - q \leq 2\sqrt{q} \).
- The Frobenius map \( \varphi_E : E \to E \) satisfies \( \varphi^2 - a \varphi + [q] = 0 \).
- \( a = 1 + q - \deg(1 - \varphi) \), and \( [a] = \varphi + \hat{\varphi} \).

Proof: 1, 2 are special cases of (13.5.9.3). 3, 4 follow from (13.5.7.9) and (13.5.6.17).

\( \square \)

Cor. (13.8.3.3). Let \( k = \mathbb{F}_q, p \neq 2 \) and \( E \) is given by \( y^2 = x^3 + a_2x^2 + a_4x + a_6 \), then
\[
| \sum_{x \in \mathbb{F}_q} \left( \frac{x^3 + a_2x^2 + a_4x + a_6}{\mathbb{F}_q} \right) | \leq 2\sqrt{q}.
\]

Proof: This is because \( \#E(\mathbb{F}_q) = \sum_{x \in \mathbb{F}_q} (1 + (\frac{x^3 + a_2x^2 + a_4x + a_6}{\mathbb{F}_q})) \).

\( \square \)
Supersingular Elliptic Curves

Def. (13.8.3.4) [Supersingular Elliptic Curve]. Let $k \in \text{Field}$, $\text{char } k = p > 0$, $F_{E/k,r} : E \to E(p^r)$ the relative Frobenius (5.2.10.1), and $\hat{F}_{E/k}$ be its dual. Then the following are equivalent:

- $E[p^r] = 1$ for all $r \geq 1$.
- $E[p^r] \not\cong \mathbb{Z}/p^r\mathbb{Z}$ for some $r \geq 1$.
- $\hat{F}_{E/k,r}$ is purely inseparable for one (thus all) $r$.
- $[p] : E \to E$ is purely inseparable, and $j(E) \in \mathbb{F}_{p^2}$.
- $\text{End}(E)$ is an order in a quaternion algebra.
- The formal group $\hat{E}/K$ associated to $E$ has height $2(\neq 1)$.

Such curves are called supersingular elliptic curves, otherwise $E$ is called an ordinary elliptic curve.

Being supersingular is stable and reflective under base change.

Proof: Cf. [Silverman P144]. □

Prop. (13.8.3.5) [Ordinary Elliptic Curves]. Let $k \in \text{Field}$, $\text{char } k = p > 0$, $E \in \text{Ell }/k$ be an ordinary elliptic curve, then

- If $j(E) \in \mathbb{F}_p$, then $\text{End}(E)$ is an order in an imaginary quadratic field over $\mathbb{Q}$. In particular, this is the case when $k$ is a finite field.
- If $j(E) \notin \mathbb{F}_p$, then $\text{End}(E) \cong \mathbb{Z}$.

Proof: 1: If $j(E) \in \mathbb{F}_p$, then $E$ is defined over some $F_q$. Let $\varphi$ be the Frobenius, then if $\varphi^r \in \mathbb{Z}$, $\varphi^r = [\pm q^r]$, so $\#E[\varphi^r] = \deg_s(\varphi^r) = 1$ by (13.5.6.3), contradicting the fact $E$ is ordinary. Thus the assertion follows from (13.8.1.27).

2: ? □

Def. (13.8.3.6) [Hasse Invariant].

Prop. (13.8.3.7) [Supersingular and Trace]. Let $E \in \text{Ell }/\mathbb{F}_q$ and $\varphi_E$ be the Frobenius of $E/\mathbb{F}_q$, then

- $E$ is supersingular iff $\#E(\mathbb{F}_q) \equiv 1 \mod p$, iff $a_p = \alpha + \beta \equiv 0 \mod p$ in (13.8.3.2).
- If $q = p \geq 5$ is a prime, then $E$ is supersingular iff $\#E(\mathbb{F}_p) = p + 1$. This is false for $p = 2$ or $p = 3$.

Proof: 1: By (13.8.3.2), let $a = 1 + q - \#E(\mathbb{F}_q)$, then $\hat{\varphi}_E = [a] - \varphi$ is separable iff $a = 0 \in \mathbb{F}_q$ by ?? . Thus the assertion follows from (13.8.3.4).

2: Because $|\alpha + \beta| \leq 2\sqrt{p} < p$ in this case. □

Cor. (13.8.3.8). Let $p \geq 5$ and $E \in \text{Ell }/\mathbb{F}_p$ be supersingular, then

$$\#E(\mathbb{F}_{p^n}) = \begin{cases} p^n + 1 & n = 2k + 1 \\ (p^{n/2} - (-1)^{n/2})^2 & n = 2k \end{cases}$$

Proof: This is because $\alpha = -\beta = \sqrt{p}i$. □
Prop.(13.8.3.9)[Supersingular in Characteristic 2]. Let \( k \) be a field of characteristic 2, then \( E/k \) is supersingular iff \( j(E) = 0 \). In particular, \( y^2 + y = x^3 \) is the only supersingular elliptic curve over \( \overline{k} \).

**Proof:** We use the condition \( \# E(\mathbb{F}_2) = 2 \). We use the reduced Weierstrass equations in (13.8.1.4). By doubling formula (13.8.1.8), this is equivalent to the non-existence of a point \( (x, y) \in E(\overline{k}) \setminus O \) s.t. \( a_1 x + a_3 = 0 \). And it can be checked this is true iff \( j(E) = 0 \). \( \square \)

Prop.(13.8.3.10)[Supersingnals over Finite Fields]. Let \( p \in \mathbb{P} \) and \( E \in \mathfrak{E} \ell / \mathbb{F}_p \).
1. If \( p = 2 \), the only supersingular elliptic curve over \( \mathbb{F}_2 \) is isomorphic to \( y^2 + y = x^3 \).
2. If \( p \geq 3 \) and \( E \) is given by a Weierstrass form \( y^2 = f(x) \), then \( E \) is supersingular iff

\[
\text{Coef}(\frac{f(x)}{x^{p-1}/2}) = 0 \in \mathbb{F}_p.
\]
3. If \( p \geq 3 \) and \( E \) is given by a Legendre form \( y^2 = x(x-1)(x-\lambda) \), then \( E \) is supersingular iff

\[
H_p(\lambda) = \sum_{i=1}^{(p-1)/2} \left( \frac{p-1}{i} \right)^2 \lambda^i = 0.
\]
4. If \( p \geq 3 \), the polynomial \( H_p \) has distinct roots in \( \overline{\mathbb{F}}_p \), and the number of supersingnlar elliptic curves over \( \mathbb{F}_p \) is

\[
\sum_{E/\overline{\mathbb{F}}_p \text{ supersingular}} \frac{1}{\text{Aut}(E)} = \frac{p-1}{24}.
\]

**Proof:** 1: This follows from (13.8.3.9).
2: Let \( E \in \mathfrak{E}ll / \mathbb{F}_q \), denote \( A_q = \text{Coef}(\frac{f(x)^{(q-1)/2}}{x^{q-1}}) \), then

\[
\# E(\mathbb{F}_q) \equiv \sum_{x \in \mathbb{F}_q} (1 + (\frac{x^3 + a_2 x^2 + a_4 x + a_6}{\mathbb{F}_q})) \equiv 1 - A_q \mod p.
\]

Then \( A_q \equiv a_E \mod p \), and the assertion follows from (13.8.3.7).
3: Finally, it can be seen from the equation \( f(x)^{(p+1-1)/2} = f(x)(p^r-1)/2[f(x)(p-1)/2]^{p^r} \) that \( A_{p+1} = A_{p} A_q^{p^r} \). So by an induction argument, \( A_q = 0 \) iff \( A_p = 0 \).

4: Consider the Picard-Fuchs differential operator

\[
D = 4t(t-1) \frac{\partial^2}{\partial t^2} + 4(1-2t) \frac{\partial}{\partial t} - 1,
\]
then direct calculation shows
\[ DH_p(t) = p \sum_{i=1}^{(p-1)/2} (p - 2 - 4i) \left( \frac{p-1}{i} \right)^2 t^i = 0. \]

Thus the multiple roots can only be 1 or 0. But \( H_p(0) = 1 \), and \( H_p(1) = \left( \frac{p-1}{2} \right)^2 \), thus \( H_p(t) \) has no multiple roots.

Let \( \varepsilon_p(j) = 1 \) if the elliptic curve \( E \) with the indicated \( j \)-invariant is supersingular, and \( \varepsilon_p(j) = 0 \) otherwise. Notice for \( p \geq 5 \), \( j : \lambda \rightarrow j(E_\lambda) \) is 6 to 1 except \( \#j^{-1}(0) = 2 \) and \( \#j^{-1}(1728) = 3 \), thus by counting the number of zeros of \( H_p(\lambda) \), the number of supersingular elliptic curves is
\[
\frac{1}{6} \left( \frac{p-1}{2} - 2\varepsilon_p(0) - 3\varepsilon_p(1728) \right) + \varepsilon_p(0) + \varepsilon_p(1728) = \frac{p-1}{12} + \frac{2}{3} \varepsilon_p(0) + \frac{1}{2} \varepsilon_p(1728).
\]

Thus the assertion follows from determining elliptic curves of \( j \)-invariants 0 and 1728 are supersingular or not, which is done by \((13.8.3.11)\).

5: It follows from the proof of item 4 that this number is 1/2 of number of roots of \( H_p(\lambda) = \frac{p-1}{24} \).

\[
\text{Lemma (13.8.3.11)} \text{[Examples of Supersingular Elliptic Curves].} \\
\begin{itemize}
  \item For \( p \geq 5 \), the elliptic curve \( E : y^3 = x^3 + 1 \) with \( j \)-invariant 0 is supersingular iff \( p \equiv 2 \mod 3 \).
  \item For \( p \geq 3 \), the elliptic curve \( E : y^2 = x^3 + x \) with \( j \)-invariant 1728 is supersingular iff \( p \equiv 3 \mod 4 \).
\end{itemize}
\]

\[ \text{Proof:} \] These follows form calculating the \( x^{p-1} \)-term of \( (x^3 + 1)^{p-1}/2 \) or \( (x^3 + x)^{p-1}/2 \) and \((13.8.3.10)\) item 2. \( \square \)

4 Reduction of Elliptic Curves

Main references are [Liu02].

In this subsection, let \( S \) be a Dedekind scheme with generic point \( \eta \) and function field \( K \).

\[ \text{Prop. (13.8.4.1)} \text{[Minimal Models of Elliptic Curves].} \text{Let} \ E \in \mathcal{E}ll/K \text{and} \mathcal{E}/S \text{be a minimal model for} \ E, \text{then} \\
\begin{itemize}
  \item \( \mathcal{E}_{\text{sm}}(S) = \mathcal{E}(S) = E(K) \).
  \item The automorphism \( (m, pr_2) : E \times_K E \rightarrow E \times_K E \) extends to an automorphism \( t : \mathcal{E} \times_S \mathcal{E}_{\text{sm}} \rightarrow \mathcal{E} \times_S \mathcal{E}_{\text{sm}} \).
  \item \( t \) induces an automorphism \( \mathcal{E}_{\text{sm}} \times_S \mathcal{E}_{\text{sm}} \rightarrow \mathcal{E}_{\text{sm}} \times_S \mathcal{E}_{\text{sm}} \), and \( pr_1 \circ \mathcal{E} \) makes \( \mathcal{E}_{\text{sm}} \) a smooth group scheme over \( S \) extending that of \( E \).
\end{itemize}
\]

\[ \text{Proof:} \] Cf. [Liu02]P492. \( \square \)

\[ \text{Prop. (13.8.4.2)} \text{[} N = \mathcal{E}_{\text{sm}} \text{].} \text{Let} \ (R, K) \text{be a DVR,} \ E \in \mathcal{E}ll/K \text{with minimal model} \mathcal{E}(13.7.2.4) \text{, then} \mathcal{E}_{\text{sm}} \text{is a Néron model for} \ E. \]

\[ \text{Proof:} \] To show universal property, let \( X/S \) be smooth, and \( f : X_\eta \rightarrow E \) be a morphism considered as a rational morphism \( X \rightarrow \mathcal{E}_{\text{sm}} \). Let \( \xi \in X \) be a point of codimension 1, and \( T = \text{Spec} \mathcal{O}_{X, \xi} \), then by \((13.6.5.7)\) and the proof of \((13.8.4.1)\), \( \mathcal{E} \times_S T \rightarrow T \) is an arithmetic surface with smooth locus \( N \times_S T \), so by \((13.6.2.8)\), \( N(T) = N_T(T) = E(K) \), which means \( f \) can be extended to \( \xi \). Then in fact \( f \) is a morphism by \((7.1.1.20)\). \( \square \)
over DVRs

In this subsubsection, let \((R, K, \mathfrak{m}, k)\) be a DVR, \(S = \text{Spec } R\).

**Def. (13.8.4.3) [Minimal Weierstrass Equation].** Let \(E \in \mathcal{E}/K\), then a **minimal Weierstrass equation** for \(E\) is an Weierstrass equation for \(E\) in \(R[X, Y]\) with determinant \(\Delta\) with minimal valuation.

**Prop. (13.8.4.4) [Uniqueness of Minimal Weierstrass Equations].** Let \(E \in \mathcal{E}/K\), then \(E\) has a minimal Weierstrass equation, and it is unique up to change of variables of the form

\[
(X, Y) \mapsto (u^2 X + r, u^3 Y + su^2 X + t), \quad u \in R^*, r, s, t \in R.
\]

Moreover, given any Weierstrass equation, then any change of coordinates that is used to produce a minimal Weierstrass equation is of the form

\[
(X, Y) \mapsto (u^2 X + r, u^3 Y + su^2 X + t), \quad u, r, s, t \in R.
\]

**Proof:** Cf.[Sil16]P186. \(\square\)

**Cor. (13.8.4.5) [Weierstrass Models].** Let \(E \in \mathcal{E}/K\), a minimal Weierstrass of \(E\) defines a model \(W/R\) of \(E\), and it is invariant of the Weierstrass equation chosen, called the **Weierstrass model** of \(E\). Denote \(\tilde{E} = \mathcal{W}_k\).

**Cor. (13.8.4.6) [Néron Differentials].** Let \(E \in \mathcal{E}/K\), a minimal Weierstrass equation of \(E\) defines an invariant differential on \(W/R\) by(13.8.1.10), called the **Néron differential** of \(E\).

**Prop. (13.8.4.7) [Weierstrass Model of Elliptic Curves].** Let \((R, K)\) be a DVR, if \(E \in \mathcal{E}/K\), then a Weierstrass equation with \(a_i \in R\) defines a scheme \(W \in \mathbb{P}^2_R\). Then

- Both \(W_{\text{sm}}\) and \(W\) has generic fiber \(E\). If \(E\) has good reduction and \(W\) is a minimal Weierstrass equation, then \(W = W_{\text{sm}}\) is smooth.
- The natural map \(W(R) \to E(K)\) is a bijection. If \(W\) is regular, then \(W_{\text{sm}}(R) \to W(R)\) is also a bijection.
- The group structure on \(E/K\) extends to a group structure on \(W_{\text{sm}}/R\), and the addition further extends to a group action of \(W_{\text{sm}}/R\) on \(W/R\).

**Proof:** Cf.[?]P321. \(\square\)

**Prop. (13.8.4.8) [Weierstrass Model and Minimal Models].** Let \((R, K)\) be a DVR, if \(E \in \mathcal{E}/K\) with minimal model \(\mathcal{E}\), then any minimal Weierstrass model \(W\) can be obtained by blowing down the finitely many components of \(\mathcal{E}_k\) which are disjoint from the closure in \(\mathcal{E}\) of \(O_E\). In particular, by(13.8.4.2), \(W_{\text{sm}}\) is isomorphic to the relative identity component \(\mathcal{N}_0\) of the Néron model of \(E\).

**Proof:** Cf.[Liu Qing, Thm. 9.4.35] \(\square\)

**Def. (13.8.4.9) [Reduction Types].** Let \((R, K, k)\) be a DVR with \(k\) perfect or char \(k \neq 2, 3\), and \(E \in \mathcal{E}/K\) with minimal Weierstrass model \(W\), then by(13.8.1.15), \(\tilde{E}\) is a geo.reducible cubic in \(\mathbb{P}^2\) with at most one rational singular point, and \(E\) is called

- a **good reduction** or **stable reduction** if \(\tilde{E} \in \mathcal{E}/k\).
• a **multiplicative reduction** or **semistable reduction** if $\tilde{E}$ has a node. And it is called a **split multiplicative reduction** if the node is split, otherwise it is called a non-split multiplicative reduction.

• a **additive reduction** or **unstable reduction** if $\tilde{E}$ has a cusp.

By (13.8.1.15), exactly one of the above is true.

Moreover, $E$ is called a **potentially good reduction** if $\overline{E}_{/K'} \in \text{Ell}/K'$ for some finite extension $K'/K$.


**Def. (13.8.4.10) [Reduction Modulo]**. Let $E$ be an elliptic curve over a CDVR $K$, let $W$ be a minimal Weierstrass equation for $E$, then $W$ defines a projective scheme $\mathcal{W}$ in $\mathbb{P}^2_{R}$. By valuation criterion of properness, the natural map $\mathcal{W}(\overline{R}) \to E(\overline{K})$ is an isomorphism. Let $\tilde{E} = \mathcal{W} \otimes_{R} k$, called the reduction modulo of $E$. Then there is a natural map $E(k) \to \tilde{E}(k)$, let

$$E_0(k) = \{ P \in E(k), \tilde{P} \in \tilde{E}_{\text{sm}}(k) \}, \quad E_1(k) = \{ P \in E(k), \tilde{P} = \tilde{O} \},$$

then by (13.8.1.15), $E_0(k)$ and $E_1(k)$ are Abelian groups, and $E_0(k) \to \tilde{E}_{\text{sm}}(k)$ is a group homomorphism. $E_1(k)$ is called the kernel of the reduction.

**Proof**: To see $\tilde{E}$ is well-defined, use (13.8.4.4). \hfill \Box

**Prop. (13.8.4.11)**. There is an isomorphism of groups

$$0 \to E_1(k) \to E_0(k) \to \tilde{E}_{\text{ns}}(k) \to 0.$$

**Proof**: Only the right surjectivity needs to be proved: Let $\tilde{P} \in \tilde{E}_{\text{ns}}(k)$. If $\tilde{P} = \tilde{O}$, then it is in the image, so we assume $\tilde{P}$ is a finite point $(\overline{x}, \overline{y})$. Then the minimal Weierstrass equation $f(x, y)$ of $E$ satisfies $\frac{\partial f}{\partial x} \equiv 0 \mod m$ or $\frac{\partial f}{\partial y} \equiv 0 \mod m$. We may assume the first case occurs. Let $x_0$ be a lift of $x$, then the equation $f(x_0, y) \in K[y]$ has a simple root $\overline{y}_0$ in $R$, then by Hensel’s lemma (4.3.10.6), it has a root $y_0$ in $R$ lifting $\overline{y}_0$. Then $P = (x_0, y_0) \in E(K)$ is a lift of $\tilde{P}$. \hfill \Box

**Prop. (13.8.4.12) [Formal Group is the Kernel]**. Let $E$ be given a minimal Weierstrass equation, then with notations as in (13.8.2.1),

$$\tilde{E}(K) \to E_1(K) : z \mapsto [z, -1, w(z)]$$

is an isomorphism of groups.

**Proof**: By (13.8.2.1), $\omega(z) \in z^2R[[z]]$, and by the definition of $w(z)$, $[z, -1, w(z)] \in E_1(K)$, and it is a group homomorphism by the definition of formal group law associated to $E$. It remains to prove that this map is surjective:

Clearly $\tilde{O}$ is in the image, suppose $(x_0, y_0) \in E_1(K)$, then $v(x_0) < 0, v(y_0) < 0$, thus by inspecting the Weierstrass equation, $v(x_0) = -2r, v(y_0) = -3r$ for some $r > 0 \in \mathbb{Z}$. Then $z_0 = x_0/y_0 \in m$, and $(x_0, y_0)$ is the image of $z_0$. \hfill \Box

**Prop. (13.8.4.13) [Characterizing Reductions]**. Let $E/K$ be an elliptic curve over $K$ given by a Weierstrass equation $E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$, then by (13.8.1.13),

- $\tilde{E}$ is a good reduction iff $\Delta \in R^*$.
- $\tilde{E}$ is a multiplicative reduction iff $\Delta \in m$ and $c_4 \in R^*$. 
• $\bar{E}$ is an additive reduction iff $\Delta, c_4 \in \mathfrak{m}$.

**Prop. (13.8.4.14)[Characterizing Potentially Good Reduction].** $E$ has potentially good reduction iff $j(E) \in R$.

In particular, an elliptic curve with complex multiplication over $K$ has potentially good reduction.

**Proof:** If $\bar{E}_K$ has good reduction, then $j(E) = (c'_4)^3/\Delta' \in R'$. Conversely, if $j(E) \in R$, use Legendre form or Deuring form (13.8.1.16) (13.8.1.17), the equation

$$j = 2^8(\lambda^2 - \lambda + 1)^3/\lambda^2(\lambda - 1)^2$$

implies $\lambda \in R^*, \lambda(\lambda - 1) \in R^*$ (or $\alpha \in R^*, \alpha^3 - 27 \in R^*$), so $\bar{E}_K$ has good reduction. \qed

**Prop. (13.8.4.15)[Tamagawa Numbers].** Let $(R, K, k)$ be a DVR and $E \in \mathcal{E}/K$ with minimal model $\bar{E}/R$, then $c(E)$ equals the number of geometric integral components occurring with multiplicity 1 in $\bar{E}_k$.

**Proof:** Cf.[Liu Qing, 10.2.24]. \qed

**Prop. (13.8.4.16)[Tamagawa Numbers].** Let $E/K$ be an elliptic curve. If $E$ has split multiplicative reduction over $K$, then $E(K)/E_0(K)$ is a cyclic group of order $v(\Delta) = -v(j)$. And in other cases, the group is finite and has order at most 4.

**Proof:**

**Cor. (13.8.4.17).** Let $K$ be a $p$-adic local field, then $E(K)$ contains a subgroup of finite index that is isomorphic to $\mathcal{O}_K$.

**Proof:** Because $E(K)/E_0(K)$ and $E_0(K)/E_1(K) \cong \bar{E}_{ns}(k)$ are all finite by (13.8.4.16), it suffices to prove that $E_1(K) \cong \bar{E}(\mathfrak{m})$ has a subgroup of finite index that is isomorphic to $\mathcal{O}_K$. But this follows from the fact $\bar{E}(\mathfrak{m}^r) \cong \mathfrak{m}^r$ for $r$ large (7.5.4.7). \qed

**Tate Algorithm**

**Prop. (13.8.4.18)[Kodaira-Néron].** Let $(R, m)$ be a DVR with fraction field $K$ and alg.closed residue field $k$. Let $E/K$ be an elliptic curve, and $\mathcal{C}/R$ a minimal proper regular model for $E$ over $R$, then the special fiber of $\mathcal{C}$ has one of the following Forms:

- (Type I$_0$) An elliptic curve.
- (Type I$_1$) A rational curve with a node.
- (Type I$_n$, $n \geq 2$) $n$ smooth rational curves intersecting transversally at a single point one-by-one in the shape of a $n$-gon.
- (Type II) A rational curve with a cusp.
- (Type III) Two non-singular rational curves which intersect tangentially at a single point.
- (Type I$_0^*$) A non-singular rational curve of multiplicity 2 with 4 non-singular rational curves of multiplicity 1 attached.
• (Type I*$_n$) A chain of $n+1$ non-singular rational curves of multiplicity 2, with two non-singular curves of multiplicity 1 attached at each end.

• (Type IV*) ?

• (Type III*) ?

• (Type II*) ?

**Proof:** Cf. [?] P354. □

![Figure (13.8.1): Kodaira Types](image)

**Prop. (13.8.4.19)[Tate Algorithm].** There is an algorithm that determines if a Weierstrass equation for $E$ is minimal.

**Torsion Points**

**Prop. (13.8.4.20)[Controlling Torsion Points].** Let $m \in \mathbb{Z} \cap k^\times$, then

- $E_1(K)[m] = O$
- The reduction map $E_0(K)[m] \rightarrow \tilde{E}_{sm}(k)[m]$ is injective.
- If $E$ has good reduction and $K = K^{\text{sep}}$, then it is also an isomorphism.

**Proof:**

1. By (13.8.4.12), $E_1(K)[m] \cong \tilde{E}(m)[m]$, which has only one element because $[m]_{\tilde{E}}$ is an isomorphism (7.5.3.5).

2. Follows from 1 and the exact sequence in (13.8.4.11).

3. Follows as they have the same cardinality. □

**Prop. (13.8.4.21)[Controlling Torsion Points].** Let $\text{char } K = 0$ and $\text{char } k = p > 0$, let $E$ be given by a Weierstrass equation

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6 \in R[X,Y].$$

Let $P = (x_0, y_0) \in E(K)$ be a torsion point of exact order $m$, then

- If $m$ is not a $p$-power, then $x_0, y_0 \in R$.
- If $m = p^r$, then $v(x) \geq -2\left\lceil \frac{v(p)}{p^r - p^{r-1}} \right\rceil$, $v(y) \geq -3\left\lceil \frac{v(p)}{p^r - p^{r-1}} \right\rceil$.

**Proof:** Change the Weierstrass equation to a minimal Weierstrass equation, then by (13.8.4.3), the coordinates in the new equation satisfies $v(x') \leq v(x_0), v(y') \leq v(y_0)$, thus it suffices to prove for minimal Weierstrass equations.

If $v(x_0) \geq 0$, then $v(y_0) \geq 0$. Suppose $v(x_0) < 0$, then $v(y_0) < 0$, and $v(x_0) = -2r, v(y_0) = -3r$ for some $r > 0$. Thus $P \in E_1(K)$ and thus corresponds to $z \in \tilde{E}(m)(13.8.4.12)$. Then the theorem follows from (7.5.4.6). □
Over Dedekind Domains

**Def. (13.8.4.22) [Canonical Heights].** For a number field \( F \) and \( E \in \text{Ell}/F \), by (13.5.13.4) and (13.5.4.8), \( \hat{h}_E \) only depends on \( \deg(L) \). And by (5.11.2.20), any degree 1 line bundle is ample, and the Néron-Tate bilinear form \( \langle \cdot, \cdot \rangle_{NT} \) given by this line bundle is called the **canonical height pairing** of \( E \). It is a positive-definite quadratic form on \( E(K) \otimes \mathbb{R} \) by (13.5.12.3). And for \( P \in E(K) \), \( \langle P, P \rangle_{NT} \) is called the **canonical height** of \( P \).

In particular we can take the line bundle \( \mathcal{O}(O) \), then \( \langle O, O \rangle_{NT} = 0 \), and for any \( P \neq 0 \in \mathcal{L}(O) \),

\[
\langle P, P \rangle_{NT} = \lim_{n \to \infty} h(x([2^n]^P))/4^N.
\]

**Proof:** For the final assertion, apply (13.2.4.19) to the morphism \( \varphi : E \to \mathbb{P}^1 \) associated to the rational function

\[
\langle P, P \rangle_{NT} = \lim_{n \to \infty} \hat{h}_{\mathcal{O}(2O)}([2^n]^P)/4^N = \lim_{n \to \infty} \hat{h}_{\mathcal{O}(1)}(\varphi([2^n]^P))/4^N = \lim_{n \to \infty} h(x([2^n]^P))/4^N.
\]

\( \square \)

**Prop. (13.8.4.23) [Elliptic Regulator].** Let \( F \) be a number field and \( E \in \text{Ell}/F \), then the **elliptic regulator** is the volume of a fundamental domain of \( E(K)/E(K)_{tor} \) computed using the canonical height. In particular, it is the discriminant of \( \langle (X_i, X_j)_{E,F} \rangle_{i,j} \) where \( \{X_i\} \) is a basis for \( E(K)/E(K)_{tor} \).

**Def. (13.8.4.24) [Minimal Discriminant].** For an elliptic curve \( E \) over a global field \( K \), define the **minimal discriminant** \( \mathcal{D}_{E/K} \) to be \( \mathcal{D}_{E/K} = \prod v \mathfrak{o}_v^{\text{ord} \Delta_v} \), where \( \Delta_v \) is the discriminant of a minimal Weierstrass equation for \( E \).

Then for any Weierstrass equation for \( E \), by (13.8.1.12), \( \mathcal{D}_{E/K} = \Delta(a_\Delta)^12 \) for some ideal \( a_\Delta \) of \( K \), and the ideal class of \( a_\Delta \) is stable under change of Weierstrass equations, called the **Weierstrass class** of \( E \), denoted by \( \mathfrak{a}_{E/K} \).

**Prop. (13.8.4.25) [A Curve Related to Fermat’s Last Theorem].** Let \( a, b, c \in \mathbb{Z}^\times \) satisfy \( (a, b, c) = 1 \), let \( E \) be the elliptic curve defined by the Weierstrass equation

\[
E : y^2 = x(x+a)(x-b),
\]

then

- the minimal Weierstrass equation \( \Delta_E^{\text{min}} \) for \( E \) is either \( 2^4|abc|^2 \) or \( 2^{-8}|abc|^2 \).
- \( E \) has semistable reduction for any odd prime.

**Proof:** By calculation

\[
\Delta_E = 2^4(ab)^2, \quad c_4 = 2^4(a^2 + ab + b^2), \quad c_6 = -2^5(2a^3 + 3a^2b + 3ab^2 + 2b^3),
\]

\[
(22a^2 - 8ab - 8b^2)c_4 + (a + 2b)c_6 = 288a^2, \quad -(8a^2 + 8ab - 22b^2)c_4 - (2a + b)c_6 = 288b^2.
\]

1: Any change of variable of \( E \) to the minimal Weierstrass equation satisfies \( u^4|c_4, u^6|c_6, \) so \( u^4|(288a^2, 288b^2) \)

so \( u = 1 \) or 2, and \( \Delta_E^{\text{min}} = u^{-12}\Delta_E = 2^4|abc|^2 \) or \( 2^{-8}|abc|^2 \).

2: If \( p \in \mathbb{P}\backslash\{2\} \) and \( p|\Delta_E \), then \( p \) divides \( a \) or \( b \) or \( c \). In each case, \( p \nmid c \), so \( E \) has multiplicative reduction at these \( p(13.8.4.13) \). \( \square \)
**Prop. (13.8.4.26) [Global Minimal Weierstrass Equation].** \(E/K\) has a global minimal Weierstrass equation if its Weierstrass class is trivial.

In particular, any elliptic curve over a global field \(F\) of class number 1, e.g. \(\mathbb{Q}\), has a global minimal Weierstrass equation.

**Proof:** Choose any Weierstrass equation for \(E\) over \(K\), let

\[
x = u_v^2 x + r_v, \quad y = u_v^3 y + s_v u_v^2 x + t_v, \quad u_v, r_v, s_v, t_v \in \mathcal{O}_{K,v}
\]

be the local change of variable to get the minimal Weierstrass equation at place \(v\), then by hypothesis, \((u_v)_v\) is principal, which means there is some \(u \in K\) s.t. \(v(u) = v(u_v)\) for any \(v\). Then choose by Chinese remainder theorem \(r, s, t \in \mathcal{O}_K\) that is closed to \(r_v, s_v, t_v\) for each relevant \(v\), then the change of variables

\[
x = u^2 x + r, \quad y = u^3 y + su^2 x + t
\]

changes the coordinates to a minimal Weierstrass equation.

**Cor. (13.8.4.27).** Let \(F\) be a global field with class number prime to 6 and \(E/K\) is an elliptic curve over \(F\) with everywhere good reduction, then \(E\) has a minimal model.

**Proof:** Because in this case the Weierstrass class \(a_\Delta\) is a 12-torsion in \(\text{Cl}(F)\), which implies it is trivial.

**Cor. (13.8.4.28).** If \(F\) is a global number field and \(S\) is a finite set of places of \(K\) s.t. \(\text{Cl}(\mathcal{O}_{F,S}) = 1\), then any elliptic curve over \(F\) has a minimal Weierstrass equation of the form \(y^2 = x^3 + Ax + B\) with \(A, B \in \mathcal{O}_{K,S}\) satisfying \(\Delta \mathcal{O}_{F,S} = D_{E/F} \mathcal{O}_{F,S}\).

**Proof:** The proof is easier than that (13.8.4.26).

**Prop. (13.8.4.29).** If \(F\) is a number field with class number \(\neq 1\), there exists an elliptic curve over \(F\) with no global minimal Weierstrass equations.

**Proof:** Cf. [Weierstrass equations and the minimal discriminant of an elliptic curve”, Mathematika 31 (1984), no. 2, 245–251].

**Prop. (13.8.4.30) [Density of Global Minimal Models].**

**Proof:** Cf. [The density of elliptic curves having a global minimal Weierstrass equation”, J. Number Theory 109 (2004), no. 1, 41–58].

5 Tate Curves

**Def. (13.8.5.1) [Formal Power Series].** Define power series

\[
s_k(q) = \sum_{n \geq 1} \sigma_k(n) q^n = \sum_{n \geq 1} \frac{n^k q^n}{1 - q^n} \in \mathbb{Z}[[q]],
\]

\[
a_4(q) = -5s_3(q), \quad a_6(q) = -\frac{5s_3(q) + 7s_5(q)}{12} \in \mathbb{Z}[[q]],
\]

\[
X(u, q) = \sum_{n \in \mathbb{Z}} \frac{q^n u}{(1 - q^n u)^2} - 2s_1(q), \quad Y(u, q) = \sum_{n \in \mathbb{Z}} \frac{(q^n u)^2}{(1 - q^n u)^2} + s_1(q) \in \mathbb{Z}[u][[q]].
\]
Prop. (13.8.5.2).

\[ s_1(q) = \sum_{n \geq 1} \frac{q^n}{(1 - q^n)^2} \in \mathbb{Z}[[q]], \]

\[ X(u, q) = \frac{u}{(1 - u)^2} + \sum_{n \geq 1} \frac{(q^n u)^2}{(1 - q^n u)^2} + \frac{q^n u^{-1}}{1 - q^n u^{-1}} - \frac{2q^n}{(1 - q^n)^2} \in \mathbb{Z}[u][[q]], \]

\[ Y(u, q) = \frac{u^2}{(1 - u)^3} + \sum_{n \geq 1} \frac{(q^n u)^3}{(1 - q^n u)^3} + \frac{q^n u^{-1}}{1 - q^n u^{-1}} - \frac{q^n}{(1 - q^n)^3} \in \mathbb{Z}[u][[q]], \]

Thus

\[ X(qu, q) = X(u, q) = X(u^{-1}, q), \quad Y(qu, q) = Y(u, q) \in \mathbb{Z}[u, u^{-1}][[q]]. \]

Proof: The first one follows from (7.5.2.2).

Prop. (13.8.5.3) [Relation to Weierstrass Ψ-Functions]. Let \( \Psi(z; \tau) \) be the Weierstrass \( \Psi \)-function associated to the lattice \( \Lambda_z = \text{span}\{1, \tau\}(10.5.7). \) Then \( X(e^{2\pi i z}, q(\tau)), Y(e^{2\pi i z}, q(\tau)) \) converges and uniformly and absolutely on \( \mathbb{C} \setminus \Lambda_z \) in \( \mathbb{C} \) to holomorphic functions, and

\[ \frac{1}{(2\pi i)^2} \Psi(z; \tau) = X(e^{2\pi i z}, q(\tau)) + \frac{1}{12}, \quad \frac{1}{(2\pi i)^3} \Psi(z; \tau)' = X(e^{2\pi i z}, q(\tau)) + 2Y(e^{2\pi i z}, q(\tau)). \]

Proof: The convergence of \( X, Y \) is clear. By (13.8.5.1), \( X(e^{2\pi i z}, q(\tau)) \) is \( \{1, \tau\}\)-doubly periodic, and clearly it has a double pole at the origin. Also the Laurent part of \( X(e^{2\pi i z}, q(\tau)) \) at \( z = 0 \) is the Laurent part of \( \frac{e^{2\pi i z}}{1 - e^{2\pi i z}q} \), which is \( \frac{1}{(2\pi i)^2 z} - \frac{1}{12} \). Then by comparison with that of \( \Psi(z; \tau)(10.5.7.6) \) and use Liouville’s theorem.

The second identity follows from applying \( \frac{\partial}{\partial z} \).

Prop. (13.8.5.4) [Tate Curve over \( \mathbb{C} \)]. Notation as in (13.8.5.1), then for \( q \in \mathbb{C}, 0 < |q| < 1, \)

- \( E_q : y^2 + xy = x^3 + a_4(q)x + a_6(q) \) is an elliptic curve over \( \mathbb{C} \), and

\[ \varphi : \mathbb{C}^*/q\mathbb{Z} \to E_q^0 : u \mapsto [X(u, q), Y(u, q), 1] \]

is a complex analytic isomorphism.

- The discriminant of \( E_q \) is given by

\[ \Delta(E_q) = \Delta(q) : q \prod_{n \geq 1} (1 - q^n)^{24}(15.11.5.8), \quad j(E_q) = j(q)(15.11.5.10) \]

- For any elliptic curve \( E/\mathbb{C} \), there exists a \( q \in \mathbb{C}^*, |q| < 1 \) s.t. \( E \) is isomorphic to \( E_q \).

Proof: Cf. [Sil99] P410.

Prop. (13.8.5.5) [Formal Identities]. There are identities

1. \(-a_6(q) + a_4^2(q) + 72a_4a_6 - 64a_4^3 - 432a_6^3 = \Delta(q) \in \mathbb{Z}[[q]]. \)

2. \( Y(u^{-1}, q) = -Y(u, q) - X(u, q) \in \mathbb{Z}[u, u^{-1}][[q]]. \)

3. \( Y(u, q)^2 + X(u, q)Y(u, q) = X(u, q)^3 + a_4(q)X(u, q) + a_6(q) \in \mathbb{Z}[u][[q]]. \)
4. 

\[(X(u_2, q) - X(u_1, q))^2 X(u_1 u_2, q) = (Y(u_2, q) - Y(u_1, q))^2 + (Y(u_2, q) - Y(u_1, q))(X(u_2, q) - X(u_1, q))\]

\[- (X(u_2, q) - X(u_1, q))^2 (X(u_2, q) + X(u_1, q))\]

\[(X(u_2, q) - X(u_1, q)) Y(u_1 u_2, q) = -(Y(u_2, q) - Y(u_1, q)) (X(u_2, q) - X(u_1, q)) X(u_1 u_2, q)\]

\[- (Y(u_1, q) X(u_2, q) - Y(u_2, q) X(u_1, q))\]

**Proof:** Verify these in the complex analytic case.

3: By (10.5.7.7) and (13.8.5.3) (15.11.5.5),

\[\Psi'(z)^2 = 4\Psi(z)^3 - g_2\Psi(z)^2 - g_3\Psi(z)\]

implies the desired equation.

\[\square\]

**Cor. (13.8.5.6) [Tate Curve].** \(E_q : y^2 + xy = x^3 + a_4(q)x + a_6(q)\) is an elliptic scheme over \(\mathbb{Z}[[q]]\), called the **Tate curve**. The discriminant of \(E_q\) is given by

\[\Delta(E_q) = \Delta(q) : q \prod_{n \geq 1} (1 - q^n)^{24} (15.11.5.10), \quad j(E_q) = j(q)(15.11.5.10).\]

**Prop. (13.8.5.7) [Tate Curve over \(\mathbb{R}\)].** Let \(E/\mathbb{R}\) be an elliptic curve, then there exists a unique \(q \in \mathbb{R}, 0 < |q| < 1\) s.t.

- \(E\) is isomorphic to \(E_q : y^2 + xy = x^3 + a_4(q)x + a_6(q)\) over \(\mathbb{R}\).

- the isomorphism composed with

\[\varphi : C^*/q^\mathbb{Z} \cong E^*_{\mathbb{R}} : u \mapsto (X(u, q), Y(u, q))\]

as in (13.8.5.9) induces an isomorphism of complex Lie groups \(\psi : C^*/q^\mathbb{Z} \to E^*_{\mathbb{C}}\) that commutes with complex conjugation. In particular, \(\psi\) induces an isomorphism of real Lie groups

\[\psi : \mathbb{R}^*/q^\mathbb{Z} \cong E^{R-an}._{\mathbb{R}}\]

**Proof:** 1: By (13.5.8.11) and (13.5.8.12), there are exactly on \(\tau \in \mathbb{C}' = \{it|t \geq 1\} \cup \{1/2 + it|t > 1/2\}\) s.t. \(j(\tau) = j(E) \in \mathbb{R}\), and

\[J = \{it|t > 0\} \cup \{1/2 + it|t > 0\}\]

corresponds to \(q \in \mathbb{R}, 0 < |q| < 1\) via \(\tau \mapsto q = e^{2\pi it}\). Also there are identifications

\[
\begin{bmatrix}
1 & -1 \\
1 & 1
\end{bmatrix} \{it|t > 1\} = \{it|t < 1\}, \quad \begin{bmatrix}
1 & -1 \\
2 & 1
\end{bmatrix} \{1/2 + it|t > 1/2\} = \{1/2 + it|t < 1/2\}, \quad \begin{bmatrix}
1 & -1 \\
1 & 1
\end{bmatrix} (i) = \frac{1 + i}{2}.
\]

thus it suffices to show that for any two \(q, q' \in J\) with \(q \neq q'\), \(E_q \not\cong E_{q'}\). It suffices to show for the twists, where we can use (13.8.6.3) to show that their \(c_4, c_6\) changed sign, so they are not isomorphic over \(\mathbb{R}\).

2: This follows from (13.8.5.9).  \(\square\)
Cor. (13.8.5.8) [Connected Components]. Let $E \in \Ell / \mathbb{R}$, then

$$E(\mathbb{R}) \cong \begin{cases} \mathbb{R}/\mathbb{Z} & \Delta(E) < 0 \\ \mathbb{R}/\mathbb{Z} \times \mathbb{Z}/(2) & \Delta(E) > 0 \end{cases}$$

as real Lie groups.

Proof: Notice $\text{sgn}(\Delta) = \text{sgn}(q)$ by (13.8.5.9). The $q > 0$ case is clear. For $q < 0$, notice there is an isogeny $E_{q^2} \to E_q$ with kernel $q$, so $E^{\mathbb{R}-\text{an}} \cong [\mathbb{R}/\mathbb{Z} \times \mathbb{Z}/(2)]/(1/2, -1) \cong \mathbb{R}/\mathbb{Z}$. □

Prop. (13.8.5.9) [over Complete Valued Fields]. Notation as in (13.8.5.1), let $K$ be a complete non-Archimedean valued field, then for $q \in K$, $0 < |q| < 1$,

- $E_q : y^2 + xy = x^3 + a_4(q)x + a_6(q) \in \Ell / K$. The discriminant of $E_q$ is given by

$$\Delta(E_q) = \Delta(q) : q \prod_{n \geq 1} (1 - q^n)^{24}(15.11.5.8), \quad j(E_q) = j(q)(15.11.5.10)$$

- $\varphi : \overline{K}^* \to E_q(\overline{K}) : u \mapsto [X(u, q), Y(u, q), 1]$

is a continuous surjective homomorphism with kernel $q \mathbb{Z}$, and it is $\text{Gal}_K$-invariant, thus for any $K \subset L \subset \overline{K}$ inducing a continuous surjective homomorphism

$$\varphi : L^* \to E_q(L)$$

with kernel $q \mathbb{Z}$.

Proof: 1: This follows from (13.8.5.6) by base change.

2: Clearly $X(u, q), Y(u, q)$ converges for any $u \in K^*/q \mathbb{Z}$, and by (13.8.5.1) it suffices to consider the case $|q| < |u| < |q|^{-1}$. In this case, the formal power series for $X(u, q), Y(u, q)$ are convergent in the complete field $K(u)$, and it follows from (13.8.5.5) that $\varphi(K^*) \in E_q$. It is clearly continuous for $u \not= 1$, and if $u$ converges to 1, $X(u, q)/Y(u, q) \to 0$ by the expansion in (13.8.5.5), so $\varphi(1) = O$.

To show $\varphi$ is a homomorphism, it suffices to verify for $1 < |u_1| < |q|^{-1}, |q| < |u_2| < 1$ that $\varphi(u_1) + \varphi(u_2) = \varphi(u_1 u_2)$. Notice by the argument above, $\varphi(u) = O$ iff $u = 1$. If $u_1 = 1$ or $u_2 = 1$, then $\varphi(u_1) + \varphi(u_2) = \varphi(u_1 u_2)$ is clear, and if $u_1 u_2 = 1$, then $\varphi(u_1) + \varphi(u_2) = O$ by the identities in (13.8.5.5) and (13.8.1.8). When $u_1 \not= 1, u_2 \not= 1, u_2 \not= 1, \varphi(u_1) \not= \varphi(u_2)$, $\varphi(u_1) + \varphi(u_2)$ are determined by polynomial equations with coordinates of $\varphi(u_1), \varphi(u_2)$, and we can show this equation holds for $\varphi(u_1 u_2)$ because it holds in the complex case (13.8.5.9). For the case $\varphi(u_1) = \varphi(u_2)$, notice that $\text{Im}(\varphi)$ is infinite, as for $|t| < 1, |X(1 + t)| = |t|^{-2}$ by the formula in (13.8.5.5). Now this case follows from (2.1.3.14).

Next, we show $\varphi : L^* \to E_q(L)$ is surjective. As $K$ is arbitrary, we may assume $L = K$. For this, Cf.[Tate, a review of non-Archimedean Elliptic Functions].

Lemma (13.8.5.10). Let $\alpha \in K$ with $|\alpha| > 1$, then there exists a unique $q \in K$ s.t. $|q| < 1$ s.t.

$$j(q) = \alpha.$$

Moreover, $q \in \mathbb{Z}[[\frac{1}{\alpha}]]$.

Proof: Let $f(q) = j(q)^{-1} \in q + q^2 \mathbb{Z}[[q]]$, thus by (7.5.1.3) there exists a $g \in q \mathbb{Z}[[q]]$ s.t. $f(g(q)) = q = g(f(q))$. So if $f(q) = \frac{1}{\alpha}$, then $q = f\left( \frac{1}{\alpha} \right)$. And this $q$ do satisfies $j(q) = \alpha$. □

Thm. (13.8.5.11) [p-Adic Uniformization, Tate]. Let $K$ be a complete valued field, $E \in \Ell / K$ with $|j(E)| > 1$, then
There exists a unique \( q \in K \) s.t. \( E_K \cong (E_q)_K \).

For this \( q \), the following are equivalent:

- \( E \cong E_q \).
- \( \gamma(E) = 1(13.8.6.3) \).
- \( E \) has split multiplicative reduction.

**Proof:** 1 follows from (13.8.5.10) and (13.8.1.13).

2: Firstly \( \gamma(E_q) = 1 \), because
\[
c_4(E_q) = 1 - 48a_4(q) = 1 + 240s_3(q), \quad -c_6(E_q) = 1 - 72a_4(q) - 864a_6(q) = 1 - 504s_5(q)
\]
are all of the form \( 1 + 4\alpha, |\alpha| < 1 \), thus they are both squares in \( K^\times \), as \( 1 + 4\alpha = [(1 + 4\alpha)^{1/2}]^2 \).

Next, \( |a_4(q)|, |a_6(q)| \leq 1 \), so \( \tilde{E}_q : y^2 + xy = x^3 \) has split multiplicative reduction. Then \( 1 \iff 2 \) by (13.8.6.3), and to show \( 1 \iff 3 \), it suffices to show that if \( E \) has split multiplicative reduction, then \( \gamma(E) = 1 \): Let the valuation ring of \( K \) be \( R \) with maximal ideal \( m \) and residue field \( k \). Let \( y^2 + a_1xy + a_3 = x^3 + a_2x^2 + a_4x + a_6 \) be a minimal polynomial. We may assume the singular point is \((0, 0) \in \tilde{E}(k)\), then \( a_3 \equiv a_4 \equiv a_6 \equiv 0 \mod m \), thus \( b_4 = a_1a_3 + 2a_4 \equiv 0 \mod m \), and \( c_4 = b_2^2 - 2b_4 \equiv b_2^2 \mod m \). Thus \( b_2 \in R^* \), and
\[
\gamma(E) = -\frac{c_4}{c_6} = \frac{1}{b_2} \frac{1 - 24b_4/b_2^2}{1 - 36b_4/b_2^2 + 216b_6/b_2^3} \mod (K^\times)^2.
\]

So by??gain, \( \gamma(E) \equiv b_2 \mod (K^\times)^2 \).

Because \( E \) has multiplicative split reduction, \( y^2 + \alpha_1 xy - \alpha_2 x^2 = (y - \alpha x)(y - \beta x) \in k \), \( \alpha \neq \beta \).

Thus by Henselian lifting, \( y^2 + a_1xy - a_2x^2 = (y - \alpha x)(y - \beta x) \in K \) for some \( \alpha, \beta \), and \( b_2 = a_1^2 + 4a_2 = (\alpha - \beta)^2 \in (K^\times)^2 \).

**Cor. (13.8.5.12).** If \( \gamma(E) \neq 1 \), let \( L = K(\sqrt{\gamma(E)}) \), then \( E_L \cong (E_q)_L \), and
\[
E(K) \cong \{ u \in L^* / \mathbb{Q} | N_{L/K}(u) \in \mathbb{Z} \}.
\]

**Proof:** Cf.[Sil99]P444.

---

## 6 Galois Cohomology

**Prop. (13.8.6.1) [Twists of Elliptic Curves].** Because the category of smooth curves with a fixed point is an algebraic stack, thus the set \( \text{Twist}(E/k) \) of twisted curves of an elliptic curve over \( k \) is in bijection with \( H^1(G_k, \text{Isom}(E_k)) \) by (5.1.5.2).

Also the category of elliptic curves over \( k \) with the origin fixed is an algebraic stack, thus the set \( \text{Twist}(E,O/k) \) of twisted elliptic curves of an elliptic curve over \( k \) is in bijection with \( H^1(G_k, \text{Aut}(E_k)) \).

**Remark (13.8.6.2).** [?]P318,342 has a direct proof, and can find the twist corresponding to a cocycle explicitly.

**Prop. (13.8.6.3) [Twist((E,O)/k)].** Let \( k \) be a field s.t. \( \text{char } k \neq 2,3 \), \( E \in \text{Ell} / k \). Denote \( n = \# \text{Aut}(E_k) \), then

- \( \text{Twist}((E,O)/k) \) is canonically isomorphic to \( K^\times / (K^\times)^n \).
For \( E/k \) with Weierstrass equation \( y^2 = x^3 + Ax + B \), the twisted elliptic curve of \( E \) corresponding to \( D \mod (K^\times)^n \) has the Weierstrass equation

\[
E_D : \begin{cases} y^2 = x^3 + D^2Ax + D^3B, & j(E) \neq 0, 1728 \\ y^2 = x^3 + DAx, & j(E) = 1728 \\ y^2 = x^3 + DB, & j(E) = 0 \end{cases}
\]

In case \( j(E) \neq 0, 1728 \), \( n = 2 \), define \( \gamma(E) = -c_4/c_6 \in K^\times/(K^\times)^2 \), which equals \( A/B \) in the short form, then for \( E, E' \in \text{Ell}/k \) with \( j(E), j(E') \neq 0, 1728 \),

\[ E \cong E' \iff j(E) = j(E') \land \gamma(E) = \gamma(E'). \]

**Proof:** This is because the Kummer sequence and (13.8.1.18) implies \( H^1(G_k, \text{Aut}(E_\bar{k})) \cong H^1(G_k, \mu_n(\bar{k})) = K^\times/(K^\times)^n \). For the corresponding elliptic curve, Cf.[Sil16]P343. □

**Def. (13.8.6.4)[Weil-Châtelet Groups].** Define the Weil-Châtelet Group \( WC(X/k) \) of an elliptic curve \( X/k \) to be the isomorphism classes of \( X \)-torsors on \( \text{Sch}_{\text{ét}}/\text{Spec} \, k \).

**Prop. (13.8.6.5)[Torsors for \( E \)].** For any \( E \)-torsor \( X \), choose a geometric point (exists by definition), then we see that \( X \) is a smooth curve of genus 1, and is a twist of \( A \).

In fact, there is an isomorphism of pointed set \( WC(E/k) \cong H^1(G_k, (E_\bar{k})) \), by[Sil16]P325.

**Prop. (13.8.6.6).** If \( C \) is an étale torsor for \( E/k \), then \( \text{Jac}(C) \cong E \).

**Proof:** Because \( C \) is a smooth curve, let \( p \in C \) be a geometric point, and take the line bundle \( \mu^*L(p) - \text{pr}_2^*L(p) - \text{pr}_1^*L(O) \), where \( \mu : E \times C \to C \) is the action. Then after a base change to \( k(p) \), this map corresponds to the canonical isomorphism \( E \cong \tilde{E} \) (13.8.1.19), thus it is also an isomorphism because \( \text{Sch}_X \) is a prestack over \( \text{Sch}_{\text{fpqc}} \). □

**Prop. (13.8.6.7).** Let \( E \in \text{Ell}/\mathbb{R} \), then

\[ WC(E/\mathbb{R}) \cong \begin{cases} 0 & \Delta(E) > 0 \\ \mathbb{Z}/(2) & \Delta(E) < 0 \end{cases} \]

**Proof:** By (13.8.6.5) and (13.8.5.7), the Galois cohomology of the exact sequence \( 1 \to q^\mathbb{Z} \to \mathbb{C}^\times \to E(\mathbb{C}) \to 1 \)

\[ 0 \to W(E/\mathbb{R}) \to H^2(\text{Gal}(\mathbb{C}/\mathbb{R}), q^\mathbb{Z}) \to H^2(\text{Gal}(\mathbb{C}/\mathbb{R}), \mathbb{C}^\times), \]

and \( H^2(\text{Gal}(\mathbb{C}/\mathbb{R}), q^\mathbb{Z}) \cong q^\mathbb{Z}/q^{2\mathbb{Z}}, H^2(\text{Gal}(\mathbb{C}/\mathbb{R}), \mathbb{C}^\times) \cong \mathbb{R}^\times/(\mathbb{R}^\times)^2 \) by (10.1.3.5)(10.1.1.20). So we are done by observing \( \text{sgn}(\Delta) = \text{sgn}(q) \) by (13.8.5.9). □

**Conj. (13.8.6.8).** The Shafarevich-Tate group is finite.

**Proof:**

**Rem. (13.8.6.9).** There is no elliptic curve \( E \) over \( \mathbb{Q} \) with \( \text{rank}_{an}(E/\mathbb{Q}) \geq 2 \) s.t. \( \text{II}(E/\mathbb{Q}) \) can be shown to be finite.
Prop. (13.8.6.10). Let $F$ be a global number field and $E$ an elliptic curve over $F$. Assume $p$ is a prime and $E$ has good ordinary reduction over all primes lying over $p$. Assume $F_{\infty} = \cup_n F_n$ is a $\mathbb{Z}_p$-extension of $F$, then the natural map
\[ \text{Sel}_E(F_n)_p \to \text{Sel}_E(F_{\infty})_{p}^{\text{Gal}(F_{\infty}/F_n)} \]
has finite kernels and cokernels of bounded orders as $n \to \infty$.

Proof: Cf. [Mazur’s Control Theorem for Elliptic Curves]. □

7 Rational Points

Conj. (13.8.7.1) [Sate-Tate]. Let $E$ be an elliptic curve over a global number field $K$, then for any place $v$, define $a_v = q_v + 1 - \#\tilde{E}_v(k_v)$, then by Weil conjecture, $|a_v| \leq 2\sqrt{q_v}$. Let $a_v/2\sqrt{q_v} = \cos \theta_v, 0 \leq \theta \leq \pi$, then if $E$ has no complex multiplication, then $\{\theta_v\}$ for places $v$ leveled by $q_v$ has distribution $\frac{2}{\pi} \sin^2 \theta$.

Remark (13.8.7.2) [Clozel-Harris-Shepherd-Barron-Taylor]. The Sate-Tate conjecture (13.8.7.1) is true for elliptic curves with non-integral $j$-invariants.

Conj. (13.8.7.3) [Birch]. For a prime $p$ and let $E_p$ be the set of isomorphism classes of elliptic curves over $F_p$. For an elliptic curve $E$ over $F_p$, define $a_v = q_v + 1 - \#\tilde{E}_v(k_v)$ and $a_v/2\sqrt{q_v} = \cos \theta_v, 0 \leq \theta \leq \pi$, then the distribution of $\{\theta_p(E)\}$ for $E \in E_p$ tends to $\frac{2}{\pi} \sin^2 \theta$ for $p \to \infty$.

Proof: □

Ranks

Conj. (13.8.7.4) [Unboundedness Conjecture]. Let $F$ be a global field, the rank of elliptic curves over $F$ can take arbitrary large values.

Proof: □

Remark (13.8.7.5). For function fields, this is proven by Tate-Shafarevich.

Prop. (13.8.7.6) [Lang Conjecture]. For any $\varepsilon > 0$, there exists a constant $C_\varepsilon > 0$ s.t. for any elliptic curve $E$ over $\mathbb{Q}$, there exists a basis $\{P_1, \ldots, P_r\}$ of the free part of $E(\mathbb{Q})$ satisfying
\[ \max_{1 \leq i \leq r} \hat{h}(P_i) \leq C_\varepsilon |D_{E/\mathbb{Q}}|^{\frac{1}{12} + \varepsilon}. \]

where $D_{E/\mathbb{Q}}$ is the minimal discriminant of $E/\mathbb{Q}$ and $\hat{h}$ is the canonical height.

Conj. (13.8.7.7) [Rank Distribution]. The distribution of elliptic curves ordered by height(13.8.4.22) satisfies
\[ P_{\text{rank}}(r) = \begin{cases} 50\% & r = 0 \\ 50\% & r = 1 \\ 0 & r \geq 2 \end{cases}. \]

In particular, $\text{E}(r) = 0.5$

Prop. (13.8.7.8) [Bhargava-Shankar]. $\text{E}(r) \leq 0.99$, if it exists.

Proof: □
Integral Points

Thm. (13.8.7.9) [Siegel]. Let $E/K$ be an elliptic curve with $\#E(K) = \infty$. Let $v$ be an absolute valuation of $K$, $Q \in E(K)$ and $f \in R(E)\times$ which corresponds to a morphism $\varphi : E \rightarrow \mathbb{P}^1 : P \mapsto [1, f(P)]$, then

$$\lim_{P \in E(K), h(\varphi(P)) \rightarrow \infty} \frac{\log d_v(P; Q)}{h(\varphi(P))} = 0. (13.2.4.27)$$


Cor. (13.8.7.10) [Finiteness of Integral Points]. If $C/K$ is a complete smooth curve of genus 1 and $f \in R(C)^\times$, $S \subset \Sigma_K$ a finite set, then $\{P \in C(K) | f(P) \in \mathcal{O}_{K,S}\}$ is a finite set.

Proof: By a finite base change of fields, we may assume $\varphi^{-1}(\infty)$ contains a rational point $O$, and this point makes $C$ into an elliptic curve. Let $\varphi : E \rightarrow \mathbb{P}^1 : P \mapsto [1, f(P)]$. It follows from the definition that there is some $v \in S$ s.t.

$$h(\varphi(P)) \leq \#S \log |f(P)|_v$$

for any $P \in C(K)$ s.t. $f(P) \in \mathcal{O}_{K,S}$. Then if $\# \{P \in C(K) | f(P) \in \mathcal{O}_{K,S}\} = \{P_1, \ldots, P_n, \ldots\}$ is infinite, it follows from Northcott’s theorem (13.2.4.7) that $h(\varphi(P_i)) \rightarrow \infty$, and $|f(P_i)|_v \rightarrow \infty$ for a specific $v \in S$. Suppose $e_{\mathcal{O}(\varphi)} = e$, then

\[ \square \]

8 Twists of Elliptic Curves

See Chao Li’s Work and Ye Tian’s Work.

Congruence Number Problem

References are [A classical Diophantine problem and modular forms of weight 3/2, Tunnell], [Explicit application of Waldspurger’s theorem].

9 Elliptic Surfaces
13.9 Complex Multiplication Theory

Main references are [Mil20b], [Lang, Complex Multiplication] and [The Fundamental Theorem of Complex Multiplication, Milne, 2007].

Notations (13.9.0.1).
- Use notations defined in Arithmetic of Abelian Varieties.

1 Introduction

Abelian varieties with complex multiplication correspond to special points on the moduli variety of abelian varieties, and their arithmetic is intimately related to that of the values of modular functions and modular forms at those points.

2 CM-Algebras and CM-Types

Def. (13.9.2.1) [CM-Fields]. A CM-field is a number field that is a totally imaginary quadratic extension of a totally real field.

Prop. (13.9.2.2) [Characterizing CM-Fields]. For \( E \in \mathbb{NField} \), then \( E \) is a CM-field or totally real iff there exists exactly one \( e_E \in \text{Aut}(E) \) s.t. for any \( \rho \in \text{Hom}(E, \mathbb{C}) \), \( \rho \circ e_E = e \circ \rho \). And it is CM iff \( e_E \neq \text{id}_E \).

Proof: If \( \rho \circ e_E = e \circ \rho \) for any \( \rho \in \text{Hom}(E, \mathbb{C}) \), then \( \rho \circ e_E^2 = \rho \), so \( e_E^2 = \text{id} \). If \( F \) is the fixed field of \( e_E \), then \( [E : F] = 2 \), and clearly \( F \) is totally real. Conversely, if \( E \) is a CM-field or totally real, then clearly there exists a unique such \( e_E \), which is the identity if \( E \) is totally real and the unique involution fixing the totally real subfield \( F \).

In this case, if \( e_E \neq \text{id}_E \), then \( \rho(E) \subset \mathbb{R} \) for any \( \rho \in \text{Hom}(E, \mathbb{C}) \), thus \( E \) is totally imaginary. And if \( e_E = \text{id}_E \), then \( E \) is also totally real. \( \Box \)

Cor. (13.9.2.3). A finite composite of CM-fields is a CM-field. In particular, the Galois closure of a CM-field is a CM-field.

And the composite of all CM-fields in \( \mathbb{C} \) are the field \( \mathbb{Q}^{cm} \subset \overline{\mathbb{Q}} \) corresponding to the subgroup of \( \text{Gal}_{\mathbb{Q}} \) generated by all the elements \( \{[\sigma, e] | \sigma \in \text{Gal}_{\mathbb{Q}} \} \), which is a normal subgroup.

Proof: The complex involutions on these CM-fields is compatible on their intersections, thus defines a complex involution on their composite. \( \Box \)

Cor. (13.9.2.4). Any CM-field \( E \) is of the form \( E = F(\alpha) \), where \( F \) is totally real, \( \alpha^2 \in F \), and \( \rho(\alpha^2) \in \mathbb{R}_- \) for any homomorphism \( \rho : F \rightarrow \mathbb{C} \).

Proof: If \( F \) is the totally real field contained in \( E \) and \( \alpha \in E \) generates \( E \) over \( F \), then by completing the square, we can assume \( \alpha^2 \in F \). Then \( \rho(\alpha^2) \in \mathbb{R}_- \) for any \( \rho : F \rightarrow \mathbb{C} \), otherwise \( E \) is not totally imaginary. \( \Box \)

Def. (13.9.2.5) [CM-Algebras]. A CM-algebra is a finite product of CM-fields.

Def. (13.9.2.6) [CM-Types]. A CM-type for a CM-algebra \( E \) is a subset \( \Phi \subset \text{Hom}(E, \mathbb{C}) \) s.t. \( \text{Hom}(E, \mathbb{C}) = \bigoplus \Phi^e \).

A pair \( (E, \Phi) \) where \( E \) is a CM-algebra and \( \Phi \) is a CM-type on \( E \) is called a CM-pair.

More generally, if \( E \) is an étale algebra over \( \mathbb{Q} \), then a CM-type on \( E \) is a subset \( \Phi \subset \text{Hom}(E, \mathbb{C}) \) s.t. \( \text{Hom}(E, \mathbb{C}) = \sigma \Phi \bigoplus e \circ \sigma \Phi \) for any \( \sigma \in \text{Gal}_{\mathbb{Q}} \).
Prop. (13.9.2.7). Let $E$ be an étale algebra over $\mathbb{Q}$ and $F$ the product of the largest totally real subfields of the factors of $E$, then choosing a CM-type is equivalent to choosing an extension $\rho'$ to $E$ of any homomorphism $\rho : F \to \mathbb{R}$. Thus a CM-pair $(E, \Phi)$ defines an isomorphism

$$E \otimes_{\mathbb{Q}} \mathbb{R} \xrightarrow{\Phi} \prod_{\rho : F \to \mathbb{R}} \mathbb{C} \cong \mathbb{C}^\Phi : a \otimes r \mapsto (\rho'(a)r)_{\rho}, \quad \Phi = \{\rho'|\rho : F \to \mathbb{R}\}$$

Def. (13.9.2.8) [Primitive CM-Fields]. If $E_0$ is a CM-field and $E/E_0$ is a finite extension, then a CM-type $\Phi_0$ on $E_0$ extends to a CM-type on $E$ (13.9.2.6) by defining

$$\Phi = \{\varphi \in \text{Hom}(E, \mathbb{C})|\varphi|_{E_0} \in \Phi_0\}.$$ 

A primitive CM-field is a CM-pair (13.9.2.6) $(E, \Phi)$ where $E \in \text{Field}$ and there doesn’t exist a proper subfield $E_0 \subset E$ s.t. $\Phi$ is the extension of a CM-type on $E_0$.

Prop. (13.9.2.9). Every CM-pair $(E, \Phi)$ where $E$ is a field is an extension of a unique primitive CM-pair $(E_0, \Phi_0)$ s.t. $E_0 \subset E$. Moreover, for any Galois CM-field $E_1$ containing $E$, $E$ is the fixed field of $E$ defined by the subgroup

$$H = \{\sigma \in \text{Gal}(E_1/\mathbb{Q}) : \Phi_1^\sigma = \Phi_1\},$$

where $\Phi_1$ is the extension of $\Phi$ to $E_1$.

Proof: If $E$ is Galois over $\mathbb{Q}$, and $E_0$ is defined as above, then $\Phi e_E = e \Phi \neq \Phi$, so $e_E \notin H$, thus $e_E$ acts non-trivially on $E_0$. And $e_E$ preserves $E_0$. We need to show that $e_E a = e_E a$ for any $a \in E_0$. For which it suffices to show that $e_E \sigma e_E \in H$. For this, notice

$$\Phi e_E \sigma e_E = e \Phi \sigma e_E = e \Phi e_E = \Phi.$$ 

Thus $E_0$ is CM-subfield of $E$. And $\Phi_0 = \Phi|_{E_0}$ is a CM-type on $E_0$, because if $\varphi'|_{E_0} = e \varphi|_{E_0}$ for different $\varphi, \varphi' \in \Phi$, then $e \varphi \in \varphi'H \subset \Phi$, contradiction.

And if $E_0$ is extended from another CM-subfield $E'$, then any $\sigma \in \text{Gal}(E/\mathbb{Q})$ fixing $E'$ will fix $\Phi$ and lies in $H$. This shows $E_0 \subset E'$. So $(E_0, \Phi_0)$ is primitive.

For the general case, it suffices to notice that this $E_0$ is contained in $E$ because any $\sigma \in \text{Gal}(E_1/\mathbb{Q})$ fixing $E$ will fix $\Phi_1$ thus fixes $E_0$ by definition. And $\Phi$ clearly extends $\Phi_0$. \qed

Cor. (13.9.2.10). A CM-pair $(E, \Phi)$ where $E$ is a field is primitive iff there exists a Galois CM-field $E_1$ containing $E$ s.t. $E$ is the fixed field of $E$ defined by the subgroup

$$H = \{\sigma \in \text{Gal}(E_1/\mathbb{Q}) : \Phi_1^\sigma = \Phi_1\},$$

where $\Phi_1$ is the extension of $\Phi$ to $E_1$.

Prop. (13.9.2.11) [Shimura-Taniyama]. Let $E$ be a CM-field, $F = E^e$ (13.9.2.2) and $E = F(\alpha)$ where $\alpha^2 \in F$ is totally negative. Then

$$\Phi = \{\varphi \in \text{Hom}(E, \mathbb{C}) : \text{Im}(\varphi(\alpha)) > 0\}$$

is a CM-type on $E$. And $(E, \Phi)$ is a primitive CM-pair iff

- $E = \mathbb{Q}(\alpha)$. 

• \( \sigma(\alpha)/\alpha \) is not totally positive for any \( \sigma \in \text{Gal}(E/Q) \).

**Proof:** \( \Phi \) is a CM-type on \( E \) because for any \( \varphi \in \Phi, \varphi e_E \notin \Phi \) because \( \text{Im}(\varphi e_E(\alpha)) = -\text{Im}(\varphi(\alpha)) < 0 \).

Let \( F_1 \) be the Galois closure of \( F \) and \( E_1 = F_1(\alpha) \), and \( \Phi_1 \) is the extension of \( \Phi \) to \( E_1 \), then
\[
\Phi_1 = \{ \varphi \in \text{Hom}(E_1, C) : \text{Im}(\varphi(\alpha)) > 0 \}.
\]

and if
\[
H = \{ \sigma \in \text{Gal}(E_1/Q) : \Phi_1^\sigma = \Phi_1 \},
\]
then \( H \) is exactly the group of \( \sigma \in \text{Gal}(E_1/Q) \) s.t. \( \sigma(\alpha)/\alpha \in \mathbb{R}_+ \). Then the assertion follows from (13.9.2.10).

**Reflex Fields**

**Def. (13.9.2.12) [Reflex Fields of CM Pairs].** Let \( (E, \Phi) \) be a CM-pair, then the **reflex field** \( E^* \) of \( (E, \Phi) \) is the subfield of \( \overline{Q} \) generated by the elements \( \{ \sum_{\varphi \in \Phi} \varphi(a) | a \in E \} \).

**Prop. (13.9.2.13).** Let \( (E, \Phi) \) be a CM-pair with reflex field \( E^* \), then
- \( E^* \) is the fixed field of the group \( \{ \sigma \in \text{Gal}_Q | \sigma(\Phi) = \Phi \} \).
- \( E^* \) is a CM-field.
- If \( (E_1, \Phi_1) \) is an extension of \( (E, \Phi) \) (13.9.2.8), then the reflex field of \( (E_1, \Phi_1) \) is just \( E^* \).

**Proof:**
1: This group is clearly in the fixed group of \( E^* \), and if \( \sigma \) is in the fixed group of \( E^* \), then
\[
\sum_{\varphi \in \Phi} \varphi(a) = \sum_{\varphi \in \Phi} \sigma \varphi(a),
\]
so \( \sigma(\Phi) = \Phi \) by the linear independence of characters.
2: For \( \sigma \in \text{Gal}_Q \) and \( a \in E \),
\[
e \sigma(\sum_{\varphi \in \Phi} \varphi(a)) = e \sum_{\varphi \in \Phi} \sigma \varphi(a) = \sum_{\varphi \in \Phi} \sigma \varphi(e_E(a)) = \sum_{\varphi \in \Phi} \varphi(e_E(a)) = e \sum_{\varphi \in \Phi} \varphi(a).
\]
Thus \( E \) is a CM-field or totally real by (13.9.2.2). The latter case is not possible because of the linear independence of characters and the fact \( e(\Phi) \neq \Phi \).
3 is trivial.

**Def. (13.9.2.14) [Reflex CM-Pairs].** Let \( (E, \Phi) \) be a CM-pair that \( E \) is contained in \( \overline{Q} \), let \( E_1 \) be the Galois closure of \( E \), and \( \Phi_1 \) the extension of \( \Phi \) to \( E_1 \). Then \( (E_1, \Phi_1^{-1}) \) is also a CM-pair. Then the primitive subfield \( (E^*, \Phi^*) \) satisfies \( E^* \) is the reflex field of \( (E, \Phi) \).

\( (E^*, \Phi^*) \) is called the **reflex CM-pair** of \( (E, \Phi) \).

**Classification of Primitive CM-Pairs**

**Prop. (13.9.2.15).** Milne, Prop1.30.

**Cor. (13.9.2.16).** Milne, Prop1.31.
Positive Involutions

Def. (13.9.2.17) [Positive Involutions]. Let $B$ be a f.d. $\mathbb{Q}$-algebra, and $\text{tr} : B \to \mathbb{Q}$ is a $\mathbb{Q}$-linear functional, then a **positive involution** w.r.t. $\text{tr}$ is an involution $\iota$ on $B$ s.t.

$$\text{tr}(x) = \text{tr}(\iota(x)), \quad \text{tr}(x \cdot \iota(x)) > 0$$

for any nonzero $x \in B$.

Prop. (13.9.2.18)[Positive Involutions are Semisimple]. If $B$ is a f.d. $\mathbb{Q}$-algebra with a positive involution $\iota$, then $B$ is semisimple. And if $Z$ is the center of $B$, then $Z = \prod_i K_i$ where $K_i \in \text{NF}ield$, and each $K_i$ is stable under $\iota$.

Proof: By (2.4.2.8), it suffices to show that $B$ is Jacobson semisimple: If $a$ is a nonzero nilpotent two-sided ideal of $B$, $a \neq 0 \in a$ is nilpotent, then $b = a\iota(a) \neq 0$ because $\text{tr}(a\iota(a)) > 0$. Thus $b \neq 0 \in a$, and $\iota(b) = b$. So by the same reason $b^2 \neq 0$, and so on, so $b$ is not nilpotent, contradicting (2.4.2.6).

The center is clearly invariant under the isomorphism given, so it is also semisimple, which is then a product of fields. To show each factor is stable under $\iota$, notice that if $1 = \sum_i e_i$ is a decomposition w.r.t. this product, then $1 = \sum_i \iota(e_i)$, so $\{\iota(e_i)\} = \{e_i\}$. Moreover, $\iota(e_i) = e_i$ for each $i$, because otherwise $e_i\iota(e_i) = 0$, and $\text{tr}(e_i\iota(e_i)) = 0$. □

Prop. (13.9.2.19). Let $B$ be a f.d. $\mathbb{Q}$-algebra an $\iota$ an involution on $B$, then the following are equivalent:

- There is a faithful $B$-module $V$ with a positive definite symmetric $\mathbb{Q}$-bilinear form $(-, -) : V \times V \to \mathbb{Q}$ s.t.
  $$\langle bu, v \rangle = \langle u, \iota(b)v \rangle, \quad b \in B, u, v \in V.$$
- For any f.d. $B$-module $V$, there exists a positive definite symmetric $\mathbb{Q}$-bilinear form $(-, -) : V \times V \to \mathbb{Q}$ s.t.
  $$\langle bu, v \rangle = \langle u, \iota(b)v \rangle, \quad b \in B, u, v \in V.$$
- There exists a $\mathbb{Q}$-linear functional $\text{tr}$ on $B$ s.t. $\iota$ is positive w.r.t. $\text{tr}$.

Proof: 1 $\to$ 2: As $B$ is semisimple, any f.d. $B$-module is a direct summand of a direct sum of the faithful module $V$.

2 $\to$ 3: Apply item2 to the $B$-module $B$ itself, then we find a positive definite symmetric $\mathbb{Q}$-bilinear form $(-, -)$ on $B$, and an orthonormal basis $(e_1, \ldots, e_n)$ of $B$. Then we define

$$\text{tr} : B \to \mathbb{Q} : \text{tr}(b) = \sum_i \langle bb_i, b_i \rangle$$

then $\text{tr}(b) = \text{tr}(\iota(b))$, and

$$\text{tr}(b\iota(b)) = \sum_i \langle b\iota(b)b_i, b_i \rangle = \sum_i \langle \iota(b)b_i, \iota(b)b_i \rangle > 0.$$

3 $\to$ 1: $B$ is semisimple by (13.9.2.18), and then we can take $V = B$, and the positive definite symmetric $\mathbb{Q}$-bilinear form

$$\langle x, y \rangle \mapsto \text{tr}(\iota(y)x).$$

then $\langle bx, y \rangle = \text{tr}(\iota(y)bx) = \text{tr}(\iota(b)y) = \langle (x, \iota(b)y)\rangle$. □
**Prop. (13.9.2.20)** [Commutative Positive Involutions]. Every f.d. commutative Q-algebra with a positive involution \( \iota \) is a product of the following two:

- \( F \) is a totally real field and \( \iota = \text{id}_F \).
- \( E \) is a CM-field and \( \iota = e_E \).

**Proof:** Firstly, any product of these two are positive involutions. Conversely, if \((B, \text{tr})\) is a f.d. Q-algebra with a positive involution, then by (13.9.2.18), \( B \) is semisimple, thus a finite product of number fields. Then by (13.9.2.18), each factor is fixed by the involution, so it suffices to consider the case \( B \in \text{NField} \). Let \( F \) be the fixed field of \( \iota \). Because the trace form \( \text{tr}_{B/Q} \) is non-degenerate, we can assume \( \text{tr}(x) = \text{tr}(ax) \) for some \( a \in B^\times \).

If \( F = B \), then \( F \) is totally real: if there exists a non-real embedding \( \sigma : F \to \mathbb{C} \), then we can use weak approximation to find \( x \in F^\times \) s.t. \( \sigma(ax^2) \) is near \(-1\) and \( \varphi(ax^2) \) is near \( 0 \) for any other embedding \( \varphi : F \to \mathbb{C} \). Then clearly \( \text{tr}(ax^2) < 0 \), contradiction.

If \( F \neq B \), then \( |B : F| = 2 \), and \( \text{tr}_{B/Q}(ax\iota(x)) > 0 \) for any \( x \in B^\times \). Take \( x = 1 \), we see \( \text{tr}_{B/Q}(a) > 0 \). In particular, \( a + \iota(a) \neq 0 \in F \). Then in particular, \( \text{tr}_{B/Q}(ax\iota(x)) = \text{tr}_{F/Q}((a + \iota(a))x\iota(x)) > 0 \). So by the argument above, \( F \) is totally real. And \( B \) is totally imaginary: if there exists a real embedding \( \sigma : B \to \mathbb{C} \), then \( \sigma \) and \( \iota \sigma \iota \) corresponds to different places, and by weak approximation, we can find \( x \in B^\times \) s.t. \( \sigma((a + \iota(a))x) \) is near \(-1\) and \( \sigma(\iota(x)) \) is near \( 1 \), and \( \varphi(x) \) is near \( 0 \) for any other \( \varphi : B \to \mathbb{C} \). Then \( \text{tr}_{F/Q}((a + \iota(a))x\iota(x)) < 0 \), contradiction. So in this case \( B \) is a CM-field, and \( \iota = e_B \).

**Cor. (13.9.2.21).** There exists uniquely a positive involution on any CM-algebra, which is \( e_E \).

**Weil q-Integers**

**Def. (13.9.2.22)** [Weil \( q \)-Integers]. For \( q \in \mathbb{Z}_+ \), a **Weil \( q \)-integer** is an algebraic integer \( \pi \) s.t. for any embedding \( \rho : \mathbb{Q}(\pi) \to \mathbb{C} \), \( |ho(\pi)| = q^{1/2} \).

**Prop. (13.9.2.23)** [Weil \( q \)-Integers and CM Fields]. If \( p \in \mathbb{P}, q \in p^\mathbb{Z} \) and \( \pi \) is a Weil \( q \)-integer, then \( \mathbb{Q}(\pi) \) is either isomorphic to \( \mathbb{Q} \) or \( \mathbb{Q}(\sqrt{q}) \) or a CM-field.

**Proof:** For any embedding \( \rho : \mathbb{Q}(\pi) \to \mathbb{C} \),

\[
\rho(\pi)\rho(\pi) = q = \rho(\pi)\rho(q/\pi),
\]

so \( \tilde{\rho}(\rho(\pi)) = \rho(q/\pi) \), and \( E = \mathbb{Q}(\pi) \) is a CM-field with the endomorphism \( e_E : \pi \mapsto q/\pi \).

**Prop. (13.9.2.24).** Let \( p \in \mathbb{P}, q \in p^\mathbb{Z} \), \( E \in \text{NField} \) and \( \pi, \pi' \in E \) be Weil \( q \)-integers. If \( \text{ord}_v(\pi) = \text{ord}_v(\pi') \) for any \( v \in S(p) \), then \( \pi / \pi' \) is a roots of unity in \( E \).

**Proof:** This is because there is an endomorphism of \( E \) taking \( \pi \) to \( q/\pi \), so for any \( v \notin S(p) \), \( \text{ord}_v(\pi) = 0 \). Since the same is true for \( \pi' \), and \( \text{ord}_v(\pi) = \text{ord}_v(\pi') \) for \( v \in \Sigma_E^\infty \) too, by the definition of Weil \( q \)-integers. Thus \( |\pi / \pi'|_v = 1 \) for any \( v \in \Sigma_E \), and the assertion follows from (12.2.5.31).

**3 Complex CM Abelian Varieties**

**Def. (13.9.3.1)** [Complex Multiplications]. For \( A \in \text{AbVar}/\mathbb{C} \),

\[
[\text{End}_\mathbb{Q}(A) : \mathbb{Q}]_{\text{red}} \leq 2 \dim A.
\]

And \( A \) is called an Abelian variety with **complex multiplication** or a CM Abelian variety if the equality holds.
Proof: $\text{End}_\mathbb{Q}(A)$ acts faithfully on $H_1(A, \mathbb{Q})$, which has dimension $2\dim A$ by (11.8.5.4), so we finish by (13.5.6.11) and (2.4.3.23). □

Prop. (13.9.3.2). For $A \in \text{AbVar} / \mathbb{C}$, the following are equivalent:
- $A$ is CM.
- $\text{End}_\mathbb{Q}(A)$ contains an étale subalgebra of degree $2\dim A$ over $\mathbb{Q}$.
- For any Weil cohomology $H^*$ with coefficients in $\Omega \in \text{Field}$, the centralizer of $\text{End}_\mathbb{Q}(A)$ in $\text{End}_\Omega(H^1(A))$ is commutative (and equals $Z(\text{End}_\mathbb{Q}(A)) \otimes_\mathbb{Q} \Omega$).

Proof: $1 \iff 2$ follows from the fact the maximal étale subalgebra of $\text{End}_\mathbb{Q}(A)$ has degree $\left| \text{End}_\mathbb{Q}(A) : \mathbb{Q} \right|_{\text{red}}$ (2.4.3.22).

$2 \iff 3$ follows by noticing $\dim_\Omega(H_1(A)) = 2\dim A$, and $\text{End}_\mathbb{Q}(A)$ acts faithfully on it. Then use (2.4.3.23). □

Lemma (13.9.3.3). Let $A \in \text{AbVar} / \mathbb{C}$ and $F \subset \text{End}_\mathbb{Q}(A)$. If $F$ has a real place, then $[F : \mathbb{Q}] \left| \dim A\right.$.

Proof: ? □

Prop. (13.9.3.4). Let $A \in \text{AbVar} / \mathbb{C}$, then
- if $A$ is simple, then $A$ is CM iff $\text{End}_\mathbb{Q}(A)$ is a CM-field of degree $2\dim A$ over $\mathbb{Q}$.
- If $A$ is isotopic, then $A$ is CM if $\text{End}_\mathbb{Q}(A)$ contains a CM-field of degree $2\dim A$ over $\mathbb{Q}$, which is invariant under some Rosati involution.
- $A$ is CM iff $\text{End}_\mathbb{Q}(A)$ contains an étale CM-algebra of degree $2\dim A$ over $\mathbb{Q}$, which is invariant under some Rosati involution. And in this case, $H_1(A, \mathbb{Q})$ is free of rank 1 over this algebra.

Proof: We use (13.9.3.2).

1: It suffices to show that if $\text{End}_\mathbb{Q}(A)$ is a field of degree $2\dim A$, then it is CM.?

2: ?

3 follows from 2. □

Prop. (13.9.3.5) [CM-Types of Abelian Varieties]. Let $E$ be a CM-algebra of degree $2g$, $A \in \text{AbVar}^g / \mathbb{C}$ and $E \subset \text{End}_\mathbb{Q}(A)$, then the action of $E$ on $\text{Tgt}_0(A)$ is faithful, so

$$\text{Tgt}_0(A) \cong \bigoplus_{\varphi \in \Phi} C_\varphi$$

where $\Phi$ is a set of homomorphisms from $E$ to $\mathbb{C}$. Then from the decomposition

$$H_1(A, \mathbb{R}) \cong \text{Tgt}_0(A) \oplus \overline{\text{Tgt}_0(A)}$$

and the fact $H_1(A, \mathbb{Q})$ is a free $E$-module of rank 1 (13.9.3.4), we see $\Phi \bigoplus \Phi = \text{Hom}(E, \mathbb{C})$. So $\Phi$ is a CM-type on $E$.

Thus $A$ is said to have **CM-type** $(E, \Phi)$ if $\Phi$ is a CM-type on $E$ and

$$\text{Tgt}_0(A) \cong C^\Phi$$

as $E$-algebras.
Def. (13.9.3.6) [Reflex Field of a CM Abelian Variety]. Let \( A \in \text{AbVar}_/\mathbb{C} \) be CM, then if \( E_0 \) is the center of \( \text{End}_\mathbb{Q}(A) \), by (13.9.3.4) and (13.9.3.5), \( E_0 \) is a CM-algebra, and there exists a CM-type \( \Phi_0 \) on \( E_0 \) s.t. for any CM-pair \( E \) s.t. \( A \) is of CM-type \( (E, \Phi) \), there \( \Phi \) is the extension of \( \Phi_0 \) to \( E \).

Then the reflex field of \( (E, \Phi) \) equals that of \( (E, \Phi_0) \) for any \( (E, \Phi) \), called the **reflex field** of \( A \).

Prop. (13.9.3.7) [Abelian Varieties attached to CM-Pairs]. Let \( (E, \Phi) \) be a CM-pair and \( \Lambda \) is a \( \mathbb{Z} \)-lattice in \( E \), then

\[
\Lambda \otimes \mathbb{Z} \mathbb{R} \cong E \otimes \mathbb{Q} \mathbb{R} \overset{\Phi}{\cong} \mathbb{C}^\phi(13.9.2.7).
\]

Thus \( \Lambda \otimes \mathbb{Z} \mathbb{R} \) has a complex structure and we get a Riemann pair \( (\Lambda, J_\phi) \), which corresponds to a complex torus \( A_\Phi \).

Then \( R = \{ x \in E | a\Lambda \subset \Lambda \} \subset \text{End}(A_\Phi) \) is an order in \( E(4.2.7.40) \), and then \( E \subset \text{End}_\mathbb{Q}(A_\Phi) \).

Then there is a Riemann form on \( (\Lambda, J_\phi) \) whose associated positive Rosati involution (13.5.8.2) stabilizes \( E \) (and thus equals \( e_E \) on \( E \) by (13.9.2.21)). In particular, \( A_\Phi \) is a complex Abelian variety (13.5.8.1).

**Proof:** To give such a Riemann form, by (11.8.5.9), it suffices to give a non-degenerate bilinear form \( \psi : E \times E \to \mathbb{Q} \) that satisfies

1. \( \psi(ax, y) = \psi(x, \bar{y}a) \) for \( a, x, y \in E \).
2. \( \psi(x, y) = -\psi(y, x) \) for \( x, y \in E \).
3. \( \psi(J_\phi x, J_\phi y) = \psi(x, y) \) for \( x, y \in E \otimes \mathbb{Q} \mathbb{R} \).
4. \( \psi(x, J_\phi x) > 0 \) for any non-zero \( x \in E \otimes \mathbb{Q} \mathbb{R} \).

Now because the trace form \( \text{tr} : E \times E \to \mathbb{Q} \) is non-degenerate, non-degenerate \( \mathbb{Q} \)-bilinear forms of \( E \) are exactly of the form

\[
\psi(x, y) = \text{tr}_{E/\mathbb{Q}}(\bar{y}x), \quad \alpha \in E^\times.
\]

And the conditions (1) is automatic, and (3) is automatic because in the isomorphism

\[
E \otimes \mathbb{Q} \mathbb{R} \overset{\Phi}{\cong} \prod_{\rho : F \to \mathbb{R}} \mathbb{C} \cong \mathbb{C}^\phi : a \otimes r \mapsto (\rho'(a)r)_\rho, \quad \Phi = \{ \rho' | \rho : F \to \mathbb{R} \}, (13.9.2.7)
\]

\( \psi_\mathbb{R} \) corresponds to

\[
\psi'( ((x_\varphi), (y_\varphi)) = \sum_{\varphi \in \Phi} \text{tr}_{C/F}(\varphi(a)\bar{x}_\varphi \varphi)
\]

and \( J_\phi \) corresponds to the isomorphism

\[
(x_\varphi)_{\varphi \in \Phi} \mapsto (i x_\varphi)_{\varphi \in \Phi}.
\]

Thus it suffices to choose \( \alpha \) s.t. \( \varphi(\alpha) \in i \mathbb{R}_+ \) for any \( \varphi \in \Phi \).

By (13.9.2.4), there exists \( \alpha \in E^\times \) s.t. \( E = F(\alpha) \) s.t. \( \varphi(\alpha) \in i \mathbb{R} \) for any \( \varphi \in \Phi \), and we can then use weak approximation on \( F \) to modify \( \alpha \) s.t. \( \varphi(\alpha) \in i \mathbb{R}_+ \) for any \( \varphi \in \Phi \). So this \( \alpha \) clearly exists. Moreover, any other element \( \alpha' \) is \( \alpha \) times some element \( a \in F \) that is totally positive. \( \square \)
Classifications of Complex CM Abelian Varieties

Prop. (13.9.3.8) [Classifications up to Conjugacy]. The map \((A, i) \mapsto (E, \Phi)\) defines a bijection between the set of isogeny classes of CM Abelian varieties \(A\) with an embedding \(i : E \to \text{End}_Q(A)\) and the set of isomorphism classes of CM-pairs \((E, \Phi)\), with inverse \((E, \Phi) \mapsto (A_{\Phi}, i_{\Phi})\) which is the Abelian variety corresponding to the lattice \(\Lambda = \mathcal{O}_E(13.9.3.7)\), called the principally-CM Abelian variety of type \((E, \Phi)\).

Proof: Notice in (13.9.3.7), any two choice of the lattice \(\alpha\) give isogenous Abelian varieties, and because \(H_1(A, \mathbb{Q})\) is free of rank 1 over \(E\), let \(e \in H_1(A, \mathbb{Q})\) be a basis vector, then \(a \cdot e = H_1(A, \mathbb{Z})\) for some lattice \(a \subset E\). Then this \(e\) defines an isomorphism \(E \cong H_1(A, \mathbb{Z}) \otimes \mathbb{Q} = H_1(A, \mathbb{Q})\)

thus the isomorphism

\[ A \cong H_1(A, \mathbb{C}) / H_1(A, \mathbb{Z}) \xrightarrow{\cong} E \otimes \mathbb{Q} C / \alpha \xrightarrow{\Phi} C^\Phi / \Phi(\alpha) \sim C^\Phi / \Phi(\mathcal{O}_E). \]

This is clearly a bijection. □

Prop. (13.9.3.9). Let \(A\) be a simple complex Abelian variety with CM and \(E = \text{End}_Q(A)\), then \(E\) is a CM-field, and the map \(A \mapsto (E, \Phi_A)\) defines a bijection between the set of isomorphism classes of simple complex Abelian varieties with CM and the set of isomorphism classes of primitive CM-paris.

Proof: \(E \in \text{Field}\) by (13.9.3.4), and if it is not primitive, then \((E, \Phi)\) is extended from a primitive CM-field \((E_0, \Phi_0)\), and a choice of \(E_0\)-basis of \(E\) defines an embedding \(E \subset \text{Mat}(\left[ E : E_0 \right], E_0) \subset \text{End}_0(A_{\Phi_0}^{[E:E_0]}),\) and

\[ E \otimes \mathbb{R} = E \otimes_{E_0} (E_0 \otimes \mathbb{R}) \cong E \otimes_{E_0} (C^{\Phi_0}) \cong C^\Phi \]

shows \(A_{\Phi_0}^{[E:E_0]}\) is also of type \((E, \Phi)\). Thus \(A \sim A_{\Phi_0}^{[E:E_0]}\) by (13.9.3.8), contradicting the fact \(A\) is simple. □

Cor. (13.9.3.10). The simple Abelian varieties with complex multiplications are classified up to conjugacy by the \(\text{Gal}_\mathbb{Q}\)-orbits of CM-types on \(\mathbb{Q}^\text{cm}\), by (13.9.2.16).

4 CM Abelian Varieties

Good Reductions

Prop. (13.9.4.1) [Potential Good Reduction of CM-Abelian Varieties]. Let \(E \in \mathbb{N}\text{Field}, A \in \text{AbVar}/\mathbb{C}\) has complex multiplication by \(E\), then \(A\) is defined over some number field \(F\). And \(F\) can be chosen s.t. \(A_F\) has good reduction.

Proof: Cf. [Milne, Abelian Varieties, P55]. □

5 Mumford-Tate Groups

6 Fundamental Theorem

Thm. (13.9.6.1) [Fundamental Theorem of Complex Multiplication, Shimura-Taniyama]. Let \(A \in \text{AbVar}/\mathbb{F}_q\) be the reduction from an complex Abelian variety of CM-type \((E, \Phi)\), then the Weil-\(q\)-integers of \(A\) can be constructed as follows:

Proof: Cf. [Milne, Abelian Varieties, P83]. □
CHAPTER 13. ARITHMETIC GEOMETRY

7 Elliptic Curve Case

Prop.(13.9.7.1)[Serre]. Let $F \in \text{NField}$ and $E/K$ be an elliptic curve without complex multiplication, then for a.e. $\ell \in \mathbb{P}$, $E[\ell]$ has no non-trivial $\text{Gal}_K$-invariant subgroups.

Proof: If $E[\ell]$ has a non-trivial $G_K$-invariant subgroup $\Phi_\ell$, then it must be isomorphic to $\mathbb{Z}/(\ell)$ by (13.5.6.14), thus by (13.5.1.8) corresponds to an isogeny $\varphi_\ell : E \to E_\ell$ of degree $l$ defined over $K$. Then by Shafaverich’s theorem (13.15.3.4) there are only f.m. such $E_\ell$. But if $E_\ell \cong E_{\ell'}$, then $\hat{\varphi}_{\ell'}\varphi_\ell$ is an element of $\text{Hom}(E, E) \cong \mathbb{Z}$ by hypothesis, thus it has degree $n^2 = \ell\ell'$, which is impossible. Thus there are only f.m. $\Phi_\ell$. □

Prop.(13.9.7.2). If $K$ is a $p$-adic local field with valuation ring $R$. If $E$ is an elliptic curve over $K$ with complex multiplication, then $j(E) \in R$.

Proof: □

Prop.(13.9.7.3)[Integral $j$-Invariants]. If $F \in \text{NField}$ and $E \in \text{Ell}/F$ has complex multiplication, then $j(E) \in \mathcal{O}_F$.

Proof: Cf.[Sil99]P447. □

Prop.(13.9.7.4). If $k \in \text{Field}$, and $E \in \text{Ell}/k$ has complex multiplication, then $j(E) \in \mathbb{F}_q \cap k$.

Proof: Use the fact $\text{End}(E)$ is an order. □

Prop.(13.9.7.5)[Serre]. If $K$ is a number field and $E \in \text{Ell}/k$ without complex multiplication, then

- $\rho_\ell(\text{Gal}_K) \subset \text{Aut}(T_\ell(E))$ is of finite index for any $\ell \in \mathbb{P}$.
- $\rho_\ell(\text{Gal}_K) = \text{Aut}(T_\ell(E))$ for a.e. $\ell \in \mathbb{P}$.

Proof: Cf.[Sil16]P92. □

Prop.(13.9.7.6). If $k$ is a field and $E \in \text{Ell}/k$ with complex multiplication, then for any $\ell \in \mathbb{P} \setminus \text{char} k$, $\rho_\ell(G_k) \subset \text{Aut}(T_\ell(E))$ is Abelian.

Proof: ? Use the action of $\text{End}(E)$ on $T_\ell(E)$. □

Conj.(13.9.7.7)[Lang-Trotter]. For $E \in \text{Ell}/\mathbb{Q}$ with CM,

$$\# \{ p \in \mathbb{P}, p \leq x \, | \, E/F_p \text{ supersingular elliptic} \} \sim \frac{c\sqrt{x}}{\log x}.$$

Proof: □

Prop.(13.9.7.8)[Serre-Elkies]. For an elliptic curve $E/\mathbb{Q}$ without complex multiplication,

$$\# \{ p \in \mathbb{P}, p \leq x \, | \, E/F_p \text{ supersingular elliptic} \} \leq x^{3/4+\varepsilon}.$$

In particular, supersingular primes have density 0.

Proof: Cf.[Sil16]P153. □

Prop.(13.9.7.9)[Elkies]. For an elliptic curve $E/\mathbb{Q}$ without complex multiplication, then there are infinitely many primes $p$ s.t. $\tilde{E}$ the reduction modulo $p$ of $E$ is elliptic supersingular.

Proof: Cf.[Sil16]P153. □
8 Theorems

Thm. (13.9.8.1). Let $F = \mathbb{Q}(\sqrt{-d})$ be a quadratic imaginary field, then $F^{ab}$ can be constructed from $F$ by adjoining all the coefficients of torsion points of elliptic curves over $K$ with complex multiplications.
13.10 Arithmetic Moduli of Elliptic Curves

References are [K-M85].

1 Moduli Problems

Def. (13.10.1.1) [$\Gamma(N)$-Structure]. Let $S \in \text{Sch}$ and $E \in \text{Ell}/S$, a

- $\Gamma(N)$-structure on $E/S$ is a homomorphism $\varphi: (\mathbb{Z}/(N))^2 \to \ker([N])(S)$ s.t. there is an equality of effective Cartier divisors
  \[ E[N] = \sum_{(a,b) \in (\mathbb{Z}/(N))^2} [\varphi((a,b))]. \]

- $\Gamma_1(N)$-structure on $E/S$ is a homomorphism $\varphi: \mathbb{Z}/(N) \to \ker([N])(S)$ s.t. the effective Cartier divisor
  \[ \sum_{a \in \mathbb{Z}/(N)} [\varphi(a)]. \]
  is a subgroup scheme of $E$.

- balanced $\Gamma_1(N)$-structure on $E/S$ is an exact sequence
  \[ 0 \to K \to E[N] \to K' \to 0 \]
  of group schemes over $S$ s.t. $K, K'$ both has rank $N$ over $S$.

- $\Gamma_0(N)$-structure on $E/S$ is a finite subgroup scheme $K \subset E[N]$ over $S$ cyclic of rank $n$.

Prop. (13.10.1.2) [Functors].

Prop. (13.10.1.3) [Weil-Pairing]. Let $S \in \text{Sch}$ and $E \in \text{Ell}/S$ with a $\Gamma(N)$-structure,

Prop. (13.10.1.4) [Moduli Interpretation of Modular Curves]. The functor $\text{Sch}/\mathbb{Q} \to \mathbb{S}	ext{et}$ that maps $S$ to the isomorphism classes of elliptic curves over $S$ with a $\Gamma(N)$-structure is representable by

Def. (13.10.1.5) [Atkin-Lehner Involutions].

13.11 Arithmetic of K3 Surfaces

References are [Arithmetic and Geometry of K3 surfaces and Calabi-Yau Threefolds].
13.12 \(\ell\)-adic Étale Cohomologies over Finite Fields

Basic References are [Conrad Seminar note in Princeton], [Seminars on Gross-Zagier over Function Fields, Lei Fu], [Seminars on Weil 2 Bhatt], [Weil conjectures Perverse Sheaves and \(\ell\)-adic Fourier Transform Kiehl/Weissauer].

Notations (13.12.0.1).
- \(p \in \mathbb{P}, r \in \mathbb{Z}^+, q = p^r, k \simeq \mathbb{F}_q\). Denote \(k_n\) the unique extension of \(k\) of degree \(n\) in \(\overline{k}\).
- \(\ell \in \mathbb{P}\setminus\{p\}\).
- \(X_0 \in \text{Sch}^f/k, X = X_0 \otimes_k \overline{k}\) is its base change.
- If \(\mathcal{F}_0\) is a sheaf on \(X_0\), then \(\mathcal{F} = \mathcal{F}_0 \otimes_k \overline{k}\).
- If \(x_0 \in X_0(\overline{k}), x = x_0 \otimes_k(\overline{x})\), and \(\overline{x} \in \overline{x}\) is a point over \(x_0\).
- Fix a CDVR \((\Lambda, K, \mathfrak{m}, k)\) of characteristic \((0, \ell)\).
- For a Noetherian ring \(A\) with a distinguished ideal \(I \subset A\), let \(A_n = A/I^n\).

1 Weil Sheaves


Weil Sheaves

Def. (13.12.1.2)[Weil Sheaves]. By Galois descent, the pullback induces an equivalence of categories between the category of constructible \(\overline{\mathbb{Q}}_\ell\)-sheaves on \(X_0\) to the category of constructible \(\overline{\mathbb{Q}}_\ell\)-sheaves on \(X\) with an specified \(G(X/X_0) = G(\overline{k}/k) \cong \mathbb{Z}\)-actions. In practice, sometimes it is hard to verify the action of \(\mathbb{Z} \in \widehat{\mathbb{Z}}\) is continuous, which leads to the following definition:

The category \(\text{WSh}_\ell(X_0)\) of Weil sheaves on \(X_0\) consists of pairs \(\mathcal{G}_0 = (\mathcal{G}, F_\mathcal{G})\) where \(\mathcal{G}_0\) on an algebraic scheme \(X_0\) over \(k\) consists of a constructible \(\overline{\mathbb{Q}}_\ell\)-sheaf \(\mathcal{G}\) on \(X\) and an isomorphism \(F_\mathcal{G} : F^*_X \mathcal{G} \to \mathcal{G}(5.2.10.1)\). Notice \(F^*_X\) is not \(\mathbb{F}\)-linear! There are natural definition of morphisms of Weil sheaves. A lisse Weil sheaf is a Weil sheaf that \(\mathcal{G}\) is lisse.

Prop. (13.12.1.3)[Constructible \(\overline{\mathbb{Q}}_\ell\)-Sheaves as Weil Sheaves]. For any constructible \(\overline{\mathbb{Q}}_\ell\)-sheaf \(\mathcal{F}_0\) on \(X_0\), the canonical \(F^*_X \pi^*_0 \mathcal{G}_0 \cong (\pi \circ F_X)^* \mathcal{G}_0 = \pi^* \mathcal{G}_0\) makes \(\mathcal{F}\) into a Weil sheaf.

Prop. (13.12.1.4).
- \(\text{WSh}_\ell(X_0)\) is an Abelian category, and contains the category of lisse \(\overline{\mathbb{Q}}_\ell\)-sheaves form an Abelian subcategory.
- The constructions like \(R^i f_*, R^i f_!, f^*\) is functorial thus is defimable on \(\text{WSh}_\ell(X)\) by (6.4.2.18).
- The specified isomorphism \(F^*_\mathcal{G}_0 : F^*_X \mathcal{G} \to \mathcal{G}\) gives us an action \(F^*_X\) of \(F_X\) on \(H^i_{\text{ét},c}(X, \mathcal{G})\), just like in (6.4.2.27).
- Let \(x_0 \in X_0(\overline{k}), x = x_0 \otimes_\mathbb{k} \overline{x}, \overline{x} \in \overline{x}\), there is an action \(F^*_x\) of \(F_X\) on \(\mathcal{G}_x\), by pulling back \(\mathcal{G}_0\) to a Weil sheaf on \(x_0\), and given as follows: \(F^*_x \mathcal{G}_x \cong \mathcal{G}_x\), gives an isomorphism \(\mathcal{G}_\mathcal{F}^i(\overline{x}) \cong \mathcal{G}_\mathcal{F}^i(\overline{x})\), whose composition \(\mathcal{G}_\overline{x} \cong \mathcal{G}_\mathcal{F}^{\deg(x_0)-1}(\overline{x}) \cong \cdots \cong \mathcal{G}_\mathcal{F}(\overline{x}) \cong \mathcal{G}_\overline{x}\). For different choice of \(\overline{x}\), the actions are conjugate.

In the case \(\mathcal{G}_0\) is a constructible sheaf on \(X_0\), this map is just the inverse of (the base change of) \(\varphi_\mathcal{G}(x_0)\) on \((\mathcal{G}_0)(x_0)\), by (6.4.2.28), as .
Prop. (13.12.1.5) [Weil Sheaves and Representation]. When $X_0$ is geo.connected, there is an equivalence of categories

$$W\text{Sh}_\ell(X_0) \cong \text{Rep}_\ell(W(X_0, \overline{\mathbb{F}})) : \mathcal{G}_0 \mapsto (\mathcal{G}_0)_\overline{\mathbb{F}},$$

and the correspondence defined in (6.4.7.15) is a sub-correspondence of this.

Proof: Because by the correspondence (6.4.7.15), $\mathcal{G}$ corresponds to a representation of $\pi_1(X, \overline{\mathbb{F}})$, and $\pi_1(X, \overline{\mathbb{F}})$ acts trivially on the Galois cover $X/X_0$. Now a representation of $W(X_0, \overline{\mathbb{F}})$ is equivalent to an automorphism $\rho(\sigma)$ (where $\sigma \in W(X_0, \overline{\mathbb{F}})$ satisfies $\deg(\sigma)$ corresponds to the geometric Frobenius) that $\rho(\sigma)\rho(\pi_1(X, \overline{\mathbb{F}}))\rho(\sigma^{-1}) = \rho(\sigma\pi_1(X, \overline{\mathbb{F}})\sigma^{-1})$, which is equivalent to an isomorphism $F_\ell^* \mathcal{G} \to \mathcal{G}$.

Prop. (13.12.1.6) [Weil Sheaves and Eigenvalues]. If $X_0$ is geometrically connected, a lisse Weil sheaf $\mathcal{G}_0$ on $X_0$ is a usual $\overline{\mathbb{Q}}_\ell$-sheaf iff some deg1 element $\sigma$ in $W(X, \overline{\mathbb{F}})$ acts on $\mathcal{G}_0\overline{\mathbb{F}}$ with eigenvalues which are $\ell$-adic units.

Proof: This is purely a Galois representation problem, concerning whether the representation of $W(X_0, \overline{\mathbb{F}})$ can be extended to a representation of $\pi_1(X_0, \overline{\mathbb{F}})$, and it is a continuity problem.

Firstly the representation of $\pi_1(X, \overline{\mathbb{F}})$ stabilizes a lattice $O_E^\bullet$ for some $E/\overline{\mathbb{Q}}_\ell$ finite, and then extends $E$ to contain coefficients of $\rho(\sigma)$ and even its rational form. Then notice $\pi_1(X_0, \overline{\mathbb{F}})$ is the profinite completion of $W(X_0, \overline{\mathbb{F}})$, thus it suffices to see if the image $\rho(W(X_0, \overline{\mathbb{F}}))$ is compact, and this is equivalent to eigenvalues of $\rho(\sigma)$ are units.

Prop. (13.12.1.7) [Determinantal Criterion]. If $X_0$ is normal and geometrically connected, then a irreducible lisse Weil sheaf on $X_0$ is an actual $\overline{\mathbb{Q}}_\ell$-sheaf iff its determinant bundle is.

Proof: Use geometric monodromy group. Cf. [Conrad L19 P7].

First assume that $\mathcal{G}_0$ is geometrically irreducible, then (13.12.4.4) shows that there is a nonzero power $\sigma^m = g\cdot z$ where $g \in G_{\text{geo}}(\overline{\mathbb{Q}}_\ell)$ and $z \in Z(G(\overline{\mathbb{Q}}_\ell))$. Now $G_{\text{geo}}$ is a semisimple algebraic group (13.12.4.4), so the determinental character maps $G_{\text{geo}}(G(\overline{\mathbb{Q}}_\ell))$ to a finite group, because connected semisimple algebraic group has no nontrivial character as $[G, G] = G^?$.

So the determinant of $g$ is an $l$-unit, and $\det(\sigma^m) = \det(z)$ is a unit. But $z$ is a scalar by Schur’s lemma, thus $z$ is an $l$-adic unit. Now it suffices to show the eigenvalue of $g$ are all $l$-units.

Now consider $\rho(\pi_1(X, \overline{\mathbb{F}}))$ is a compact group in $\text{End}(V)$, thus it generates a finite $O_E$-submodule $A$, which is full-rank lattice in $\text{End}(V)$ by Jacobson density theorem? and the fact $\rho$ is absolutely irreducible. $g$ normalized $A$, because $\sigma$ and $z$ both normalizes $\rho(\pi_1(X, \overline{\mathbb{F}}))$, so the eigenvalue of the conjugate action of $g$ are all $l$-units, but its eigenvalue are of the form $\lambda_i\lambda_j^{-1}$ where $\lambda_k$ are eigenvalues of $g$, so this together with the fact $\det(g)$ is $l$-units shows that all $\lambda_i$ are $l$-units.

For the general case, Cf. [Conrad L19 P7].

Cor. (13.12.1.8) [Filtration of Weil Sheaf]. If $X_0$ is normal and geometrically connected, then for any lisse Weil sheaf $\mathcal{G}_0$, there is some $b \in \overline{\mathbb{Q}}_\ell^\times$ and a lisse Weil sheaf $\mathcal{F}_0$ that $\mathcal{G}_0 \cong \mathcal{F}_0 \otimes \mathcal{L}_b$, where $\mathcal{L}_b$ is the Weil sheaf corresponding to the character $W(X_0, \overline{\mathbb{F}}) \to \overline{\mathbb{Q}}_\ell^\times : x \mapsto b^{\deg(x)}$, which is a pull back from $\text{Spec} \mathbb{F}_q$.

More generally, for any lisse Weil sheaf, there is a filtration that each quotient is of the form $\mathcal{F}_0^{(i)} \otimes \mathcal{L}_{b_i}$ for some $b_i \in \overline{\mathbb{Q}}_\ell^\times$ and $\mathcal{F}_0^{(i)}$ lisse $\overline{\mathbb{Q}}_\ell$-sheaves.
Proof: Just choose $b = \chi_{\text{det}(\sigma)}^{1/n}$, where $\text{deg}(\sigma) = 1$, then
\[
\wedge (G_0 \otimes \mathcal{L}_{b^{-1}}) \cong \wedge (G_0 \otimes \mathcal{L}_{\chi_{\text{det}(\sigma)}}^{-1})
\]
which has unit eigenvalues thus is a lisse $\overline{\mathbb{Q}}_{\ell}$-sheaf. \qed

2 Trace Formulae

Def. (13.12.2.1) [Zeta-Functions]. For $\mathcal{F} \in \text{WSh}(X_0)$, the Zeta-function associated to $\mathcal{F}_0$ is defined to be
\[
Z(X_0, \mathcal{F}_0; T) = \prod_{x_0 \in X_0(k_0)} \det(1 - F_{x_0}^* T^{\text{deg}(x)}|\mathcal{F}_{\mathcal{F}})^{-1} \in 1 + \mathcal{T} \Lambda[[T]],
\]
where $F_{x_0}^*$ is defined in (13.12.1.4). Notice if $\mathcal{F}_0$ is a usual étale sheaf on $X_0$, then $F_{x_0}^* = \varphi_{x_0}^{-1}$.

Prop. (13.12.2.2). Situation as in (13.12.2.1),
\[
Z(X_0, \mathcal{F}_0; T) = \exp(\sum_{n \geq 1} \sum_{x \in X_0(k_n)} \text{tr}(F_{x}^*|\mathcal{F}_{\mathcal{F}}) \frac{T^n}{n})
\]
Proof: By (2.3.10.22),
\[
Z(X_0, \mathcal{F}_0; T) = \prod_{x_0 \in X_0(k)} \exp(\sum_{n \geq 1} \text{tr}((F_{x_0}^*)^n|\mathcal{F}_{\mathcal{F}}) \frac{T^n}{n})
\]
\[
= \exp(\sum_{n \geq 1} \sum_{x_0 \in X_0(k)} \text{deg}(x) \text{tr}((F_{x_0}^*)^n|\mathcal{F}_{\mathcal{F}}) \frac{T^n}{n})
\]
\[
= \exp(\sum_{n \geq 1} \sum_{x_0 \in X_0(k_n)} \text{tr}(F_{x_0}^*|\mathcal{F}_{\mathcal{F}}) \frac{T^n}{n})
\]
where in the last equality, notice there are exactly $\text{deg}(x_0)$ many points in $X_0(k)$ over $x_0 \in X_0(k_n)$. \qed

Cor. (13.12.2.3). If $\mathcal{F} = Q_\ell$, then
\[
Z(X_0; Q_\ell; T) = \prod_{x_0 \in X_0(k_0)} \frac{1}{1 - T^{\text{deg}(x_0)}}
\]
is just the Z-function defined in (16.1.1.1).

Lemma (13.12.2.4) [Weil Trace Formula]. Let $X_0 \in \text{Sch}^{\text{sep}, \text{ft}}/k$, $A$ be a Noetherian $\mathbb{Z}/\ell^n$-algebra, $\mathcal{F}_0 \in D^b_{\text{ctf}}(X_0, A)$, then
\[
\sum_{x_0 \in X_0(k)} \text{tr}(F_{x_0}^*|\mathcal{F}_{\mathcal{F}}) = \text{tr}(F_X^*|\mathcal{R} \Gamma_{\omega}(X, \mathcal{F}))
\]
Proof: Cf. [Fu11]P596?.

Prop. (13.12.2.5) [General Trace Formula for Frobenius]. Let $X_0 \in \text{Sch}^{\text{sep}, \text{ft}}/k, \mathcal{F}_0 \in D^b_{\text{cons}}(X_0, \overline{\mathbb{Q}}_{\ell})$, then
\[
\sum_{x_0 \in X_0(k)} \text{tr}(\varphi_{x_0}^{-1}|(\mathcal{F}_0)_{x_0}) = \text{tr}(F_X^*|\mathcal{R} \Gamma_{\omega}(X, \mathcal{F}))
\]
Theorem (13.12.2.6) [Grothendieck-Lefschetz Trace Formula]. For $S_0 \in \text{Sch}^{\text{sep}, \text{ft}} / S, \mathcal{F}_0 = (\mathcal{F}, F_{\mathcal{F}}) \in W\text{sh}(X_0)(13.12.1.2),$

$$Z(X_0, \mathcal{F}_0; T) = \prod_{n=0}^{2\dim X_0} Z(S_0, R^n f_0^* \mathcal{F}_0; T)^{(-1)^n}.$$

In particular, for $S = \text{Spec } k, X_0 \in \text{Sch}^{\text{sep}, \text{ft}} / k,$ by base change and (13.12.1.4),

$$Z(X_0, \mathcal{F}_0; T) = \prod_{n=0}^{2\dim X_0} \det(1 - F_X^* T | H^\text{\'et}_c(X, \mathcal{F}))^{(-1)^{n+1}}.$$

Notice by (6.4.5.7), the higher proper pushforwards just vanish.

Proof: We first prove for $\mathcal{F}_0$ a usual sheaf on $X_0$. By base change of compact pushforwards, it suffices to prove for $S = \text{Spec } k$: By (2.3.10.22), and in this case, the assertion follows from (13.12.2.5) and (13.12.2.2).

For general $\mathcal{F}_0$,

Cor. (13.12.2.7). $Z(X_0, \mathcal{F}_0; T)$ is a rational function in $T$.

Prop. (13.12.2.8). Cf. [Representations of Finite Groups of Lie type, Digne and Michel].

Cor. (13.12.2.9). The Lefschetz number is independent of $\ell$.

Prop. (13.12.2.10) [Grothendieck-Lefschetz Trace Formula for Weil Sheaves]. For any Weil sheaf $\mathcal{F}_0 = (\mathcal{F}, F_{\mathcal{F}}) \in W\text{sh}(X_0)(13.12.1.2),$ define the generalized L-function

$$L(X_0, \mathcal{F}_0, T) = \prod_{x_0 \text{ closed in } X_0} \det(1 - T^{\text{deg}(x)} F_{x_0}^* | H^i_{\text{et}, c}(X, \mathcal{F}))^{-1}(13.12.1.4)$$

Then we have

$$L(X_0, \mathcal{F}_0, T) = \prod_{i=0}^{2\dim X_0} \det(1 - TF_X^* | H^i_{\text{et}, c}(X, \mathcal{F}))^{(-1)^{i+1}}.$$

Proof: Use the filtration in (13.12.1.8), notice that the trace is additive for a filtration, so we can reduce to the case $\mathcal{G}_0 = \mathcal{F}_0 \otimes \mathcal{L}_b$ and $\mathcal{G}_{\mathcal{F}} = \mathcal{F}_{\mathcal{F}} \otimes \mathcal{L}_b$, then the Euler factor is

$$\det(1 - T^{\text{deg}(x)} F_{x}^* | \mathcal{F}_{\mathcal{F}})$$

and the cohomology factor is

$$\det(1 - tF_X^* | H^i_{\text{et}, c}(X, \mathcal{F} \otimes \mathcal{L}_b)) = \det(1 - tf^* F_X^* | H^i_{\text{et}, c}(X, \mathcal{F} \otimes \mathcal{L}_b))$$

where the projection formula (6.4.5.8) is used, noticing the $\mathcal{L}_b$ is pulled back from $\text{Spec } F_q$. 

□
3 Weights and Purity

Determinantal Weights

Prop. (13.12.3.1) [Structure of Weil Group of Curves]. If $X_0$ is a smooth curve over $F_q$, then the image of $\pi_1(\overline{X}, \overline{\pi})$ in $W(X_0, \overline{\pi})^{ab}$ is a product of a finite group and a pro-$p$ group.

Proof: Let $K$ be the function field of $X_0$, $\overline{X}_0$ be the regular completion of $X_0$, with $S_0 = \overline{X}_0 - X_0$, then we have an isomorphism $\pi_1(\overline{X}_0, \overline{\pi}) \cong G_K$ Cf.[Étale Cohomology Lei Fu P136]. So we can use global class field theory:

$$
\pi_1(\overline{X}, \overline{\pi})^{ab} \xrightarrow{\sim} \pi_1(\overline{X}_0, \overline{\pi})^{ab} \xrightarrow{\sim} G_k \cong \hat{\mathbb{Z}} \rightarrow 0
$$

$$
0 \xrightarrow{\sim} I_K \xrightarrow{\sim} W(\overline{X}_0, \overline{\pi})^{ab} \cong W(K, k) \rightarrow W(k) \cong \mathbb{Z} \rightarrow 0
$$

$$
0 \rightarrow K^* \backslash (A_k^{\times})^1 / \prod_v \mathcal{O}_v^* \rightarrow K^* \backslash A_K^* / \prod_v \mathcal{O}_v^* \rightarrow q^\mathbb{Z} \rightarrow 0
$$

So the image of $\pi_1(\overline{X}, \overline{\pi})$ factors through $\pi_1(\overline{X}, \overline{\pi}) \rightarrow \pi_1(\overline{X}_0, \overline{\pi})^{ab} \rightarrow K^* \backslash A_K^* / \prod_v \mathcal{O}_v^*$ which is the class number of $K$, is finite.

In this diagram, $W(X_0, \overline{\pi})$ corresponds to $K^* \backslash A_K^* / \prod_v \mathcal{O}_v^*$, so

$$
0 \rightarrow \ker(W(X_0, \overline{\pi}) \rightarrow W(\overline{X}_0, \overline{\pi})) \rightarrow \text{Im}(\pi_1(X_0, \overline{\pi})) \rightarrow \text{Im}(\pi_1(\overline{X}_0, \overline{\pi})) \rightarrow 0
$$

But the kernel is a quotient of $\prod_v \mathcal{O}_v^*$, which is a pro-$p$ group times a finite group, so finally $\text{Im}(\pi_1(X_0, \overline{\pi}))$ is a product of a pro-$p$-group times a finite group. \qed

Lemma (13.12.3.2) [Curve Rank 1 case]. If $X_0$ is a geometrically connected smooth curve over $F_q$ and $\chi : W(X_0, \overline{\pi}) \rightarrow \overline{Q}_\ell^\times$ be a continuous character, then there exists a $c \in \overline{Q}_\ell^\times$ that $\chi$ is a product of a character of finite order and the character $\sigma \mapsto c^{\deg(\sigma)}$.

In particular, the Weil sheaf corresponding to $\chi$ is punctually $\nu$-pure of weight $2 \log_q |\iota(c)|$.

Proof: By(14.1.1.2), the image of $\chi$ is in $\mathcal{O}_k^\times$ for some $E/\mathbb{Q}_\ell$ finite, so use(13.12.3.1), it has an open subgroup which is pro-$p$ and pro-$\ell$ so trivial, thus $\pi_1(X_0, \overline{\pi})$ is mapped to a finite group.

In particular there is an $n$ that $\chi^n = \text{id}$ on $\pi_1(X_0, \overline{\pi})$, so there is some $b$ that $\chi^n = b^{\deg(\sigma)}$, hence if $c$ is an $n$-th roots of $b$ and we let $\chi' = \chi/c^{\deg(\sigma)}$, then $\chi'^n = 1$. \qed

Cor. (13.12.3.3) [Rank 1 Lisse Sheaf is Pure]. If $X_0$ is a geometrically connected smooth curve, then any lisse Weil sheaf of rank 1 is pure.

Def. (13.12.3.4) [Determinential Weight]. Let $\mathcal{F}_0$ be a lisse Weil sheaf on a geometrically connected smooth scheme $X_0$, and $0 = \mathcal{F}_n \subset \mathcal{F}_{n-1} \subset \ldots \subset \mathcal{F}_0$ be a filtration of lisse sheaves that the quotients are irreducible, we define the determinential $\nu$-weights of $\mathcal{F}_0$ to be that of the $\nu$-weights of the top wedge products of the successive quotients divided by their ranks, which exists by(13.12.3.3).

Notice that the determinental $\nu$-weights are unchanged when $\mathcal{F}_0$ is replaced by its semisimplification $\mathcal{F}_0^s = \bigoplus_{\nu \geq 0}(\mathcal{F}_\nu/\mathcal{F}_{\nu-1})$. 

Purity

Def. (13.12.3.5) [Purity]. For an embedding $\iota : \overline{Q}_\ell \to \mathbb{C}$, $F_0 \in \text{Wsh}(X_0)$ is called $\iota$-pure of weight $w$ if for any closed point $x \in X$, the $\overline{Q}_\ell$-eigenvalues of $F_x$ on $F_x^*$ satisfies $|\iota(\alpha_i)| = (q^{\deg(x)})^{w/2}$. It is called pure of weight $w$ iff for any closed point $x \in X$, the $\overline{Q}_\ell$-eigenvalues are $q^{\deg(x)}$-Weil numbers of weight $w$, i.e. $\iota$-pure for any embedding $\iota : \overline{Q}_\ell \to \mathbb{C}$.

It is said to be (\-

Prop. (13.12.3.7). $Q_\ell(1)$ is pure of weight $-2$, thus $Q_\ell(r)$ is pure of weight $-2r$. This is because the geometric Frobenius $F_x$ acts by $1/q^{d_\ell}$-th power, which is additively multiplying by $(q^{d_\ell})^{-2}/2$.

Prop. (13.12.3.8) [Permanence Properties].

- $f_0 : X_0 \to Y_0$ is a morphism, and $\mathcal{G}_0$ is a Weil sheaf on $Y_0$, then if $\mathcal{G}_0$ is $\iota$-pure, then $f_0^* \mathcal{G}_0$ is also $\iota$-pure, and the converse is also true if $f$ is surjective.
- If $f_0 : X_0 \to Y_0$ is finite, and $\mathcal{G}_0$ is a Weil sheaf on $X_0$, then if $j_0^* \mathcal{G}_0$ is $\iota$-pure, then $\mathcal{G}_0$ is $\iota$-pure.
- Let $k'/k$ be a finite field extension, then a Weil sheaf $\mathcal{G}_0$ on $X_0$ is pure of weight $\beta$ iff $(\mathcal{G}_0)_{k'}$ is on $(X_0)_{k'}$.

Proof: 1 is because the stalk corresponds.
2: This is because the stalks can be calculated, by $\Box$.

Semicontinuity of Weights

Def. (13.12.3.9) [Maximal Weight]. For a general Weil sheaf $\mathcal{G}_0$ on $X_0$, we can also define the maximal $\iota$-weight of $\mathcal{G}_0$ as

$$w(\mathcal{G}_0) = \sup_{x \in |X_0|} \sup_{\alpha_i} 2 \log_{N(x)}(|\iota(\alpha_i)|).$$

Lemma (13.12.3.10). $|X_0(k_n)| = O(q^{n \dim X})$

Proof: We can pass to the reduced structure of $X_0$, then we can use excision to pass to the integral case. Then choose an open affine dense subset $U_0$ of $X_0$, then by Noetherian normalization, it factors through a finite map $f : U_0 \to \mathbb{A}^n_{k_n} \times X_0$, so

$$|U(k_n)| \leq (\deg f)q^{n \dim X_0}$$

Then we can use induction on dimension, because $\dim(X_0 - U_0) < \dim X_0$. $\Box$

Lemma (13.12.3.11). Let $\mathcal{G}_0$ be a Weil sheaf on $X_0$ and $\beta$ be a real number that $\beta \geq w(\mathcal{G}_0)$, then the $L$-function

$$\iota(L(X_0, \mathcal{G}_0, t)) = \prod_{x \in |X_0|} \iota(\det(1 - t^{d_\ell} F_x, \mathcal{G}_0, x)^{-1})$$

converges for $|t| < q^{-\beta/2 - \dim X_0}$ and has no zero or pole there.
Lemma (13.12.3.12) [Semicontinuity of Weights for Curves]. Let $X_0$ be a smooth curve over $k$ and $U_0 \to X_0$ be a nonempty open with $S_0 = X_0 - U_0$. Let $\mathcal{G}_0$ be a Weil sheaf on $X_0$ s.t. the restriction $j_0^* \mathcal{G}_0$ is lisse and $H^0_S(X, \mathcal{G}) = 0$, then $w(j_0^* (\mathcal{G}_0)) \leq \beta$ implies $w(\mathcal{G}_0) \leq \beta$.

**Proof:** For any point $x$, consider an affine open subset of $X_0$, then reduce to the affine case, and because $H^0_S(X, \mathcal{G}) = 0$ and the excision sequence (6.4.5.5), we have $\mathcal{G} \hookrightarrow j_* j^* \mathcal{G}$, so the weights of $\mathcal{G}_0$ are no more than that of $j_* j^* \mathcal{G}$, and replacing $\mathcal{G}_0$ with $j_0^* j_0^* \mathcal{G}_0$, we can assume $\mathcal{G}_0 = j_0^* j_0^* \mathcal{G}_0$. Then

$$H^0_c(X, \mathcal{G}) = H^0_c(X, j_0^* j_* \mathcal{G}) = H^0_c(U, j_* \mathcal{G}) = 0$$

by Poincaré duality and the fact $j_*$ is exact because it is finite.

Now by Grothendieck-Lefschetz trace formula,

$$L(X_0, \mathcal{G}_0, t) = L(U_0, j_0^* (\mathcal{G}_0), t) \cdot \prod_{s \in S_0} \det(1 - t^d s F_s, \mathcal{G}_s^{-1}) = \frac{\det(1 - F_X t | H^1_{\et, c}(X, \mathcal{G}))}{\det(1 - F_X t | H^2_{\et, c}(X, \mathcal{G}))}$$

Denote $\mathcal{F}_0 = j_0^* \mathcal{G}_0$, then

$$H^2_c(X, \mathcal{G}) = H^2_c(U, \mathcal{F}) = (\mathcal{F}_{\overline{\tau}})_{\tau_1(U, \overline{\tau})}(-1)$$

So the weights of eigenvalues of $F_X$ on $H^2_c(X, \mathcal{G}) \leq$ weights of $\mathcal{F} + 2$, hence the $L$-function converges for $|t| < q^{-\beta/2 - 1}$. Now the LHS has $L(U_0, j_0^* (\mathcal{G}_0), t)$ converges for $|t| < q^{-\beta/2 - 1}$ because $w(\mathcal{F}_0) \leq \beta$, and so for the points in $S_0$, we also have $\det(1 - t^d F_s, \mathcal{G}_s)$ has no zero there, which means they have weights $\leq \beta + 1$. Now consider replacing $\mathcal{G}_0$ with $\mathcal{G}_0 \otimes k$ and let $k \to \infty$, then their weights $\leq \beta$. □

Prop. (13.12.3.13) [Semicontinuity of Weights]. Let $X_0$ be geo.normal, $\mathcal{G}_0$ be a lisse sheaf on $X_0$ and $j_0 : U_0 \to X_0$ be an open dense subscheme, then

- $w(\mathcal{G}_0) = w(j_0^* \mathcal{G}_0)$.
- If $j_0^* (\mathcal{G}_0)$ is $\nu$-pure of weights $\beta$, then $\mathcal{G}_0$ is also $\nu$-pure of weights $\beta$.
- Let $X_0$ be irreducible and normal, and $\mathcal{G}_0$ is irreducible, then if $j_0^* \mathcal{G}_0$ is $\nu$-mixed, then $\mathcal{G}_0$ is $\nu$-pure.
Proof: 1: The weights is local so we may assume $X_0$ is irreducible, and then for any closed point $x$, we can connect it with $U_0$ with a curve(choose an affine open and use Noetherian Normalization to choose an irreducible component of an arbitrary curve in $\mathbb{A}^n$). Notice $H^0_S(X, \mathcal{G}) = 0$ because it is lisse thus $H^0(X, \mathcal{G})$ is determined by stalk thus $H^0(X, \mathcal{G}) \to H^0(U, \mathcal{G}|_U)$ is injective. So we finish by the curve case (13.12.3.12).

2: Apply item 1 to $\mathcal{G}_0$ and $\mathcal{G}_0'$.  

3: It is $\ell$-mixed so it has $\ell$-pure Weil sheaf constituents. Now by (6.4.7.9) we can find an open dense $U_0$ that restriction to $U_0$ has constituents $\ell$-pure lisse sheaves. But it is also irreducible because $\pi_1(U_0, \overline{\pi}) \to \pi_1(X_0, \overline{\pi})$ is surjective, so it is $\ell$-pure and item 2 shows $\mathcal{G}_0$ is $\ell$-pure.  

$L^2$-Norms and Maximal Weights

Def. (13.12.3.14). As in (13.12.8.1), for any $\mathcal{G}_0 \in D_{cons}(X_0, \overline{\mathbb{Q}}_\ell)$, we have a a function

$$f^{\mathcal{G}_0} : X_0(k_\eta) \to \overline{\mathbb{Q}}_\ell : x \mapsto \sum_i (-1)^i \text{tr}(F^{x|\eta}_x | (H^i(\mathcal{G}_0))_x).$$

Fix an arbitrary isomorphism $\overline{\mathbb{Q}}_\ell \cong \mathbb{C}$, we can consider the usual $L^2$-norm for functions on $X_0(k_\eta)$, denoted by $(f, g)_n$.

Def. (13.12.3.15). Notice the equation form (13.12.3.11) can be rewritten as

$$\frac{d\log}{dt} L(X_0, \mathcal{G}_0, t) = \sum_{n \geq 1} \sum_{x \in |X_0|_0 | d_x = n} d_x (\text{tr}(F^{x|\eta}_x)) t^{n-1} = \sum_n (f^{\mathcal{G}_0}, 1)_n t^{n-1}.$$

Now we define another closed related function

$$\varphi^{\mathcal{G}_0}(t) = \sum_n ||f^{\mathcal{G}_0}||_n^2 t^{n-1},$$

which works better with Fourier transform we are about to define later.

Lemma (13.12.3.16). There is a constant $C$ that $||f^{\mathcal{G}_0}(x)||^2 \leq C q^{w(\mathcal{G}_0) + \dim X_0}$, so $\varphi^{\mathcal{G}_0}(t)$ converges for $|t| < q^{-w(\mathcal{G}_0)} - \dim X_0$.

Proof: The proof is similar to that of (13.12.3.11) thus omitted.  

Def. (13.12.3.17)[Norm of a Weil Sheaf]. Define the Norm of a Weil sheaf as

$$||\mathcal{G}_0|| = \sup_{\rho} \limsup_n \frac{||f^{\mathcal{G}_0}||_n^2}{q^n (\rho + \dim X_0)} > 0.$$ 

Then $q^{-||\mathcal{G}_0|| - \dim X_0}$ is just the radius of convergence of the function $\varphi^{\mathcal{G}_0}(t)$, and $||\mathcal{G}_0|| \leq w(\mathcal{G}_0)$ by lemma (13.12.3.16) above.

Prop. (13.12.3.18)[Radius of Convergence]. Let $\mathcal{G}_0$ be a $\ell$-mixed sheaf on a smooth curve $X_0$ over $k$, and $H^0_\ell(X, \mathcal{G}) = 0$, then $||\mathcal{G}_0|| = w(\mathcal{G}_0) = \beta$.

Proof: It suffices to show $w(\mathcal{G}_0) \leq ||\mathcal{G}_0||$. First notice we can assume $X_0$ is reduced because the nilpotents corresponds to zero Frobenius eigenvalues, and also it is connected, because the function $f^{\mathcal{G}_0}$ is additive in $X$. Now we study by cases:
1: If $\mathcal{G}_0$ is a lisse $\nu$-pure sheaf on a smooth affine curve $X_0$, we may assume $\mathcal{G}_0 \neq 0$, then $\mathcal{G}_0 \otimes \overline{\mathcal{G}_0}(13.12.5.2)$ is $\nu$-real of weight $2\beta$ and $(f^{\mathcal{G}_0} \otimes \overline{\mathcal{G}_0}, 1)_n = ||f^{\mathcal{G}_0}||_n^2$, so $\varphi^{\mathcal{G}_0}(t)$ is just the logarithmic derivative of the $L$-function $L(X_0, \mathcal{G}_0 \otimes \overline{\mathcal{G}_0}, t)$, thus $(13.12.3.11)$ shows its convergence radius $\geq q^{-\beta - 1}$.

And notice the $H^0$ terms vanish so the poles can only appear as the zeros of $H^2$ term, so $(13.12.5.3)$ shows the poles of the $L(X_0, \mathcal{G}_0 \otimes \overline{\mathcal{G}_0}, t)$ has weight $2\beta + 2$, thus the poles can only appear on $|t| = q^{-\beta - 1}$.

Now consider each local Euler factor $\det(1 - F_x t^d) = (\mathcal{G}_0 \otimes \overline{\mathcal{G}_0})_x$ has non-negative coefficients, they have poles because $\mathcal{G}_0 \neq 0$, and their poles have weight $\beta$ because of purity, thus their product also has (real)poles, by previous argument, the pole has weight $\beta + 1$, thus it has convergence radius at most $q^{-\beta - 1}$, so we are done.

2: If $\mathcal{G}_0$ is a $\nu$-mixed, consider its semisimplification $\mathcal{G}_0^{ss} = \mathcal{F}_0 \oplus \mathcal{H}_0$, where $\mathcal{F}_0$ is $\nu$-pure of weight $w(\mathcal{G}_0)$, and $w(\mathcal{H}_0) \leq w(\mathcal{F}_0)$.

Then $f^{\mathcal{G}_0} = f^{\mathcal{F}_0} + f^{\mathcal{H}_0}$, and
\[
\varphi^{\mathcal{G}_0}(t) = \varphi^{\mathcal{F}_0}(t) + \sum_{n \geq 1} 2 \text{Re}(f^{\mathcal{F}_0}, f^{\mathcal{H}_0})_n t^{n-1} + \varphi^{\mathcal{H}_0}(t)
\]
then by item1 $\varphi^{\mathcal{F}_0}(t)$ has convergence radius $q^{-w(\mathcal{G}_0) - 1}$, and by $(13.12.3.16)$ $\varphi^{\mathcal{H}_0}(t)$ has radius at least $q^{-w(\mathcal{H}_0)} > q^{-w(\mathcal{G}_0) - 1}$, and by Cauchy inequality the middle term satisfies
\[
|2 \text{Re}(f^{\mathcal{F}_0}, f^{\mathcal{H}_0})_n| \leq 2 ||f^{\mathcal{F}_0}||_n ||f^{\mathcal{H}_0}||_n \leq C q^{n(w(\mathcal{F}_0) + w(\mathcal{H}_0)/2 + 1)}
\]
So the middle term has convergence radius $> q^{-w(\mathcal{G}_0) - 1}$, so their sum has convergence radius $q^{-w(\mathcal{G}_0) - 1}$. \hfill \Box

4 Geometric Monodromy

Def. (13.12.4.1) [Notations]. Let $X_0$ be a geometrically connected normal scheme over $k = \mathbb{F}_q$ in this subsection.

Def. (13.12.4.2) [Geometric Monodromy Group]. Let $\mathcal{G}_0$ be a Weil-sheaf associated to a representation $(V, \rho) = GL(V)$ of $W(X_0, \overline{x})$, the geometric monodromy group $G_{geo}$ associated to $\mathcal{G}_0$ is the Zariski Closure of $\rho(\pi_1(X, \overline{x})) \subset GL(V)$.

Every element in $\rho(W(X_0, \overline{x}))$ normalizes $G_{geo}$ by continuity, so choosing an arbitrary generator $\sigma \in W(\overline{k}/k)$, we have an action of $W(\overline{k}/k)$ on $G_{geo}$. Define $G = W(\overline{k}/k) \ltimes G_{geo}$ the arithmetic monodromy group of $\mathcal{G}_0$.

Lemma (13.12.4.3). If $G_{geo}$ is connected, then there is a positive integer $N$ that the semidirect sequence
\[
1 \to G_{geo} \to \text{deg}^{-1}(N\mathbb{Z}) \overset{\text{deg}}{\to} N\mathbb{Z} \to 1
\]
is direct, i.e. $\text{deg}^{-1}(N\mathbb{Z}) \cong G_{geo} \times \mathbb{Z}$.

Proof: Choose a $\text{deg}(g) = 1$. The representation $G_{geo}$ splits as a characters of $Z(G)$, and then some $g^n$ stabilizes these characters, hence stabilizes $Z(G)$, which then it descends to an action on $G_{adj}$, whose automorphism is the automorphism of the Dynkin diagram, so finite, so some $g^n$ fixes $G_{adj}$ after changing a semidirect product, thus induces a map $\text{Hom}(G_{adj}, Z(G))$, but $G_{adj}$ is semisimple (7.3.3.19), so the connected component is mapped to 1 in $Z(G)(7.3.3.17)$, so there are only f.m. such homomorphism, showing $g^k$ is 1, so the product is exact for $N = k$. \hfill \Box
Prop. (13.12.4.4) [Geometric Monodromy Group is Semisimple]. Let $G_0$ be a geometrically semisimple lisse Weil sheaf (13.12.1.5), then

- $G_{geo}$ and $G^0_{geo}$ are semisimple algebraic group.
- Let $Z = Z(G(\mathbb{Q}_l))$, then the map $\psi : Z \to W(\overline{k}/k)$ has finite kernel and cokernel. In particular, $Z$ contains an element of finite degree, and it is surjective after a finite base change of fields.

And notice in fact if $G_0$ is semisimple, then it is automatically geometrically semisimple by (15.1.1.23).

**Proof:** 1: $G_{geo}$ is semisimple iff $G^0_{geo}$ is semisimple. Pass to a finite étale covering, we may assume $G = G_{geo} \times \mathbb{Z}$, consider the composite $W(X_0, \pi) \to G_{geo} \times \mathbb{Z} \to G_{geo} \to G^0_{geo}$, then $\pi_1(X, \pi)$ is Zariski dense in $G^0_{geo}$, and (13.12.3.3) shows clearly $G^0_{geo}$ has no maximal torus thus finite.

For any $g \in G_{geo}$, consider $v_p g(n) = g^n g^{-1} \zeta^{-n} \in G_{geo}$, so $\varphi_g (m + n) = \varphi_g(n) \zeta^n \varphi_g(m) \zeta^{-n} = \varphi_g(n) \varphi_g(m)$, thus it is a homomorphism, and if $g' \in G_{geo}$, then

$$\varphi_{g'} = \varphi_{g(g^{-1} g')} = \varphi_{g' g} = g' \varphi_g(g')^{-1}$$

so $\varphi_g$ has image in $Z(G^0_{geo})$, which is finite, so $\varphi_g(n) = 1$ for some $n$, then $\zeta^n$ commutes with $G_{geo}$ so $\zeta^n \in Z(G)$.

Cor. (13.12.4.5) [Weights and Center Element Actions]. Let $G_0$ be a semisimple lisse Weil sheaf on $X_0$, if $z \in Z(G(\mathbb{Q}_p))$ satisfies $\deg(z) = n \neq 0$, which exists by (13.12.4.4), then if $z$ acts on $V$ with eigenvalues $\alpha_i$, then $\frac{2}{n} \log_q(|\mu(\alpha_i)|)$ is just the determinental $\iota$-weights of $G_0$.

**Proof:** $z$ is in the center, thus by Shur’s lemma, it acts on each irreducible part of $G_0$ by a constant. Thus the determinental weights are clear, by definition.

Cor. (13.12.4.6) [Properties of Determinental Weights]. Let $X_0$ be a smooth and geometrically connected curve, $\mathcal{F}_0, G_0$ be lisse Weil sheaves on $X_0$, then

- If $\alpha_i$ are the determinental $\iota$-weights of $\mathcal{F}_0$ and $\beta_j$ be that of $G_0$, then $\alpha_i + \beta_j$ are those of $\mathcal{F}_0 \otimes G_0$ with multiplicity.
- For $\gamma \in \iota$, let $r(\gamma)$ be the sum of ranks of all irreducible constituents of $\mathcal{F}_0$ which have determinental weight $\gamma \text{ w.r.t } \iota$, then the determinental weights of $\wedge^r \mathcal{F}_0$ are the numbers $\sum_n n(\gamma) n(\gamma) = r$ and $0 \leq n(\gamma) \leq r(\gamma)$, $n(\gamma) \in \mathbb{Z}$ with multiplicity.

**Proof:** Firstly notice the determinental weight is unchanged when we change $\mathcal{F}_0, G_0$ to their semisimplification $\mathcal{F}_0^{ss}, G_0^{ss}$ (13.12.3.4). And notice $(\mathcal{F}_0 \otimes G_0)^{ss} = ((\mathcal{F}_0)^{ss} \otimes (G_0)^{ss})^{ss}$, thus the determinental weights of $\mathcal{F}_0 \otimes G_0$ are also unchanged. Similarly for the wedge product.
2: We may assume \( F_0, G_0 \) are irreducible, and let \( H_0 = (F_0 \otimes G_0)^{ss} \), \( G_{geo}^{ss} \) be the geometric monodromy group of \( \pi_1(X, \mathcal{F}) \) in \( GL(F_\mathcal{F} \oplus G_\mathcal{F}) \) and \( GL(H_\mathcal{F}) \) correspondingly, then \( G_{geo}^{ss} \to G_{geo}^{ss} \) is surjective because they are both the geometric monodromy group of \( H_\mathcal{F} \). So also \( G^{ss} \to G^{ss} \) is surjective. So if \( g \) be an element in the center of \( G^{ss} \) that has nonzero degree, then it maps to the center of \( G^{ss} \) of nonzero degree. And the action of \( g \) on each factor \( F_x, G_x \) is a constant, so action on \( H_x \) is also a constant, so we are done.

3: Easy from2. 

\[ \square \]

5 Real Sheaves

**Def. (13.12.5.1) [\( \iota \)-Real Sheaf].** Let \( F_0 \) be a Weil sheaf on \( X_0 \), then \( F_0 \) is called \( \iota \)-real if for any \( x \in |X_0| \), the characteristic polynomial \( \iota(\det(1-F_xt,F_\mathcal{F})) \) of \( F_x \) real coefficients.

**Prop. (13.12.5.2).** Any \( \iota \)-pure Weil sheaf of weight \( w \) is a direct sum of a \( \iota \)-real \( \iota \)-pure Weil sheaf. In fact, \( F_0 \oplus F_0^\theta(-w) = F_\mathcal{F} \) is \( \iota \)-real.

**Lemma (13.12.5.3) [Eigenvalue of Cohomology and Stalk in Curve case].** Let \( X_0 \) be a smooth geometrically connected curve over \( \mathbb{F}_q \), \( F_0 \) is a lisse Weil sheaf on \( X_0 \), then the eigenvalues of \( F_X \) on \( H^0(X,F) \) or \( H^2_{\text{et},c}(X,F) \) is related to the determinential weights of \( F_0 \) and the eigenvalue of \( F_x \) on \( F_\mathcal{F} \).

**Proof:** Let \( V = F_\mathcal{F} \), then

\[
H^0(X,F) = V^{\pi_1(X,\mathcal{F})}, \quad H^2_{\text{et}}(X,F) = V^{\pi_1(X,\mathcal{F})}(-1).
\]

Then the base change sheaf of the sheaf \( V^{\pi_1(X,\mathcal{F})} \) or \( V^{\pi_1(X,\mathcal{F})}(-1) \) on \( \text{Spec}k \) is the maximal subsheaf/quotient lisse sheaf of \( F_\mathcal{F} \) that is constant on \( X \). Then it has determinential weights just the action of \( F_X \) on the stalk by(13.12.4.5), which are also determinential weights of \( F_0 \) by(13.12.4.6).

\[ \square \]

**Lemma (13.12.5.4) [Rankin-Selberg Method].** Let \( X_0 \) be a smooth geometrically connected curve over \( \mathbb{F}_q \), \( F_0 \) be a lisse Weil sheaf on \( X_0 \), and \( w \) be the largest determinential weight of \( F_0 \), then for any \( x \in |X_0| \), \( w_{N(x)}(\alpha) \leq w \).

**Proof:** By the arbitrariness of \( x \), we can replace \( X_0 \) by an affine open nbhd of \( x \). Then \( H^0_{\text{et}}(X,F) = 0 \) by Artin vanishing(6.4.2.12). By Grothendieck trace formula,

\[
\prod_{x \in |X_0|} \iota \det(1-t^{d_x}F_x| \otimes 2kF_\mathcal{F})^{-1} = \frac{\iota \det(1-tF^\ast_X|H^1_{\text{et}}(X,\otimes 2kF))}{\iota \det(1-tF^\ast_X|H^2_{\text{et}}(X,\otimes 2kF))}
\]

Now the weight of root \( t_0 \) of \( \det(1-tF^\ast_X|H^2_{\text{et}}(X,\otimes 2kF)) \) has weight \( \leq \) determinential weight of \( G_{ss}^{\otimes 2k+2} \leq 2kwv + 1(13.12.5.3) \leq 2kw + 1(13.12.4.6) \), so \( |t_0| \geq q^{-k\beta-1} \).

Now by the formula?? and noticing \( \text{tr}(F^m_{x}, \otimes 2kF_\mathcal{F}) = (\text{tr}(F_x, F_\mathcal{F}))^{2k} \), so \( (1-t^{d_x}F_x| \otimes 2kF_\mathcal{F})^{-1} \) has non-negative coefficients, which means their convergence radius are no less than \( q^{-k\beta-1} \), equivalently, \( (1-t^{d_x}F_x| \otimes 2kF_\mathcal{F}) \) has no zeros with eigenvalue \( < q^{-k\beta-1} \).

So for any eigenvalue \( \alpha \) of \( F_x \) acting on \( F_\mathcal{F} \), \( |\iota(\alpha-2k/d_x)| \leq q^{-k\beta-1} \), or equivalently, \( |\iota(\alpha)|^2 \leq N(x)^{\beta+1/k} \).

Now let \( k \to \infty \), we are done.

\[ \square \]
Lemma (13.12.5.5)[Real Sheaf Mixed Curve case]. Let $X_0$ be smooth geometrically irreducible curve over $k$ and $\mathcal{G}_0$ be an $\iota$-lisse Weil sheaf on $X_0$, then all irreducible constituents of $\mathcal{G}_0$ is $\iota$-pure, and their $\iota$-weights coincide with their determinental weights.

Proof: For $\beta \in \mathbb{R}$, let $\mathcal{F}_0(\beta)$ be the sum of constituents of $\mathcal{F}_0$ of determinantal weight $\beta$, and let $n(\beta) = \text{rank}(\mathcal{F}_0(\beta))$, then we need to show that $w_{N(x)}(\alpha_i(\beta)) = \beta$ for any eigenvalue of $\mathcal{F}_x$ on $\mathcal{F}(\beta)$.

By definition of determinental weight, for each $\gamma$, we have $\sum w_{N(x)}(\alpha_j(\gamma)) = \gamma n(\gamma)$. Now let $N = \sum_{\gamma > \beta} n(\gamma)$, then any determinental weight of $\Lambda^{N+1}\mathcal{F}_0$ has weight $\leq \beta + \sum_{\gamma > \beta} n(\gamma)\gamma$: This is clear by (13.12.4.6) as the determinental weights of $\Lambda^{N+1}\mathcal{F}_0$ is of the form $\sum_\gamma a(\gamma)\gamma$ that $0 \leq a(\gamma) \leq \gamma$ and $\sum_\gamma a(\gamma) = N + 1$.

But now $\alpha_i(\beta) \prod n(\gamma) \alpha_j(\gamma)$ is an eigenvalue of $(\Lambda^{N+1}\mathcal{F}_0)_\mathbb{F}$, but by lemma (13.12.5.4), $w_{N(x)}(\alpha_i(\beta)) = \beta$. □

Prop. (13.12.5.6)[Real Sheaf is Mixed]. Let $X_0$ be an algebraic scheme over $\mathbb{F}_q$, then

- Any $\iota$-real Weil sheaf on $X_0$ is $\iota$-mixed.
- If $X_0$ is irreducible and normal, any irreducible constituent of a lisse of an $\iota$-real sheaf is $\iota$-pure.

Proof: Cf.[Bhatt P28], [KW, P36].

We have the following devissages:
- Choose an open subset $j_0 : U_0 \hookrightarrow X_0, S_0 = X_0 - U_0$ and consider the fundamental excision sequence (6.4.5.4), we can reduce to an open affine subscheme $U_0 \subset X_0$.
- We may base change to a finite field extension.
- So we may reduce to the case $X_0$ is smooth, irreducible affine, and $\mathcal{G}_0$ is lisse, with all the irreducible constituents geometrically irreducible (by base change, because they are geometrically semisimple (13.12.4.4)). And we may assume $\dim X_0 > 1$ because the curve case is proven.
- Change $k$ to the alg. closure of $k$ in the function field of $X_0$, we can assume $X_0$ is geometrically irreducible by (5.4.3.16).

Embed $X_0$ in some projective space $\mathbb{P}^N_0$, then by a suitable Bertini theorem, the linear subspaces of codimension $\dim X - 1$ that intersects $X$ with a non-empty smooth irreducible curve $C_L$ is dense in the Grassmannian. Now the closed points in any $C_L$ is a pure-point for the any irreducible component $\mathcal{F}_0$ of $\mathcal{G}_0$ of the same weights. Now let $L$ vary, then there is a dense subset of a finite extension of $X_0$ that $\mathcal{F}_0$ is pure. So we are done. □

6 Deligne’s Purity Theorem

Prop. (13.12.6.1)[Deligne’s Purity Theorem]. If $f : X_0 \to Y_0$ is a separated morphism of algebraic scheme over $k$, and $\mathcal{F}_0$ is a lisse $\overline{Q}_\ell$-sheaf on $X$ that is mixed weights $\geq n$, then for any integer $i \geq 0$, the sheaf $R^i f_* \mathcal{F}$ is also $\iota$-mixed of weights $\leq n + i$.

Moreover, each $\iota$-weight of of $R^i f_* \mathcal{F}$ is equivalent modulo $\mathbb{Z}$ to an $\iota$-weight of $\mathcal{F}$.

Proof: This follows from (13.12.6.6). □

Cor. (13.12.6.2). If $X_0$ is a smooth separated algebraic scheme over $k$, $\mathcal{F}_0$ is mixed of weight $\geq n$, then $H^i_{\acute{e}t}(X, \mathcal{F})$ is mixed of weights $\geq n + i$. □
Proof: Use Poincare duality (6.4.8.10), we know $H^{2d-n}_{c,\text{\acute{e}t}}(X, \mathcal{F}^\vee(d))$ is the Galois dual representation of $H^2_{\text{c,\acute{e}t}}(X, \mathcal{F})$, and $\mathcal{F}^\vee(d)$ is still a lisse sheaf pure of weight $-w - 2d$, thus Deligne’s purity theorem (13.12.6.1) shows that $H^{2d-n}_{c,\text{\acute{e}t}}(X, \mathcal{F}^\vee(d))$ has weight $\leq (-w - 2d) + (2d - n) = -w - n$, thus we are done. □

Cor. (13.12.6.3)[Weil’s Conjecture]. Let $X_0$ be a smooth separated algebraic $k$-scheme, and $\mathcal{F}_0$ is a lisse $\mathbb{Q}_\ell$-sheaf which is pure of weight $w$, then the image of $H^n_{c,\text{\acute{e}t}}(X, \mathcal{F})$ in $H^n_{\text{\acute{e}t}}(X, \mathcal{F})$ is pure of weight $w + n$.

Proof: The morphism $H^n_{c,\text{\acute{e}t}}(X, \mathcal{F}) \to H^n_{\text{\acute{e}t}}(X, \mathcal{F})$ defined in (6.4.5.6) is compatible with Frobenius, so from (13.12.6.2) we know the image has weights $\geq w + n$, so combined with Deligne’s purity theorem (13.12.6.1), we know it is pure of weight $w + n$. □

Cor. (13.12.6.4). If $f_0 : X_0 \to Y_0$ is a smooth proper map of schemes of f.t. and $\mathcal{F}_0$ is $\iota$-pure of weight $\beta$, then $R^i f_{0,*} \mathcal{F}_0$ is $\iota$-pure of weight $\beta + i$.

Proof: Use proper base change of (6.4.5.5) to reduce to the case of (13.12.6.3). Notice in the proper case, $Rf_* = Rf_!$. □

Cor. (13.12.6.5)[Riemann Hypothesis]. If $X_0$ is smooth proper $k$-scheme, then $H^n_{\text{\acute{e}t}}(X, \mathbb{Q}_\ell)$ is pure of weight $n$.

Reduction to Curve case

Prop. (13.12.6.6). Deligne’s purity theorem can be reduced to case that $X_0$ is a smooth geometrically connected affine curve $\subset \mathbb{A}^1_{k_0}$ and $\mathcal{F}_0$ a lisse $\mathbb{Q}_\ell$-sheaf.

Proof: We have the following Devissages for Deligne’s theorem:

- It is trivial in case $f_0$ is quasi-finite. This is because of (6.4.5.7), as the fiber has dimension 0.
- We can replace $X_0$ by an affine open $U_0 \subset X_0$ by Noetherian induction and excision sequence (6.4.5.5), which commutes with Frobenius action.
- If the conclusion is true for $g_0, h_0$, then it is true for $f_0 = g_0 \circ h_0$, this follows from the Leray spectral sequence (6.4.5.5), which is Frobenius equivariant by (6.4.2.26).
- We can replace $Y_0$ with an affine open $U_0 \subset Y_0$: If the image $f_0$ is not dense, then trivial, if it is dense, then choose any affine open $U_0$, then it suffices to prove for $f_0 : f^{-1}_0(U_0) \to Y_0$ by item 2, then then by item 3 it suffice to prove for $f_0 : f^{-1}_0(U_0) \to U_0$, because $U_0 \to Y_0$ is quasi-finite and use item 1.

Now we claim we can reduce to the case of $f_0 : X_0 \to Y_0$ surjective affine smooth with the fibers being geometrically irreducible curves: By devissage 2 and 4, we may assume $X_0, Y_0$ is affine, thus $f_0$ is affine. Take a generic point $\eta$ of $Y_0$, then $(X_0)_\eta \to \text{Spec} k(\eta)$ is affine hence by Noetherian normalization (4.2.4.22) there is a finite map $X_\eta \to \mathbb{A}^n_{k(\eta)}$, and this spread out to a finite morphism $f^{-1}_0(U_0) \to U_0$ for some affine open $U_0 \subset Y_0$ because $f_0$ is of f.t.. Then by Devissage 1 and 3 we are reduced to the case $A^1_{Y_0} \to Y_0$. Now by (6.4.7.9), there is an affine open $U_0 \subset A^1_{Y_0}$ that $\mathcal{F}_0|_{U_0}$ is lisse, so by Devissage 2 we may change $X_0$ to $U_0$.

That is we reduced to the case that $\mathcal{F}_0$ is lisse and $X_0$ is open in $A^1_{Y_0}$ so $f_0$ is smooth affine, in particular open (5.6.4.4), so we can replace $Y_0$ by $f(X_0)$ and assume $f_0$ is surjective. Then the fiber are all geometrically irreducible curves.

Then the assertion about weights are clear from proper base change (6.4.5.5) and the curve case.
For the $\nu$-mixedness, we may use (13.12.5.2) and (13.12.5.6) to reduce to showing that $R^i f_!$ maps $\nu$-real sheaf to $\nu$-real sheaf.

for a geometric point $\bar{x} \to x \to X_0$, let $C \to C_0$ be the fiber, which is affine irreducible, so $H^0_c(X, \mathcal{F}) = 0$ by Poincare duality (6.4.8.10) and Artin vanishing theorem (6.4.2.12), so

$$tL(C_0, \mathcal{G}_0, t) = \frac{t \det(1 - tF^*_X|H^1_c(C, \mathcal{G}|C))}{t \det(1 - tF^*_X|H^2_c(C, \mathcal{G}|C))}$$

by Grothendieck-Lefschetz formula (13.12.2.10). Now we can use Poincare duality and the definition that $\mathcal{G}_0$ is pure of weight $\beta$, we know $H^2_c(C, \mathcal{G}|C)$ is pure of weight $\beta + 2$, by (13.12.5.3). And $H^2_c(C, \mathcal{G}|C)$ has weights smaller than $\beta + 1$ by the curve case, so the two polynomial is coprime, and both has constant coefficient 1, which shows they are both real. And then by proper base change (6.4.5.5), this just says $R^i f_{0!*}\mathcal{G}_0$ is $\nu$-real.

**Third Reduction**

**Prop. (13.12.6.7).** If $X_0$ is a smooth geometrically connected affine curve $\subset \mathbb{A}^1_{\mathbb{F}_q}$ and $\mathcal{F}_0$ a lisse $\overline{\mathbb{Q}}_\ell$-sheaf, the Deligne’s purity theorem is true.

**Proof:** We have the following devissages:

- We only need to check for $H^1_c(X, \mathcal{F})$, because $H^0_c$ vanish by Poincare duality (6.4.8.10) and Artin vanishing theorem (6.4.2.12) and, $H^2_c(X, \mathcal{F})$ is dealt with in (13.12.5.3).

- We are free to pass to finite base change.

- We may assume $\mathcal{F}_0$ is geometrically irreducible: By (13.12.4.4), all the irreducible constituents of $\mathcal{F}_0$ are geometrically semisimple, so pass to a finite base change, we may assume that its irreducible filtration is just the geometric irreducible filtration, then because $H^0_c = 0$, $H^1_c$ is left exact.

- We can assume that $\mathcal{F}_0$ can be extended to a lisse sheaf on $\infty$. This is because we can choose a closed point and move it to $\infty$ by using Möbius transform, after a finite base change.

- We can assume $\mathcal{F}_0$ is not geometrically constant: if $\mathcal{F}_0 \cong \overline{\mathbb{Q}}_\ell$, then let $i : U_0 \to P^1_{\mathbb{F}_q}$ and $Z_0 = P^1_{\mathbb{F}_q} - U_0$, then there is a short exact sequence

$$0 \to j_0!(\overline{\mathbb{Q}}_\ell) \to j_*(\overline{\mathbb{Q}}_\ell) \to Q \to 0$$

where $Q$ is supported at $S$, so its higher compact cohomology vanish, and weights of $H^0(Q) = \prod_{s \in S}(j_0!(\mathcal{F}_0))_s$ is no more than the maximal weight of $\overline{\mathbb{Q}}_\ell$ on $X_0$, which is 0, by semicontinuity of weights for curves (13.12.3.12). And $j_*(\overline{\mathbb{Q}}_\ell)$ is also geometrically constant, thus its cohomology is Pic$(P^1)|[n] = 0$ by (6.4.8.2), so $H^1(P^1, j_0!(X_0))$ has weights zero.

The actual proof will use the following lemma (13.12.6.8). After that, notice by (13.12.8.8)

$$(T \psi(\mathcal{G}_0))_{\{0\}} = R\Gamma_c(\mathbb{A}^1, \mathcal{G})[1] = R\Gamma_c(U, \mathcal{F})[1] = H^1_c(U, \mathcal{F})$$

Then to understand the Frobenius eigenvalues of $H^1_c(U, \mathcal{F})$, it suffices to understand the weights of $T \psi(\mathcal{G}_0)$, i.e.

$$w(T \psi(\mathcal{G}_0)) \leq w + 1$$
Then we use (13.12.3.18), notice the condition is satisfied by lemma (13.12.6.8), so \( w(T_\psi(G_0)) = ||T_\psi(G_0)|| \) and also \( w(G_0) = ||G_0|| \) for the same reason as \( H_0^0(\mathbb{A}^1, G) = H_0^0(U, F) = 0 \) by Poincaré duality. Now (13.12.8.12) gives the result.

\[ \square \]

Lemma (13.12.6.8) [Key Assertions of Weil Proof]. If \( G_0 = j_0! (F_0) \) where \( j_0 : U_0 \hookrightarrow A^1_{\mathbb{F}_q} \), \( \psi : \mathbb{F}_q \to \overline{\mathbb{Q}}_\ell \) is a fixed non-trivial additive character, then

- \( T_\psi(G_0) \) is a sheaf placed at degree 0.
- \( H^0_\psi(\mathbb{A}^1, T_\psi(G_0)) = 0. \)
- \( T_\psi(G_0) \) is \( \iota \)-mixed.

**Proof:**

1. By (13.12.8.8), we need to show \( H^i(\mathbb{A}^1, G_0 \otimes \mathcal{L}(\psi)) = 0 \) for \( i \neq 1 \), and this is equivalent to

\[
H^i(\mathbb{A}^1, j_! F \otimes \mathcal{L}(\psi)) = H^i(U, F \otimes \mathcal{L}(\psi)) = 0.
\]

Notice by vanishing result proper-pushforward-to-direct-image-sheafomqsk, only need to show \( i = 0, i = 2, i = 0 \) case is done by Poincaré duality (6.4.8.10) and Artin vanishing (6.4.2.12) because it is smooth and \( F \) is lisse.

\[
H^2_\psi(G_0 \otimes \mathcal{L}(\psi)) = V_{\rho \otimes \chi_a \mid \pi_1(U, \overline{x})}(-1) \text{ by (13.12.5.3), and } \rho \otimes \chi_a \text{ irreducible as } \rho \text{ does, so if } V_{\rho \otimes \chi_a \mid \pi_1(U, \overline{x})} \neq 0, \text{ then } \rho \otimes \psi_a \text{ is trivial representation. Then } G = \mathcal{L}_{\psi-a} \text{ on } \mathbb{P}^1_{\overline{F}} \text{ as an étale sheaf on } A^1 \cup \{ \infty \} = \mathbb{P}^1 \text{ by our reduction, so we have the character } \psi_{-a} \text{ factors through } \pi_1(\mathbb{P}^1, \overline{x}), \text{ i.e.}
\]

\[
\pi_1(\mathbb{A}^1, \overline{x}) \to \pi_1(\mathbb{P}^1, \overline{x}) = 0
\]

But this is in contradiction with the fact the Artin-Schreier cover is geometrically irreducible?.

2. Denote \( T_\psi(G_0) = \mathcal{K}_0 \), then by (13.12.8.7) and Fourier inversion (13.12.8.10):

\[
H^0_\psi(\mathbb{A}^1, \mathcal{K}) = \mathcal{H}^{-1}((T_\psi^{-1} \circ j_0! F_0)_0) = H^{-1}(T_\psi^{-1} \circ j_0! F_0)_0 = H^{-1}(j_0! F_0(-1))_0 = 0
\]

because \( F_0 \) is placed at degree 0.

3. To show \( \iota \)-mixed, the only thing we can do it show it is embedded in a \( \iota \)-real sheaf: Consider the \( \iota \)-real sheaf

\[
\mathcal{H}_0 = \text{pr}_2^*(j_0! F_0) \otimes m^*(\mathcal{L}(\psi)) \oplus \text{pr}_2^*(j_0! F'_0) \otimes m^*(\mathcal{L}(\psi^{-1}))(-w)
\]

Then

\[
(R^i \pi_1^!(H_0))_x = H^i(\{ \overline{x} \} \times A^1, H_0) = H^i(j_0! F_0 \otimes \mathcal{L}(\psi_x)) \oplus H^i(j_0! F'_0 \otimes \mathcal{L}(\psi_x^{-1}))(-w)
\]

which we proved to vanish for \( i \neq 1 \). So using Poincaré duality on \( \{ \overline{x} \} \times A^1 \),

\[
\det(1 - t F^d_x |(R^i \pi_1^!(H_0))_x) = \det(1 - t F_X |H^i_1(\{ \overline{x} \} \times A^1, H_0|_{\{ \overline{x} \} \times A^1}) = \prod_{y \in \mathbb{F}_q^n} \det(1 - t F^d_y |(H_0)_{(x,y)})^{-1}
\]

which is real, so by (13.12.5.5), the direct summand \( T_\psi(G_0) \) is \( \iota \)-mixed. \( \square \)

**Remark (13.12.6.9).** If we use the machinery of perverse sheaf and show that Fourier transform commutes preserves perversity, then item 1, 2 will be a direct consequence, Cf. [Bhatt notes, P39]. In fact, this is just the bigger picture, given in [Weil conjectures Perverse Sheaves and \( l \)-adic Fourier Transform Kiehl/Weissauer].
7 Semisimplicity and Hard Lefschetz

Prop. (13.12.7.1)[Semisimplicity Theorem]. If \(X_0\) is smooth and \(\mathcal{F}_0\) is a lisse and \(\ell\)-pure \(\overline{\mathbb{Q}}_\ell\)-sheaf, then \(\mathcal{F}_0\) is semisimple, thus geometrically semisimple by (13.12.4.4).

Proof: Let \(\mathcal{F}'\) be the sum of irreducible lisse subsheaves of \(\mathcal{F}\), then it is the largest semisimple subsheaf of \(\mathcal{F}_0\). It is stable under \(G(F_q) \triangleleft F_q\), thus can be descended to a lisse subsheaf \(\mathcal{F}'_0\) of \(\mathcal{F}_0\), and let \(\mathcal{F}'' = \mathcal{F}_0 / \mathcal{F}'_0\), we want to show the exact sequence

\[
0 \to \mathcal{F}'_0 \to \mathcal{F}_0 \to \mathcal{F}''_0 \to 0
\]

splits geometrically. Notice this exact sequence defines an element in \(\text{Ext}^1_X(\mathcal{F}'', \mathcal{F}') = H^1(X, (\mathcal{F}'')^\vee \otimes \mathcal{F}')\). \(\mathcal{F}_0\) is pure, hence so does \((\mathcal{F}''_0)^\vee \otimes \mathcal{F}'_0\), thus \(H^1(X, (\mathcal{F}'')^\vee \otimes \mathcal{F}')\) is \(\ell\)-mixed of weights \(\geq 1\). But the exact sequence is compatible with Frobenius action, thus it defines a Frobenius fixed element, which then must vanish. \(\Box\)

Cor. (13.12.7.2). If \(f : X \to Y\) is proper between smooth sheaves, then the sheaves \(R^i f_* \overline{\mathbb{Q}}_\ell\) are semisimple.

Prop. (13.12.7.3)[Hard-Lefschetz]. Cf.[Bhatt P42].

8 Fourier Transformation

Sheaf to Functions Correspondence

Def. (13.12.8.1)[Sheaf to Functions Correspondence]. For a complex \(K_0 \in D^b_{\text{cons}}(X_0, \overline{\mathbb{Q}}_\ell)\), we can associate a function

\[
f^{K_0} : X_0(F_q^n) \to \overline{\mathbb{Q}}_\ell : x \mapsto \sum_i (-1)^i \text{tr}(F_x \otimes dx)(H^i(K_0))
\]

Prop. (13.12.8.2). We can use Grothendieck formula for a constructible sheaf (13.12.2.6) to relate the function \(f^{K_0}\) to the compact cohomologies of \(H^i K_0\), and we can translate many know theorems:

- \(f^{f^K_0} = f^{K_0} \circ f\).
- \(f^{K_0} \cdot f^{T_0} = f^{K_0 \otimes^L T_0}\).
- (Base Change)(6.4.5.5) asserts that given a Cartesian diagram

\[
\begin{array}{ccc}
X' & \xrightarrow{g'} & X \\
\downarrow f' & & \downarrow f \\
Y' & \xrightarrow{g} & Y
\end{array}
\]

then it says in case \(Y'\) is a closed point of \(Y\),

\[
f^{Rf_{/K_0}}(y) = \sum_{x \in \pi^{-1}(F_q^n)} f^{K_0}(x)
\]

where \(y \in \pi^{-1}(F_q^n)\), and more generally

\[
\sum_{x' \in X_{g'}(Y')} f^{K_0}(g'(x')) = \sum_{x \in X_{g}(Y')} f^{K_0}(x)
\]
• The projection formula (6.4.5.8) turns out to say something trivial:

\[
\sum_{x \in X_y} (f^{K_0}(f(x)) \cdot f^{T_0}(x)) = f^{K_0}(y) \cdot (\sum_{x \in X_y} f^{T_0}(x))
\]

Artin-Schreier Sheaves

**Prop. (13.12.8.3)** [Characters]. Any character \( \psi : \mathbb{F}_q \rightarrow \overline{\mathbb{Q}}_\ell^\times \) can be extended to \( \mathbb{F}_{q^n} \) by

\[
\mathbb{F}_{q^n} \xrightarrow{\text{tr}} \mathbb{F}_q \xrightarrow{\psi} \overline{\mathbb{Q}}_\ell^\times,
\]

also denoted by \( \psi \).

**Prop. (13.12.8.4)** [Artin-Schreier Sheaf]. Let \( y^{q^n} - y - x \in \mathbb{A}_0^1 \) be the finite Galois cover of \( \mathbb{A}_0^1 \) via \( x \) coordinates, with the Galois group isomorphic to \( \mathbb{F}_q \) with \( 1 \mapsto (x \mapsto x + 1) \). Then we get a surjection \( \pi_1(\mathbb{A}_0^1, \mathfrak{p}) \rightarrow \mathbb{F}_q \), when composed with \( \psi \), we get a rank \( 1 \) étale sheaf \( \mathcal{L}_0(\psi) \) called the Artin-Schreier sheaf on \( \mathbb{A}_0^1 \).

**Prop. (13.12.8.5).** \( f^{\mathcal{L}_0}(\psi)(x) = \psi(-x) \).

**Proof:** If \( k(x) = \mathbb{F}_{q^n} \), then consider the arithmetic Frobenius \( \sigma : (x, y) \mapsto (x^{q^n}, y^{q^n}) \), then if \( y^{q^n} - y = x \), then we have

\[
y^q = y + x, \quad y^{q^2} = y^q + x^q = y + x + x^q + x, \ldots, \quad y^{q^n} = y + x + x^q + \ldots + x^{q-1} = y + \text{tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x)
\]

So in the correspondence (13.12.8.4), we know \( F_\mathfrak{p} \) acts on \( \mathcal{L}_\psi \) by multiplication by \( \psi(\text{tr}_{\mathbb{F}_{q^n}/\mathbb{F}_q}(x)) = \psi(x) \), so the geometric Frobenius acts by \( \psi(-x) \).

**Def. (13.12.8.6)** [Deligne-Fourier Transform]. Consider the multiplication map \( \mathbb{A}_0^1 \times \mathbb{A}_0^1 \rightarrow \mathbb{A}_0^1 \), let the sheaf \( \mathcal{L}(\psi) \) be placed at \( \mathbb{A}_0 \), and \( K_0 \in D^b_c(\mathbb{A}_0^1, \overline{\mathbb{Q}}_\ell) \) be placed at \( \mathbb{A}_0^1 \), then define the Deligne-Fourier transform

\[
T_\psi : D^b_c(\mathbb{A}_0^1, \overline{\mathbb{Q}}_\ell) \rightarrow D^b_c(\mathbb{A}_0^1, \overline{\mathbb{Q}}_\ell) : K_0 \mapsto R\pi_1^\ast(\mathbb{A}_0^1, \overline{\mathbb{Q}}_\ell) \otimes^L \mathcal{L}_0(\psi)[1]
\]

**Lemma (13.12.8.7).** We have \( f^{T_\psi K_0}(x) = -\sum_{y \in \mathbb{F}_{q^n}} f^{K_0}(y) \psi(-xy) \) for any \( x \in \mathbb{F}_{q^n} \).

**Proof:** Use (13.12.8.2), we have

\[
f^{T_\psi K_0}(x) = \sum_{y \in \mathbb{F}_{q^n}} f^{(\mathbb{A}_0^1, \overline{\mathbb{Q}}_\ell)}(\mathbb{A}_0^1, \mathbb{F}_q) \big( (x, y) \big)
\]

\[
= - \sum_{y \in \mathbb{F}_{q^n}} f^{\mathbb{A}_0^1}((x, y)) \cdot f^{\mathcal{L}_0}(\mathbb{A}_0^1, \mathbb{F}_q)((x, y))
\]

\[
= - \sum_{y \in \mathbb{F}_{q^n}} f^{K_0}(y) \psi(-xy).
\]

**Prop. (13.12.8.8).** Let \( a \) be a geometric point of \( \mathbb{A}_0^1 \), then

\[
(T_\psi(K_0))_a = R\Gamma_c(K \otimes^L \mathcal{L}_0(\psi_a))[1]
\]

where \( \psi_a : \mathbb{F}_{q^n} \rightarrow \overline{\mathbb{Q}}_\ell^\times \) maps \( x \mapsto \psi(ax) \). In particular, \( H^i((T_\psi(K_0))_0) = H^i_{\partial, c}(\mathbb{A}_0^1, K) \), so we placed the complex into a family of deformations.
Proof: By base change (6.4.5.5),
\[(T_\psi(K_0))_a = R\Gamma_c((pr_2^*K_0 \otimes Lm^*L_0(\psi))|_{\{a\} \times \mathbb{A}^1})[1] = R\Gamma_c(K \otimes L(\psi_a))[1].\]

\[\square\]

Lemma (13.12.8.9). If \(\delta_0 = i_0_{\ast}\mathcal{O}_\ell\) be the skyscraper sheaf, where \(i_0: \{0\} \hookrightarrow \mathbb{A}^1\), then
\[T_\psi(\mathcal{O}_\ell[1]) = \delta_0(-1).\]

Proof: For the Artin-Schreier cover \(P: x \mapsto x^q - x\), we have
\[P_{\ast}\mathcal{O}_\ell \cong \oplus_{x \in \mathbb{F}_q} L(\psi x)?\]
and \(P\) is finite thus proper and \(P_{\ast}\) is exact (6.4.1.18), so using the Leray spectral sequence (6.4.5.5), we can calculate
\[H^1_c(A^1, L(\psi x)) = 0 = H^2_c(A^1, \mathcal{O}_\ell)[1]\]
(13.12.5.3)
So
\[(R_{\pi_1}^1(m^*L_0(\psi)[1])[1])_{(x)} = R\Gamma_c(L(\psi x))[2] = \delta_0(-1).\]

\[\square\]

Prop. (13.12.8.10) [Fourier Inversion]. \(T_{\psi^{-1}}T_\psi K_0 = K_0(-1)\).

Proof: Consider
\[
\begin{array}{ccc}
A^1_0 \times A^1_0 \times A^1_0 & \xrightarrow{pr_{23}} & A^1_0 \times A^1_0 \xrightarrow{pr_2} A^1_0 \\
\downarrow{pr_{12}} & & \downarrow{pr_1} \\
A^1_0 \times A^1_0 & \xrightarrow{pr_1} & A^1_0 \\
\downarrow{pr_1} & & \\
A^1_0
\end{array}
\]
And we will use the following Cartesian diagrams:
\[
\begin{array}{ccc}
A^3_0 & \xrightarrow{\alpha(x,y,z) \mapsto (y,z-x)} & A^2_0 \\
\downarrow{\pi^{13}} & & \downarrow{pr_2}, \\
A^2_0 & \xrightarrow{\beta(x,z) \mapsto z-x} & A^1_0 \\
\end{array}
\]
Then
\[T_{\psi^{-1}}T_\psi K_0 \quad (T_{\psi^{-1}}T_\psi f)(x)\]
\[= R_{\pi_1}^1(pr_2^*R_{\pi_1}^1(pr_2^*K_0 \otimes m^*L_0(\psi)) \otimes m^*L_0(\psi^{-1}))[2] = \sum_y \left(\sum_z f(z)\psi(-yz)\psi(xy)\right)\]
By base change (6.4.5.5):
\[= R_{\pi_1}^1(R_{\pi_1}^{12}pr_{23}^*(pr_2^*K_0 \otimes m^*L_0(\psi)) \otimes m^*L_0(\psi^{-1}))[2]\]
By projection formula (6.4.5.5):
\[ = R\pi_1^1 R\pi_1^{12} (\text{pr}_{23}^* K_0 \otimes m^* L_0(\psi) \otimes \text{pr}_{12}^* m^* L_0(\psi^{-1}))[2] \]

Combine the character:
\[ = \sum_y \sum_z f(z) \psi(-yz) \psi(xy) \]

Change order of summation:
\[ = \sum_z \sum_y f(z) \psi(-y(z - x)) \]

By base change:
\[ = \sum_z f(z) \sum_y \psi(-y(z - x)) \]

Prop. (13.12.8.11) [Plancherel Formula].
\[ ||f^{T_\psi(K_0)}||_n = q^{n/2} ||f^{K_0}||_n. \]

Proof: By definition and using (13.12.8.7),
\[ ||f^{T_\psi(K_0)}||_n^2 = \sum_{x \in F_q^n} f^{T_\psi(K_0)}(x) f^{T_\psi(K_0)}(x) \]
\[ = \sum_{x,y,z} f^{K_0}(y) f^{K_0}(z) \psi(-xy) \psi(xz) \]
\[ = q^n \sum_{z=y} f^{K_0}(y) f^{K_0}(z) \]
\[ = q^n (f, f)_n \]

Cor. (13.12.8.12). Notice by the definition of norm of a Weil sheaf \( G_0 \), we have
\[ ||T_\psi(K_0)|| \leq ||K_0|| + 1 \]
9 Integrality Problems

Def. (13.12.9.1) [Integral Sheaves]. Let $X_0$ be a separated algebraic scheme over $k$ and $\mathcal{F}_0$ a lisse constructible sheaf on $X_0$, then $\mathcal{F}$ is called an integral sheaf if for all $x_0 \in X_0$, all the eigenvalues of $F_\pi^*$ acting on $\mathcal{F}_\pi$ are algebraic integers.

Prop. (13.12.9.2) [Deligne]. If $\mathcal{F}$ is an integral lisse sheaf on $X_0$, then all $H^{\text{\acute{e}t},c}_i(X, \mathcal{F})$ are also integral.

Proof: Cf. [Weil I Proof, P21].

Cor. (13.12.9.3). All eigenvalues of $H^i(X, \mathcal{F})$ are algebraic integers.
13.13 Rational Points on Abelian Varieties

Main references are [Sta], [Abelian Varieties notes Conrad], [Mil08], [B-G06], [Abelian Variety van der Geer], [BLR90], [Sil16] and [Sil99], [Sil11], http://www-personal.umich.edu/~asnowden/teaching/2013/679/index.html.

1 Mordell-Weil Theorem

Prop.(13.13.1.1)[Local Chevalley-Weil Theorem for Abelian Varieties]. Let $S$ be a Dedekind scheme with function field $F$, Let $A$ be an Abelian variety over $F$ and $m \in \mathbb{Z} \cap F^*$. Let $s \in S$ be a closed point s.t. $A$ has good reduction over $\mathcal{O}_{S,s}$ and $m \neq 0 \in \kappa(s)$, then for any $P \in A(F)$, the extension $\kappa(P)/\kappa([m]P)$ is unramified at all places over $v$.

Proof: By base change, we may assume $Q = [m]P$ is a rational point. Let $w$ be a place of $\kappa(P)$ that $w|v$ with valuation ring $R_w$. As $A$ has good reduction in $v$, $A$ extends to an Abelian scheme $\mathcal{A}$ over $\mathcal{O}_{S,s}$, then the valuation criterion of properness shows $P$ extends to a $R_w$-valued point of $\mathcal{A}$. Now the theorem follows from (13.5.6.14) and (5.6.5.16).

Cor.(13.13.1.2). Let $F$ be a global field, $X \in \text{AbVar}/F$ and $n \in \mathbb{Z} \cap F^*$, $L = K(X[n](\mathcal{F}))$, i.e. the composite of all fields in $\mathcal{F}$ obtained by adjoining $[n]^{-1}x, x \in X(F)$, then $L$ is a finite field extension of $F$.

Proof: This follows from the proposition and (12.2.4.21).

Lemma(13.13.1.3)[Weak Mordell-Weil Theorem]. Let $F$ be a global field and $X$ be an Abelian variety over $K$, then for $n \in \mathbb{Z} \cap F^*$, $X(F)/nX(F)$ is finite.

Proof: This follows from the finiteness of the Selmer group (13.5.11.8) and (13.5.11.6).

Prop.(13.13.1.4)[Mordell-Weil Theorem]. Let $F$ be a global field, then the group $X(F)$ of rational points of an Abelian variety $X$ is f.g.

Proof: Because of (13.13.1.3) and (13.5.12.2), this follows from (2.1.4.15) applied to $M = X(K')$ and the symmetric bilinear form on $X(K')$ given by (13.5.12.2).

Remark(13.13.1.5)[Computability]. The difficulty of computing $X(F)$ lies entirely at computing $X(F)/nX(F)$ for some $n$, for which, see (13.5.11.7).

Cor.(13.13.1.6)[Rank]. $X(F) \cong \mathbb{Z}^r \oplus X(F)_{\text{tor}}$, where $X(F)_{\text{tor}}$ is a finite group, and $r$ is called the rank of $X$.

Cor.(13.13.1.7)[Isogenous Varieties have the same Rank]. Let $F$ be a global field and $X, X' \in \text{AbVar}/F$ are isogenous, then $\text{rank}(X) = \text{rank}(X')$. In particular, $\text{rank}(X) = \text{rank}(\hat{X})$.

Proof: The isogeny implies $X(F)/X(F)_{\text{tor}} \rightarrow \hat{X}(F)/\hat{X}(F)_{\text{tor}}$ is injective. Thus $\text{rank}(X) \leq \text{rank}(\hat{X})$. The converse follows from (13.5.6.4).
2 Lang-Néron Theorem

Main references are [Con06].

Def. (13.13.2.1) [Regular Extensions]. A field extension $K/k$ is called primary if $k$ is separably closed in $K$. It is called regular if it is separable and primary.

Prop. (13.13.2.2). Let $K/k$ be a primary extension, then
- If $A \in AbVar/K$, then any Abelian subvariety of $A_K$ is defined over $k$.
- If $A, B \in AbVar/K$, then any homomorphism $A_K \to B_K$ is defined over $k$.

Proof: □

Prop. (13.13.2.3) [K/k-Images and K/k-Traces]. For a field extension $K/k$, the $K/k$-image is a functor $\text{Im}_{K/k} : AbVar/K \to AbVar/k$ left adjoint to the base change functor, and $K/k$-trace is a functor $\text{tr}_{K/k} : AbVar/K \to AbVar/k$ right adjoint to the base change functor.

Then for $K/k$ primary, $\text{Im}_{K/k}$ and $\text{tr}_{K/k}$ exist, and are resp. left and right inverses to the base change functor. Also there is a natural isomorphism

$$\text{Im}_{K/k}(A) \cong \text{tr}_{K/k}(A).$$

The adjunction maps are denoted by

$$\tau_{A,K/k} : \text{tr}_{K/k} A \to A, \quad \lambda_{A,K/k} : A \to \text{Im}_{K/k} A.$$

Proof: It suffices to prove for $\text{Im}_{K/k}$, and $\text{tr}_{K/k}$ follows by double duality theorem (13.5.4.16). For this, Cf. [Con06]P16?. □

Prop. (13.13.2.4). Let $K/k$ be a primary extension and $A \in AbVar/K$, the unique map $\text{tr}_{K/k} A \to \text{Im}_{K/k} A$ descending $\lambda_{A,K/k} \circ \tau_{A,K/k}$ is an isogeny.

Proof: Cf. [Con06]P22?. □

Prop. (13.13.2.5). Let $K/k$ be a regular extension, then for any $A \in AbVar/K$, the finite group $\ker(\tau_{A,K/k})$ is connected and coconnected. In particular, $\tau_{A,K/k}(K) : \text{tr}_{K/k}(A)(K) \to A(K)$ is injective.

Prop. (13.13.2.6) [Lang-Néron]. Let $K/k$ be a f.g. regular extension, then $A(K)/\text{tr}_{K/k}(A)(k)$ is a f.g. Abelian group.

Proof: Cf. [Con06]P23?. □

Prop. (13.13.2.7) [Grothendieck]. Let $K$ be an alg. closed field with prime field $k$, then any Abelian variety of CM-type over $K$ is isogenous to an Abelian variety defined over a finite extension of $k$.

Proof: Cf. [Oort, The isogeny class of a CM-type abelian variety is defined over a finite extension of the prime field]. □
3 Elliptic Curve Case

Prop. (13.13.3.1) [Controlling Torsion Points]. Let $K$ be a number field, let $E$ be given by a Weierstrass equation

$$E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \in \mathcal{O}_K[X,Y].$$

Let $P = (x_0, y_0) \in E(K)$ be a torsion point of exact order $m$, then

- If $m$ is not a $p$-power, then $x_0, y_0 \in \mathcal{O}_K$.
- If $m = p^n$, then for any place $v$ of $K$, $v(x) \geq -2\lfloor \frac{v(p)}{p^n - p^{n-1}} \rfloor$, $v(y) \geq -3\lfloor \frac{v(p)}{p^n - p^{n-1}} \rfloor$.

Proof: This follows by base change $E$ to each $\mathcal{O}_{K,v}$ and use $(13.8.4.21)$. □

Cor. (13.13.3.2) [Integrality of Torsion Points in $\mathbb{Q}$]. Let $E \in \mathcal{Ell}/\mathbb{Q}$ and $P = (x_0, y_0) \in E(\mathbb{Q})$ a torsion point of exact order $m$, then if $m$ is not a $p$-power, $x_0, y_0 \in \mathbb{Z}$. If $m = p^n$, then $\lfloor \frac{v(p)}{p^n - p^{n-1}} \rfloor = 0$ unless $p = 2$ and $n = 1$. Thus $x_0 \in \frac{1}{2}\mathbb{Z}, x_0 \in \frac{1}{8}\mathbb{Z}$, and if $m \geq 3$, $x_0, y_0 \in \mathbb{Z}$.

The former case can occur, for example

$$E : y^2 + xy = x^3 + 4x + 1, \quad (-\frac{1}{4}, \frac{1}{8}) \in E(\mathbb{Q})[2].$$

Prop. (13.13.3.3) [Nagell–Lutz]. Let $F$ be a number field and $E \in \mathcal{Ell}/F$ be given by a Weierstrass equation

$$E : y^2 = x^3 + Ax + B \in \mathbb{Z}[x,y],$$

Let $P = (x_0, y_0) \in E(\mathbb{Q})_{tor}$, then

- $x_0, y_0 \in \mathbb{Z}$.
- Either $y_0 = 0$, i.e. $[2](P) = O$ or $y_0^2$ divides $4A^3 + 27B^2$.

Proof: 1: Let $P$ has exact order $m$. If $m = 2$, then $y_0 = 0$, and then $x_0 \in \mathbb{Z}$ as it is integral over $\mathbb{Z}$. If $m \geq 2$, the results follows from $(13.3.1.3)$.

2: Suppose $[2](P) = (x_1, y_1) \neq O$, then $y_0 \neq 0$, and $x_0, y_0, x_1 \in \mathbb{Z}$. Now $(13.8.1.8)$ shows $x_1 = \varphi(x_0)/4\psi(x_0)$ where

$$\varphi(X) = X^4 - 4AX^2 - 8BX + A^2, \quad \psi(X) = X^3 + AX + B.$$  And they satisfy a polynomial equation

$$f(X)\varphi(X) - g(X)\psi(X) = 4A^2 + 27B^2$$

where $f(X) = 3X^2 + 4A, g(X) = 3X^3 - 5AX - 27B$. Then because $y_0^2 = x_0^3 + Ax_0 + B$, we get

$$y_0^2(4f(x_0)x_1 - g(x_0)) = 4A^2 + 27B^2.$$ □

Prop. (13.13.3.4). If $p \in \mathbb{P}$ and $E \in \mathcal{Ell}/\mathbb{Q}$ has a rational torsion point of order $p$, then $E$ is isogenous to $E'/\mathbb{Q}$ with a rational point of order $p$ and $\mathbb{Q}(E'[p])$ is a ramified extension of $\mathbb{Q}(\mu_p)$.

Proof: Cf. [Elliptic Curves, Group Schemes and Mazur’s Theorem, P26]? □
Prop. (13.13.3.5). If $p > 13 \in \mathbb{P}$ and $E \in \operatorname{Ell}/\mathbb{Q}$ has a rational torsion point of order $p$, then $Q(E[p])$ is an unramified extension of $Q(\mu_p)$.

Proof: Cf.[Elliptic Curves, Group Schemes and Mazur’s Theorem, P29]?.

□

Lemma (13.13.3.6) [Mazur-Tate]. For $E \in \operatorname{Ell}/\mathbb{Q}$ and $p > 7 \in \mathbb{P}$ and $p \neq 13$, $E$ doesn’t contain a rational torsion point of order $p$.


Lemma (13.13.3.7). For $E \in \operatorname{Ell}/\mathbb{Q}$, $E$ doesn’t contain a rational torsion point of order 13.


Lemma (13.13.3.8) [Kubert]. If $E \in \operatorname{Ell}/\mathbb{Q}$, then
- $E$ doesn’t contain a rational torsion point of exact order $N$ where $N \in \{14, 15, 16, 18, 20, 21, 24, 25, 27, 35, 49\}$.
- $E(\mathbb{Q})_{\text{tor}}$ doesn’t contain a subgroup isomorphic to $\mathbb{Z}/(2) \times \mathbb{Z}/(10)$ or $\mathbb{Z}/(2) \times \mathbb{Z}/(12)$.

Proof: Cf.[Kubert. Universal bounds on the torsion of elliptic curves.]?

Firstly, notice for $N \in \{11, 14, 15, 17, 19, 20, 21, 24, 27, 32, 36, 49\}$, $X_0(N)$ has genus 1(15.11.4.19). And by taking the cusp as the origin, $X_0(N)$ is an elliptic curve. Then Kubert finds that $\operatorname{rank}(X_0(N)) = 0$, and can find all the rational points. Only for $N = 21$ or $N = 27$ there are non-cusp rational points. So it suffices to show that for $X_0(21)$ and $X_0(27)$, the quadratic twists of the elliptic curves corresponding to the rational non-cusp points of $X_0(N)$ don’t have rational 21 torsion-points.

For $N = 21$, the non-cusp rational points of $X_0(N)$ are given by quadratic twists of

\[
\begin{align*}
y^2 &= x^3 + 45x - 18 \\
y^2 &= x^3 - 75x - 262 \\
y^2 &= x^3 - 1515x - 46106 \\
y^2 &= x^3 - 17235x - 870894.
\end{align*}
\]

For $N = 27$, the non-cuspidal rational points of $X_0(N)$ are given by quadratic twists of

\[
y^2 + y = x^3 - 30x - 5.
\]

For the second case, let $P$ be a generator of $\mathbb{Z}/(2)$ and $Q$ a generator of $\mathbb{Z}/(10)$ or $\mathbb{Z}/(12)$, then the dual map $E/P \to E \to E/Q$ is a cyclic isogeny, thus corresponds to a rational point on $Y_0(20)$ or $Y_0(24)$, which in fact has no rational point.

For $N = 16$, ?
For $N = 18$, ?
For $N = 25$, ?

For $N = 35$, let $E = X_0(35)/w_5$, where $w_5$ is the Atkin-Lehner involution. Then $E$ is an elliptic curve, and $E(\mathbb{Q}) \cong \mathbb{Z}/(3)$. Then Kubert computed that the preimages of these points are cusps. □

Thm. (13.13.3.9) [Mazur]. For $E \in \operatorname{Ell}/\mathbb{Q}$, $E(\mathbb{Q})_{\text{tor}}$ can only be isomorphic to one of the following 15 groups:
• \( \mathbb{Z}/(n) \) for \( n \leq 10 \) or \( n = 12 \),
• \( \mathbb{Z}/(2) \oplus \mathbb{Z}/(2n) \) for \( n \leq 4 \).

Moreover, each of these groups occur, by (13.13.3.11).

**Proof:** This follows from (13.13.3.6)(13.13.3.7) and (13.13.3.8). Notice the existence of elliptic curves with these torsion groups can also be shown using modular curves, as they parametrize elliptic curves with torsion points. \( \square \)

**Thm. (13.13.3.10) [Uniform Bound of Torsion Groups, Merel].** For any \( d \in \mathbb{Z}_+ \) there is a constant \( N(d) \) s.t. for any number field \( F/\mathbb{Q} \) of degree \( d \) and all elliptic curves \( E \) over \( K \),

\[ \#E(F)_{\text{tor}} \leq N(d). \]

**Proof:** \( \square \)

**Prop. (13.13.3.11) [Bounding Torsion Points].** The proposition (13.8.4.20) is useful in controlling torsion points of \( E \), for example: If \( E/\mathbb{Q} \) is an elliptic curve with Weierstrass equation

- \( E : y^2 + y = x^3 - x + 1 \), then \( \Delta = -13 \cdot 47 \), so \( E \) has good reduction modulo 2. But it can be calculated that \( \tilde{E}(\mathbb{F}_2) = \tilde{O}, E(\mathbb{Q})[2] = O, \) thus \( E(\mathbb{Q})_{\text{tor}} = O \).
- \( E : y^2 = x^3 + 3 \), then \( \Delta = -2^4 \cdot 3^5 \), so \( E \) has good reduction modulo \( p \) for \( p \geq 5 \). But it can be calculated that \( \#\tilde{E}(\mathbb{F}_5) = 6, \#\tilde{E}(\mathbb{F}_7) = 13 \), so \( E(\mathbb{Q})[p] = O \) for any prime \( p \), and \( E(\mathbb{Q})_{\text{tor}} = O \). In particular, \((1, 2) \in E(\mathbb{Q})\) has infinite order.
- \( E : y^2 = x^3 + x \), then \( \Delta = -2^6 \), so \( E \) has good reduction modulo \( p \) for \( p \geq 3 \). But it can be calculated that \( \tilde{E}(\mathbb{F}_3) \cong \mathbb{Z}/(4), \tilde{E}(\mathbb{F}_5) \cong \mathbb{Z}/(2) \times \mathbb{Z}/(2) \), thus \( E(\mathbb{Q})_{\text{tor}} \cong 0 \) or \( \mathbb{Z}/(2) \). The latter case is right, as \((0, 0) \in E(\mathbb{Q})\).
- \( E : y^2 = x^3 + 2 \).
- \( E : y^2 = x^3 + 8 \).
- \( E : y^2 = x^3 + 4 \).
- \( E : y^2 = x^3 + 4x \).
- \( E : y^2 = x^3 - x^2 \).
- \( E : y^2 = x^3 + 1 \).
- \( E : y^2 = x^3 - 43x + 166 \), then \( \Delta = -2^{19} \cdot 13 \), thus \( E \) has good reduction modulo 3,5. But it can be calculated that \( \#\tilde{E}(\mathbb{F}_3) = 7, \#\tilde{E}(\mathbb{F}_5) = 7 \), thus \( E(\mathbb{Q})_{\text{tor}} \cong 0 \) or \( \mathbb{Z}/(7) \). By (13.13.3.3), for any torsion point \((x, y) \in E(\mathbb{Q})\), we can find rational points

\[ \{(3, \pm 8), \ (−5, \pm 16), \ (11, \pm 32)\}. \]

And using doubling formula (13.8.1.8) for \( P = (3, 8) \),

\[ x(2)(P) = −5, \ x([4](P)) = 11, \ x([8](P)) = 3. \]

Thus \( P \) must have order 7, and \( E(\mathbb{Q})_{\text{tor}} \cong \mathbb{Z}/(7) \).

- \( E : y^2 + 7xy = x^3 + 16x \).
- \( E : y^2 + xy + y = x^3 - x^2 - 14x + 29. \)
• $E : y^2 + xy = x^3 - 45x + 81$.
• $E : y^2 + 43xy - 210y = x^3 - 210x^2$.
• $E : y^2 = x^3 - 4x$.
• $E : y^2 = x^3 + 2x^2 - 3x$.
• $E : y^2 + 5xy - 6y = x^3 - 3x^2$.
• $E : y^2 + 17xy - 120y = x^3 - 60x^2$. 
13.14 Shimura Varieties

Main references are [Lan20], [Mil17b], [Mil11], http://virtualmath1.stanford.edu/~conrad/shimsem/.

Def. (13.14.0.1) [Special Subvarieties].

 Conj. (13.14.0.2) [André-Oort]. Let $S$ be a Shimura variety. Let $V \subset S$ be a subvariety, then there are only f.m. maximal special subvarieties contained in $V$.

Proof: □

1 Connected Shimura Varieties

Def. (13.14.1.1) [Connected Shimura Data]. A connected Shimura datum is a pair $(G, D)$ where $G$ is a semisimple algebraic group over $\mathbb{Q}$ and $D$ a $G^{\text{ad}}(\mathbb{R})^{+}$-conjugacy classes of homomorphisms $u: U(1) \to G^{\text{ad}}_{\mathbb{R}}$ satisfying

SU1: Only $z, 1, z^{-1}$ appear in the character of the complex representation $\text{Ad} \circ u : U(1) \to \text{Lie}(G^{\text{ad}})_{\mathbb{C}}$.

SU2: $\text{ad}(u(-1))$ is a Cartan involution on $G^{\text{ad}}$.?

SU3: $G^{\text{ad}}$ has no $\mathbb{Q}$-factor $H$ s.t. $H(\mathbb{R})$ is compact.

Prop. (13.14.1.2). Let $H$ be an adjoint real Lie group and $u: U(1) \to H$ a homomorphism satisfying SU1, SU2, then the following are equivalent:

• $u(-1) = 1$.
• $u$ is trivial.
• $H$ is compact.

Proof: 1 $\iff$ 2: If $u(-1) = 1$, then $u$ factors through $U(1) \overset{2}{\to} U(1)$, so the characters $z, z^{-1}$ cannot occur in $\text{Ad} \circ u$. The converse is trivial.

1 $\to$ 3: by (7.3.6.19), $H$ is compact iff $\text{ad}(u(-1)) = 1$, which is equivalent to $u(-1) = 1$ as $H$ is adjoint. □

Prop. (13.14.1.3) [Equivalent Characterization of Connected Shimura Data]. A connected Shimura datum is equivalent to the following data:

• $G \in \mathbb{Alg}_0 / \mathbb{Q}$ semisimple of non-compact type.

• $D$ a Hermitian symmetric domain.

• an action of $G(\mathbb{R})^{+}$ on $D$ via a surjective homomorphism $G^{\text{ad}}(\mathbb{R})^{0} \to \text{Hol}(D)^{0}$ with compact kernel.

Proof: Cf. [Mil17b]P45.? □

Prop. (13.14.1.4). Let $(G, D)$ be a connected Shimura datum and $X$ be the $G^{\text{ad}}(\mathbb{R})$-conjugacy class of homomorphisms $S^{1} \to G_{\mathbb{R}}$ containing $D$, and $D$ is a connected component of $X$, with stabilizer $G^{\text{ad}}(\mathbb{R})^{0} \subset G^{\text{ad}}(\mathbb{R})$.

Proof: Cf. [Mil17b]P45. □
Def. (13.14.1.5) [Connected Shimura Varieties]. Let \((G,D)\) be a Shimura datum, then the map \(G^{\text{ad}}(\mathbb{R})^0 \to \text{Hol}(D)^0\) has compact kernel, so for any arithmetic \(\Gamma \subset G^{\text{ad}}(\mathbb{R})^0 \cap G^{\text{ad}}(\mathbb{Q})\), the image \(\Gamma\) is an arithmetic subgroup of \(\text{Hol}(D)^0\), thus we can apply Baily-Borel compactification (11.9.7.4) to get an algebraic structure on \(D(\Gamma) = \Gamma \setminus D\). Moreover, if \(\Gamma' \subset \Gamma \subset G^{\text{ad}}(\mathbb{R})^0 \cap G^{\text{ad}}(\mathbb{Q})\) satisfy \(\Gamma', \Gamma\) are torsion-free, then by Borel-theorem (11.9.7.5) to get a morphism \(D(\Gamma') \to D(\Gamma)\).

Then for any \(\Gamma \in G^{\text{ad}}(\mathbb{R})^0 \cap G^{\text{ad}}(\mathbb{Q})\) s.t. \(\Gamma\) is torsion-free, \(D(\Gamma)\) is called a connected Shimura variety relative to \((G,D)\). And the inverse image of these Shimura varieties are called the connected Shimura variety attached to \((G,D)\), denoted by \(\text{Sh}^0(G,D)\).

Prop. (13.14.1.6) [Galois Action on Shimura Varieties].

2 Shimura Varieties

3 Siegel Modular Varieties

Prop. (13.14.3.1) [Siegel Modular Varieties]. For \(k \in \text{Field}\), consider the functor

\[
\mathcal{M}^{g,d} : \text{Sch} / k \to \text{Set} : X \mapsto \{\text{Abelian schemes over } X \text{ with a polarization of degree } d\},
\]

then its Zariski shification \(\mathcal{M}^{g,d}_{\text{ét}}\) is representable by an algebraic variety \(\mathcal{M}^{g,d} / k\).

Proof:

Prop. (13.14.3.2) [Canonical Ample Divisor on \(\mathcal{M}^{g,d}\)]. There exists a canonical ample divisor on \(\mathcal{M}^{g,d}\).

Proof:

Prop. (13.14.3.3). The \(j\)-invariant of Elliptic schemes define an isomorphism \(\mathcal{M}_Q^{1,1} \to \mathbb{A}_Q^1\).

Proof:

4 Hodge Type Shimura Varieties

5 PEL Type Shimura Varieties

6 Complex Multiplication

7 Canonical Models

Remark (13.14.7.1). Delete this? . For a Shimura datum \((G,X)\), attached to each compact open subgroup \(K \subset G(\mathbb{A}^f)\), there is a map

\[
f_K : \text{Sh}_k(G,X) \to \pi_K,
\]

where \(\pi_K\) is a the theory of canonical model defines

- a reflex field \(E = E(G,X)\), which is a number field.

- A canonical model \((f_K)_0 : \text{Sh}_k(E,G)_0 \to (\pi_K)_0\) of \(f_K\) over \(E\), which is uniquely characterized by the reciprocity law at the special points.

and also describes the action of \(\text{Aut}(\mathbb{C}/E)\) on \(\pi_K\).
Remark (13.14.7.2). Delete this? The method of constructing the canonical model is the following: When our Shimura variety arises naturally as a moduli space over $\mathbb{C}$, then we can use the action of $\text{Gal}(\mathbb{C}/E)$ on the $\mathbb{C}$-points to define a model of the variety over a specific number field.

The theory of complex multiplication will give us an explicit description of the action on certain special points, called the reciprocity law at these points, which will determine the model uniquely.

Remark (13.14.7.3). Delete this? A heuristic reason that a Shimura variety has a canonical model is that if it is defined only on a transcendental field, then it can be spread out to give a flat family of varieties. But there are only countably many arithmetic locally symmetric varieties up to isomorphism, so there cannot be a
13.15 Mordell-Lang Conjecture (Faltings Theorem)

References are [Mordell Seminar notes, Bhatt], [http://virtualmath1.stanford.edu/~conrad/mordellsem/], [?] and [Mil08].

1 Tate Hom Conjecture

Lemma (13.15.1.1). Let $k$ be a field, $A_1, A_2 \in \text{AbVar} / k$, and $\ell \in \text{P} \setminus \text{char } k$, then the natural map
\[
\text{Hom}(A_1, A_2) \otimes \mathbb{Z}_\ell \to \text{Hom}_{\mathbb{Z}_\ell}(T_\ell(A_1), T_\ell(A_2))
\]
is injective.

Proof: Same as the proof of the Elliptic case. Cf.[Silverman]. □

Thm. (13.15.1.2) [Tate’s Hom Conjecture, Faltings]. Let $K$ be a finite field or a global field, $\ell \in \text{P} \setminus \text{char } K$, if $A_1, A_2 \in \text{AbVar} / k$, then
\[
\text{Hom}(A_1, A_2) \otimes \mathbb{Z}_\ell \to \text{Hom}_{\text{Gal}_K}(T_\ell(A_1), T_\ell(A_2))
\]
is an isomorphism.

Proof: For a finite field, it suffices to prove that □

2 Heights of Abelian Varieties

Def. (13.15.2.1) [Faltings Heights]. Let $F$ be a number field and $A \in \text{AbVar} / F$, take the Néron model $\mathcal{A}/\mathcal{O}_F$, then $\mathcal{K}_{A/\mathcal{O}_F}$ is an invertible sheaf, and thus $M_s^{-1}\mathcal{K}_{A/\mathcal{O}_F}$ is an invertible $\mathcal{O}_F$-sheaf, represented by a fractional ideal $M \subset F$, and $M \otimes_F F = \Gamma(A, \mathcal{K}_{A/F})$ by (7.1.1.14).

We define a norm on $M \otimes_F F_v = \Gamma(A_v, \mathcal{K}_{A_v/F_v})$ for each $v \in \Sigma F$:
\[
||\omega||_v = \left(\frac{i}{2} g \int_{A(F_v)} \omega \wedge \overline{\omega}\right)^{1/2}.
\]
This make $\tilde{M}$ a metrized line bundle on $\mathcal{O}_F(17.2.1.1)$.

Then we define the Faltings height of $A$:
\[
H(A) = H((\tilde{M}, |\cdot|))(17.2.1.2), \quad h(A) = \frac{1}{[F : \mathbb{Q}]} \log H(A).
\]

More explicitly, take a non-zero holomorphic $g$-form $\omega$ on $A$, and for $v \in \Sigma F$, let $\omega_v$ be a Néron differential $\omega_v$ on $A_v$ (i.e. corresponding to an element in $K_v$ of valuation 1), then
\[
H(A) = \frac{1}{\prod_{v \in \Sigma F} ||\omega_v||_v \cdot \prod_{v \in \Sigma F} \left(\frac{i}{2} g \int_{A_v(F_v)} \omega \wedge \overline{\omega}\right)^{[K_v: \mathbb{Q}_v]/2}}
\]

Def. (13.15.2.2) [Stable Faltings Height]. Let $F$ be a number field and $A \in \text{AbVar} / F$, then by (13.10.15) there exists a finite extension $L/F$ s.t. $A_L$ is semistable. Then the Néron model of $A_L$ are stable under base change. Then we can define the stable Faltings height $h_s(A) = h(A_L)$, which is invariant of $L$ chosen.

Prop. (13.15.2.3). Let $F$ be a number field and $A \in \text{AbVar} / F$, then $h(A) = h(A^\vee)$.

Proof: Cf.[Szpiro, La Conjecture de Mordell, Séminaire Bourbaki, 1983/84]. □

Thm. (13.15.2.4).
Modular Heights

**Def. (13.15.2.5)** [Modular Heights]. Consider the Siegel modular varieties $\mathcal{M}_{g,d}/\mathbb{Q}$ parametrizing Abelian schemes (13.14.3.1), then for any number field $K$, $(A, \lambda) \in \text{AbVar}^\text{dim=g,polar=d}_/K$ defines a $K$-point $j((A, \lambda))$ of $\mathcal{M}_{g,d}$. Then we can define the modular height $h_M(A, \lambda)$ to be $h(j((A, \lambda)))$, where $h$ is the Weil height associated to the canonical ample divisor on $\mathcal{M}_{g,d}(13.14.3.2)$, which is defined up to a bounded function on $\mathcal{M}_{g,d}$.

**Prop. (13.15.2.6)** [Comparison of Heights]. Let $F$ be a number field, then there are constants $c_1, c_2, c_3$ s.t. for any $(A, \lambda) \in \text{AbVar}^\text{polar}/F$,

$$|h_F(A) - c_1 h_M(A, \lambda)| < c_2 \log h_M(A, \lambda) + c_3.$$

*Proof:* Hard. Cf. [Chai and Faltings, 1990].

**Prop. (13.15.2.7)** [Height I]. Let $F$ be a number field and $g, d, C \in \mathbb{Z}_+$, then up to isomorphism, there are only f.m. semistable $(A, \lambda) \in \text{AbVar}^\text{dim=g,polar=d}/F$ s.t. $h_M(A, \lambda) < C$.

*Proof:* By the definition of Siegel modular varieties, two objects in $(A, \lambda) \in \text{AbVar}^{\text{dim=g,polar=d}}/F$ corresponds to the same point of $\mathcal{M}_{g,d}(13.15.2.5)$ iff they are isomorphic over $F$. And by Northcott’s theorem(13.2.4.20) the image of polarized Abelian varieties with bounded modular heights is finite. Thus the assertion follows from(13.15.3.2).

**Cor. (13.15.2.8)** [Height II]. Let $F$ be a number field and $g, C \in \mathbb{Z}_+$, then up to isomorphism, there are only f.m. semistable $A \in \text{AbVar}^{g}/F$ s.t. $h(A) < C$, by(13.15.2.6).

*Proof:* By the proposition(13.15.2.7) and(13.15.2.6), the set of isomorphism classes of semistable Abelian varieties $(B, \lambda) \in \text{AbVar}^{\text{dim=g,polar=d}}/F$ is finite. Now notice for any $A \in \text{AbVar}/F$, $B = (A \times A^\vee)^4$ is principally polarized by(13.5.7.2), and $h(B) = 8h(A)$ by(13.15.2.3), so we are done.

3 Finiteness Theorems

**Prop. (13.15.3.1)**. Let $L/F$ be a Galois extension of number fields, then for any $A \in \text{AbVar}/F$, there exists f.m. isomorphism classes of $B \in \text{AbVar}/F$ s.t. $A_L \cong B_L$.

*Proof:* Cf.[Conrad note, L14]

**Prop. (13.15.3.2)** [Finiteness Theorems]. Let $F$ be a number field and $(A, \lambda) \in \text{AbVar}^{\text{dim=g,polar=d}}/F$, then there exists only f.m. isomorphism classes of $(B, \lambda) \in \text{AbVar}^{\text{dim=g,polar=d}}/F$ s.t. $(A_{\overline{\mathbb{F}}}, \lambda) \cong (B_{\overline{\mathbb{F}}}, \mu)$.

*Proof:* Firstly, by(13.5.10.10), any such $B$ is also semistable, so the set of good reductions are stable under base change, thus the set of good reductions of $A$ and $B$ in $\Sigma_F$ are the same.

Then by(13.13.1.1) and(12.2.4.21), for $\ell \in \mathbb{P}\setminus\{2\}$, there is a finite extension $L/F$ s.t. every $\ell$-torsion points of such $B$ are in $B(L)$.

Now any such $B$ are isomorphic to $A$ over $L$ as above: Given any isomorphism $\alpha : (A_{\overline{\mathbb{F}}}, \lambda) \cong (B_{\overline{\mathbb{F}}}, \mu)$, for $\alpha' \in \text{Gal}_L$, $\alpha$ and $\sigma(\alpha)$ has the same action on $\ell$-torsion points, as all these points are $L$-rational, so $\sigma(\alpha)^{-1} \circ \alpha$ acts trivially on $A[\ell]$, which implies by(13.5.7.5) that $\sigma = \alpha(\sigma)$, so $\sigma$ is defined over $L$ and we are done.

Finally we finish using(13.15.3.1) and(13.5.7.3).
Thm. (13.15.3.3) [Finiteness of Heights in an Isogeny class]. Let $F$ be a number field and $A \in \text{AbVar}/F$ be semistable, then the set of Faltings height of $B \in \text{AbVar}/k$ isogenous to $A$ is finite.

Proof: This is the hardest part of the proof. Cf.[Conrad Seminar, L20]. 

Thm. (13.15.3.4) [Finiteness I]. Let $F$ be a number field and $A \in \text{AbVar}/F$, then there are only f.m. isomorphism classes of Abelian varieties $B \in \text{AbVar}/k$ isogenous to $A$.

Proof: If $A$ is semistable, then by (13.5.10.10), any $B \in \text{AbVar}/k$ isogenous to $A$ is also semistable. Then we are done by (13.5.10.15). For a general $A$, there exists a finite extension $L/k$ s.t. $A_L$ is semistable by (13.5.10.15). Then the general case reduced to the semistable case by using (13.15.3.1).

Thm. (13.15.3.5) [Finiteness II, Shafarevich/Faltings]. Let $F$ be a number field, $S \subset \Sigma_F$ be a finite set of places, then there are only f.m. isomorphism classes of $A \in \text{AbVar}^{\text{dim}=g}/F$ having good reduction at all finite places outside $S$.

Proof: By (13.15.3.4), it suffices to show that there are only f.m. isogeny classes of $A \in \text{AbVar}^{\text{dim}=g}/F$ having good reduction at all finite places outside $S$. But then we can use (13.5.10.14) and the fact there are only f.m. such polynomials $P_t(A_v,t)$ because of Weil conjecture.

4 Curves

Prop. (13.15.4.1) [Genus 0 Curves]. Any genus 0 smooth complete curve $C$ over a global field $F$ of characteristic $\neq 2$ is a conic in $\mathbb{P}^2$, thus by (5.11.8.2), it is isomorphic to $\mathbb{P}^1$ iff it has a rational point. But by Hasse-Weil principle, this is equivalent to it having a rational point over each local field of $F$, and this can be understood via Hilbert symbol.

Thm. (13.15.4.2) [Shafarevich’s Conjecture, Faltings]. Let $F$ be a global field, $S \subset \Sigma_F$ be a finite set of places, $g \in \mathbb{Z}_+$, then there are only f.m. isomorphism classes of smooth curves over $k$ of genus $g$ having good reduction at all non-Archimedean places outside $S$.

Proof: This follows from (13.5.13.16)/(13.5.13.15) and (13.5.7.3)/(13.15.3.5).

Prop. (13.15.4.3) [Kodaira-Parshin]. Let $F$ be a number field and $S$ is a finite set of places of $F$ containing all places over 2, then for any complete smooth curve $C$ over $k$ of genus $g \geq 1$ having good reduction at non-Archimedean places outside $S$, there exists a finite extension $L/k$ and a constant $N$, s.t.: For any $P \in C(F)$, there exists a complete smooth curve $C^P$ over $L$ and a finite map $\psi^P : C^P \to C_L$, that satisfies
- $g(C^P) \leq N$.
- $\psi_P$ is ramified exactly at $P$.

Proof: Cf.[Mil08]P115, 145.

Thm. (13.15.4.4) [Mordell Conjecture, Faltings]. Let $F$ be a number field and $C$ be a curve of genus $g \geq 2$ defined over $F$, then $C(F)$ is finite.
Proof: Using the construction of Kodaira-Parshin (13.15.4.3), there is a finite extension $L/F$ s.t. any $P \in C(F)$ corresponds to a curve $C^P$ over $L$ and a map $\varphi_P : C^P \to C_L$. By Shafarevich’s conjecture applied to $L(13.15.4.2)$, there are only f.m. isomorphism classes of $C^P$. But for different $P, Q$ s.t. $C^P \cong C^Q$, the maps $\varphi_P, \varphi_Q$ are non-isomorphic, as they are ramified at different places. So we are done by de Franchis’ theorem (5.11.1.34).

Conj. (13.15.4.5) [Mordell-Lang]. Let $X$ be a closed geometrically integral subvariety of a semi-Abelian variety $A$ defined over a field $K$ of characteristic 0. Let $\Gamma$ be a f.g. subgroup of $A(\overline{K})$ and $\Gamma'$ be a subgroup of the divisible hull of $\Gamma$. If $X$ is not a translate of a semi-Abelian subvariety of $A$, then $X(\overline{K}) \cap \Gamma'$ is not Zariski dense in $X$.

Proof: □

Cor. (13.15.4.6) [Manin-Mumford]. Let $K$ be a number field and $C$ be a curve of genus $g \geq 2$ defined over $K$, and $J$ the Jacobian of $C$. Fix an embedding $C \hookrightarrow J$ defined over $K$, then the set $C(\overline{K}) \cap J(\overline{K})_{\text{tor}}$ is finite.

Proof: □
13.16 Tate Conjecture & Hodge Conjecture

Main references are [Tate, Conjectures on Algebraic Cycles in \(\ell\)-adic Cohomology, Motives, 1991], [RECENT PROGRESS ON THE TATE CONJECTURE, Totaro] and [Tate Conjecture over Finite Fields, Milne].

1 Statements

Prop. (13.16.1.1) [\(\ell\)-adic Cycle Classes]. Let \( k \in \text{Field} \) and \( X \in \text{SmProjVar}/k, \overline{X} = X \otimes_k k^s, \ell \in \mathbb{P} \setminus \text{char} \ k \), then there exists a cycle map

\[ c^r : \text{CH}^r(\overline{X}) \to H^{2r}_\text{et}(\overline{X}, \mathbb{Q}_\ell(r)), \]

as étale cohomology is a Weil cohomology theory? Let \( A'_{\text{et}, \ell}(\overline{X}) \) be the image, and \( A^{r}_{\text{et}, \ell}(X) \) be the image of \( \text{CH}^r(X) \subset \text{CH}^r(\overline{X}) \) under this map. Then there are maps

\[ A'_{\text{et}, \ell}(\overline{X}) \otimes \mathbb{Q}_\ell \subset H^{2r}(\overline{X}, \mathbb{Q}_\ell(r)), \quad A^{r}_{\text{et}, \ell}(X) \otimes \mathbb{Q}_\ell \subset H^{2r}(\overline{X}, \mathbb{Q}_\ell(r))^\text{Gal}_k. \]

Conj. (13.16.1.2) [Tate]. Situation as in (13.16.1.1), if \( k \) is f.g. over its prime field, then

\[ (T^r(X/k), \ell) : A'_{\text{et}, \ell}(X) \otimes \mathbb{Q}_\ell \to H^{2r}(\overline{X}, \mathbb{Q}_\ell(r))^\text{Gal}_k. \]

\[ (E^r(X/k), \ell) : A^{r}_{\text{et}, \ell}(X) \cong \text{GH}^r(X). \] In particular, \( A^{r}_{\text{et}, \ell}(X) \) doesn’t depend on \( \ell \).

\[ (S^r(X/k), \ell) : \text{Fr}_X \text{ acts semisimply on the } 1\text{-eigenpart } H^r_{\text{et}}(X, \mathbb{Q}_\ell(r)). \]

Proof: \( \square \)

Conj. (13.16.1.3) [Integral Tate Conjecture]. Situation as in (13.16.1.1), if \( k \) is f.g. over its prime field, then we may ask if

\[ A^{r}_{\text{et}, \ell}(X) \otimes \mathbb{Z}_\ell = H^{2r}(\overline{X}, \mathbb{Z}_\ell(r))^\text{Gal}_k. \]

Cf. [Tate Conjecture, Milne, P3].

Prop. (13.16.1.4).

Prop. (13.16.1.5) [(\(E^1\) Holds]. The Kummer exact sequence of étale sheaves on \( \overline{X} : 0 \to \mu_{\ell^n} \to G_m \xrightarrow{\ell^n} G_m \to 0 \) induces an injection \( \text{Pic}(\overline{X})/\ell^n \text{Pic}(\overline{X}) \hookrightarrow H^2(\overline{X}, \mu_{\ell^n}). \) Taking limits gives an injection \( \text{Pic}(\overline{X}) \otimes \mathbb{Q}_\ell \hookrightarrow H^2(\overline{X}, \mathbb{Q}_\ell(1)). \) And \( c^1 \) is just

\[ c^1 : Z^1(\overline{X}) \to \text{Pic}(\overline{X}) \to \text{Pic}(\overline{X}) \otimes \mathbb{Q}_\ell \hookrightarrow H^2_{\text{et}}(\overline{X}, \mathbb{Q}_\ell(1)). \]

Thus the kernel of \( c^1 \) is just the \( \text{Pic}(X) \) modulo \( \ell^n \)-divisible elements and torsion elements, but \( \text{Pic}^0(\overline{X}) \) is \( \ell^n \)-divisible as it is the \( k^s \)-points of an Abelian variety over \( k^s \). And also \( \text{Pic}(\overline{X})/\text{Pic}_{\text{num}=0}(\overline{X}) \to \text{Pic}(X^\text{F})/\text{Pic}^\ell(X^\text{F}) = N^1(X^\text{F}) \) is injective by [Sta]0CC5?, and \( N^1(X^\text{F}) \) is finite free, so \( \text{Pic}_{\text{num}=0}(\overline{X}) = \text{Pic}(\overline{X})_{\text{tor}}, \) and \( A^{1}_{\text{et}, \ell}(X) = \text{GH}^1(X) \).

Remark (13.16.1.6) [Hodge & Tate Conjecture]. In characteristic 0, we can embed \( k \) into \( \mathbb{C} \) and use étale-singular comparison to see the Hodge conjecture implies the Tate conjecture?

Prop. (13.16.1.7). Situation as in (13.16.1.2), let \( X, Y \in \text{SmProjVar}/k, \) then

\[ (T^1(X \times_k Y)) \iff (T^1(X)) + (T^1(Y)). \]
Proof:

**Proposition (13.16.1.8).** Situation as in (13.16.1.2), let \( f : X \to Y \in \text{SmProjVar} / k \) be a dominant rational map, then \((T^1(X/k)) \Rightarrow (T^1(Y/k))\).

Proof:

**Corollary (13.16.1.9).** The Fermat curve \( S_n : z_0^n + z_1^n + z_2^n + z_3^n = 0 \) is dominated by the product of two curves

\[
C_1 : x_0^n + x_1^n = x_2^n, \quad C_2 : y_0^n + y_1^n = -y_2^n
\]

by \( C_1 \times C_2 \to S : ([x_0, x_1, x_2], [y_0, y_1, y_2]) \mapsto [x_0y_2, x_1y_2, y_0x_2, y_1x_2] \), so \((T^1(S_n))\) holds.

## 2 over Finite Fields

Main references are [Milne, Tate Conjecture over Finite Fields], and [Endomorphisms of abelian varieties over finite fields, Tate, 1966].

**Proposition (13.16.2.1) [(T^1)].** Let \( k \neq \infty \) and \( X \in \text{SmProjVar} / k \), Tate proved that \( H^{2r}(\overline{X}, \mathbb{Q}_\ell(r))^{\text{Gal}_k} \cong H^{2r}_{\text{et}}(X, \mathbb{Q}_\ell(r)) \), and the Kummer sequence gives an exact sequence?

Proof:

**Connection with BSD**

**Proposition (13.16.2.2) [Tate].** Let \( k \neq \infty \), \( X \in \text{SmProjVar} / k \), then \((T^r(X/k))\) and \((E^r(X/k))\) hold iff

\[
\text{ord}_{s=r}(Z(X, s)) = -\text{rank } GH^r(X).
\]

Proof:

**Proposition (13.16.2.3) [(T^1) and BSD].** Let \( k \neq \infty \) and \( C \) a smooth complete curve over \( k \) with function field \( K \), \( E/C \) is a regular elliptic surface with generic fiber \( E \in \text{Ell} / K \), then \((T^1(E/k))\) is equivalent to the BSD conjecture for \( E/K \).

Proof:

**Proposition (13.16.2.4) [Grothendieck].** Let \( k \neq \infty \) and \( C \) a smooth complete curve over \( k \) with function field \( K \), \( E/C \) is a regular elliptic surface with generic fiber \( E \in \text{Ell} / K \), then \( \text{Br}(E/k) \cong \text{III}(E/K) \).

Proof: Cf.[Grothendieck, Alexander, Le groupe de Brauer. III. 1968].
13.16. TATE CONJECTURE & HODGE CONJECTURE

3 K3 Surfaces

Main references are [The Tate Conjecture For K3 Surfaces In Odd Characteristic, Pera], [The Tate Conjecture For K3 Surfaces—A Survey Of Some Recent Progress], [2-adic integral canonical models and the Tate conjecture in characteristic 2].

Thm. (13.16.3.1) [Pera]. \((T^1(X))\) holds if \(X\) is a K3 surface.

Proof: Cf. [The Tate Conjecture For K3 Surfaces In Odd Characteristic, Pera] and [2-adic integral canonical models and the Tate conjecture in characteristic 2].

Cor. (13.16.3.2) [Lieblich-Maulik-Snowden]. There are only finitely many isomorphism classes of K3 surfaces over a finite field of characteristic \(\geq 5\).

Proof: [Finiteness Of K3 Surfaces And The Tate Conjecture, Lieblich-Maulik-Snowden].

Kuga-Satake construction

4 Hodge Conjecture

Main references are [Hodge cycles on abelian varieties, Deligne].

Def. (13.16.4.1) [Hodge Classes]. For \(X \in \text{SmProj}/\mathbb{C}\), define \(\text{Hodge}^{2k}(X) = H^{2k}_{\text{Betti}}(X, \mathbb{Q}) \cap H^{k,k}_{\text{Betti}}(X)\), called the Hodge classes of \(X\) of degree \(2k\).

Prop. (13.16.4.2). If \(X \in \text{SmProj}/\mathbb{C}\) and \(Z \subset Z^r(X)\), then \([Z] \subset \text{Hodge}^k(X)\).

Proof: ??

Conj. (13.16.4.3) [Hodge]. For \(X \in \text{SmProj}/\mathbb{C}\), every Hodge class is algebraic.

Proof: ??

Arithmetic Theory

Thm. (13.16.4.4) [Deligne]. Let \(k \in \text{Field}^0, k = \overline{k}\), \(X \in \text{AbVar}/k\), and let \(t \in H^{2p}_X(X)(p)\). Then if \(t\) is a Hodge cycle w.r.t. one embedding \(\sigma : k \to \mathbb{C}\), then it is absolutely Hodge.

Proof: ??

Def. (13.16.4.5) [Hodge Classes]. Let \(k \in \text{Field}^0, k = \overline{k}\), and \(X \in \text{SmProj}/k\), then for any embedding \(\sigma : k \hookrightarrow \mathbb{C}\), \(H^{2k}_{\text{dR}}(X/k)\) satisfies

\[
H^{2k}_{\text{dR}}(X/k) \otimes_{k,\sigma} \mathbb{C} \cong H^{2k}_{\text{dR}}(X, \mathbb{C}) \cong H^{2k}_{\text{Betti}}(X, \mathbb{C}).
\]

Thus we can define the space \(\text{Hodge}^{2k}(X)\) of Hodge cycle on \(X\) of degree \(2k\) w.r.t. \(\sigma\) as the subspace of elements in \(H^{2k}_{\text{dR}}(X/k)\) that are mapped to \((2\pi i)^k\) times a Hodge class of \(\sigma X\) of degree \(2k\).

This notion is independent of the embedding \(\sigma\).

Proof: ??
13.17 André-Oort Conjecture

References are [Canonical Heights on Shimura Varieties and the André-Oort Conjecture].
13.18 Logarithmic Geometry

Main references are [DLLZ19], [LOG p-DIVISIBLE GROUPS].
13.19 Arithmetic Topology


1 Knots and Primes
14  |  $p$-Adic Geometry

14.1 Galois Representations

Main references are [Theories of $p$-adic Galois Representations, Fontaine/Yi Ouyan], [Local Langlands for GL(n), Zijian Yao]. [notes on $p$-adic Hodge Theory, Conrad].

For $K \in \text{Field}$, $E \in \text{Field}^{\text{top}}$, the theory of Galois representations study the category $\text{Rep}_E(\text{Gal}_K)$.

Notations (14.1.0.1).
- Use notations defined in Classical Representation Theory.

1 Basics

Def. (14.1.1.1) [$p$-adic Galois Representations]. For a topological group $G$ and $p \in \mathbb{P}$, an $p$-adic Galois representation is a f.d. $\mathbb{Q}_p$-action of $G$.

Prop. (14.1.1.2) [Compact Group Stablizes a Lattice]. Let $\Gamma$ be a compact group and let $\rho : \Gamma \rightarrow GL(n, \mathbb{Q}_p)$ be a continuous homomorphism, then there exists a finite extension $L/\mathbb{Q}_p$ that $\rho(\Gamma) \subset GL(n, L)$, and up to conjugation, $\rho(\Gamma) \subset GL(n, \mathcal{O}_L)$, or equivalently, $\Gamma$ fixes a $\mathcal{O}_L$-lattice. 

Proof: Notice $\rho(\Gamma)$ is compact and Hausdorff, so by Baire category theorem, now that $GL(n, L)$ is closed in $GL(n, \mathbb{Q}_p)$ for all $L/\mathbb{Q}_p$ finite, and all this extensions are countable by primitive element theorem, so there is an $L$ that $\rho(\Gamma) \cap GL(n, L)$ contains an open subset of $\rho(\Gamma)$, so it is an open subgroup, thus of finite index, hence by adding all the coset representations into $L$, we get an $L'$ finite.

For the second assertion, notice $\rho(\Gamma)$ is compact in $GL(n, L)$, thus by (13.3.1.5), it is conjugate to $GL(n, \mathcal{O}_L)$. □

Prop. (14.1.1.3) [Brauer-Nesbitt]. If two $n$-dimensional representations have the same characteristic polynomial or that char $k = 0$ or char $k > n$ and they have the same character, then their semisimplification are the same.

Proof: The proof is not hard, use the Artin-Wedderburn theorem, and the fact the representation may not by semisimple. □

Def. (14.1.1.4) [Cyclotomic Characters and Tate Twists]. For $K \in \text{Field}$, $\ell \in \mathbb{P}$, the $\ell$-adic cyclotomic character $\chi_\ell$ of $\text{Gal}_K$ is the character corresponding to the 1-dimensional $\ell$-adic Tate module of $\mathbb{G}_{a,K}$.

For any representation $(\rho, V) \in \text{Rep}_{\mathbb{Z}_\ell}(\text{Gal}_K)$, we can define the Tate twist $\rho(n)$ as the representation twisted by the $n$-power of the cyclotomic character $\chi_\ell$. 

2 \( \ell \)-adic Local Galois Representations

**Def. (14.1.2.1) [Notations].** Let \( p \in \mathbb{P}, q \in \mathbb{P}^2, K \in p - \text{Field} \) with residue field \( F_q, t_\ell : I_K/R_K \to \mathbb{Z}_\ell \) be the \( \ell \)-adic tame character(12.2.2.20). Let \( \varphi \) be a fixed lift of \( \text{Frob} \in \text{Gal}_{F_q} \). Let \( \chi = \chi_\ell \) be the unramified cyclotomic character(14.1.1.4) \( Z \cong \text{Gal}_K/I_K \to \mathbb{Z}_\ell : \varphi \mapsto q \).

**Remark (14.1.2.2).** Most \( \ell \)-adic representation of \( \text{Gal}_K \) are constructed via étale cohomology.

**Prop. (14.1.2.3) [C-Representations].** For any representation, and also the same as a continuous/smooth \( \mathbb{C} \)-representation.

**Proof:**

**Prop. (14.1.2.4).** If \( \rho : \Gamma \to GL(n,k) = GL(V) \) is a representation, then it has a filtration \( 0 = V_0 \subset V_1 \subset \ldots \subset V_n = V \) where \( V_{i+1}/V_i \) is irreducible, then there is a semisimplification of \( \rho \), which is \( \rho^{ss} = \oplus V_{i+1}/V_i \).

**Def. (14.1.2.5) [Residual Representation].** If \( L/Q_p \) finite, we may take a \( \Gamma \)-stable \( \mathcal{O}_L \)-lattice \( \Gamma \), then the residual representation \( \tilde{\rho}_L \) is defined by \( \Gamma \to GL(\Lambda/\pi \Lambda) \). Then the semisimplification of \( \tilde{\rho}_L \) is independent of \( \Lambda \) chosen.

**Prop. (14.1.2.6) [Induced Galois Representations].** Let \( F \) be a local field with residue characteristic \( p \). Let \( (n, q) = 1 \), then any irreducible representation \( \rho, V \) of \( \text{Gal}_F \) of dimension \( n \) is induced from a character \( \chi \) of \( K^* \) for a field extension \( K/F \) of degree \( n \).

**Proof:** Suppose \( \chi \) factors through a normal subgroup \( G(L/F) \). It suffices to show \( \rho \) is an induced representation from a subgroup, then use induction. Suppose it is not, then consider the filtration of Galois groups \( R_v \subset I_v \subset G_F \). \( R_v \) is a \( p \)-group, thus all irreducible \( \mathbb{F}_p \)-representations are \( p \)-powers, by(15.1.2.12), thus it is 1-dimensional. Now \( R_v \) is a normal subgroup, by(15.1.1.23), \( R_v \) acts by scalars on \( V \). Now the exact sequence \( 1 \to R_v \to I_v \to I_v/R_v \to 0 \) is a split exact sequence(12.2.2.17), and \( I_v/R_v \) is cyclic, thus \( \rho_{I_v} \) also contains a character, and the same argument as above shows \( I_v \) acts by characters. Then a twist of \( \rho \) factors through \( G/I_v \), which is a cyclic group, contradiction.

3 Weil Representations

**Def. (14.1.3.1) [Notations].** We use notations as in(14.1.2.1), the Weil group \( W_K \subset \text{Gal}_K \) be defined as in?, and the Artin map \( \text{Art} : K^* \to W_K^{ab} \) gives a character \( || \cdot || : x \mapsto |\text{Art}^{-1}(x)| \) on \( W_K^{ab} \), which maps a lift of the geometric Frobenius in \( G(\overline{F}_q/F_q) \) to \( q^{-1} \).

We consider smooth representations of \( W_K \), so \( C \)-representations and \( \overline{Q}_\ell \)-representations are the same. (continuous representations are considered in(14.1.3.12)).

**Prop. (14.1.3.2) [Primitive Weil Representation].** \( \pi \in \text{Rep}^{\infty}(W_K) \) is called primitive if it is not induced from a representation of a proper subgroup. Then for any primitive representation of \( W_F \), it factors through \( C_E/F \) for some finite extension \( E/F \) by continuity, and by Clifford’s theorem(15.1.1.23), the normal subgroup \( C_E \) acts by scalars, so the image of \( W_E/F \) in \( GL(V) \) is a finite group.

**Def. (14.1.3.3) [Images of 2-Dimensional Representations].** By(14.1.3.2), any representation \( W_F \to GL(2, \mathbb{C}) \) has finite image in \( PGL(2, \mathbb{C}) \cong SO(3, \mathbb{C}) \). Thus by conjugacy into \( SO(3, \mathbb{R}) \), the image is isomorphic to a cyclic, dihedral, tetrahedral, octahedral or icosahedral group by(11.6.4.18), called the type of this representation.
Def. (14.1.3.4) [Artin Conductor]. Let \((\rho, W)\) be a smooth representation of \(W_K\). define the Artin conductor
\[ c(\rho) = c(\chi_\rho) = \sum_{i>0} \frac{1}{[G_0 : G_i]} (\dim V - \dim V^{G_i}) \]
where \(G_i\) are the higher ramification groups of \(G\).

Def. (14.1.3.5) [Twisting Character of \(W_K\)]. Let \(s \in \mathbb{C}\), we define the quasi-character \(\omega_s : W_F \to \mathbb{C}^\ast\) that \(\omega_s(g) = q^{-ks}\) for \(g\) that maps to \(\text{Frob}^k \in \text{Gal}_{\mathbb{F}_q}\).

Prop. (14.1.3.6) [Twisting of Weil Representation]. For any \(\rho \in \text{Irr}^{\text{alg}}(W_F)\), there exists some \(s\) that \(\omega_s \otimes \rho\) factors through \(W_F \to G_F\), thus the image of \(\omega_s \otimes \rho\) is a finite subgroup of \(GL(V)\).

Proof: \(\ker(\sigma) \cap I_F\) is an open subgroup of \(I_F\). Let \(\sigma \in W_F\) that maps to \(\text{Frob} \in G(\overline{\mathbb{F}_q}/\mathbb{F}_q)\), then conjugation by \(\sigma\) induces a permutation on the finite subgroup \(I_F/\ker(\rho) \cap I_F\), so there is some \(n\) that \(\rho^n = \text{id}\) on \(I_F/\ker(\rho) \cap I_F\), which means \(\rho(\sigma^n)\) commutes with each elements of \(W_F\), thus it is a scalar by Schur’s lemma. Thus we can chose \(s\) that \(\omega_s \otimes \rho(\sigma^n) = 0\), then \(\omega_s \otimes \rho\) is trivial on a subgroup of \(W_F\) with finite index generated by \(\sigma^n\) and \(\ker(\rho) \cap I_F\). Thus the image is finite.

Also the closed subgroup \(U\) in \(G(\overline{\mathbb{F}}/\mathbb{F})\) generated by \(\sigma^n\) and \(\ker(\rho) \cap I_F\) has finite index, and \(U \cap W_F = U\), thus \(W_F/U \cong \text{Gal}_{\mathbb{F}/U}\), thus this representation extends to \(G(\overline{\mathbb{F}}/\mathbb{F})\). \(\square\)

Cor. (14.1.3.7) [Galois Type Representations]. A representation of \(W_F\) coming from a smooth representation of \(G_F\) is called a representation of Galois-type.

Thus, (14.1.3.6) shows \(\text{Rep}(\text{Gal}_K)\) are almost the same as \(\text{Rep}^\infty(W_K)\). A representation of \(W_F\) is of Galois type iff it has a finite image.

Def. (14.1.3.8) [\(\varphi\)-Semisimple Weil Representations]. \(\rho \in \text{Irr}^{\text{alg}}(W_K)\) is called \(\varphi\)-semisimple iff \(\rho(\varphi)\) is semisimple.

Prop. (14.1.3.9). Let \(\rho\) be a representation of \(W_K\) that \(\rho(I_K)\) is finite, the following are equivalent:
- \(\rho(\sigma)\) is semisimple for any \(\sigma \in W_K\).
- \(\rho(\varphi)\) is semisimple.
- \(\rho\) is a semisimple representation.

Proof: Cf.[Yao17]P4. \(\square\)

Def. (14.1.3.10) [\(\ell\)-Integral Representations]. Let \(r\) be a smooth representation of \(W_K\) on \(\overline{\mathbb{Q}_\ell}\), then by (14.1.3.6), the eigenvalues of \(r\) are \(\ell\)-adic units iff the eigenvalues of \(r(\varphi)\) are all \(\ell\)-adic units, iff the characteristic polynomial of \(r(\varphi)\) are in \(\mathcal{O}_L[X]\) and \(|\det(r(\varphi))| = 1\). Such a representation is called an \(\ell\)-integral representation.

Deligne-Weil Representations

Def. (14.1.3.11) [Deligne-Weil Representations]. Let \(L\) be a field, the category \(\mathfrak{w}b_L(W_K)\) of Deligne-Weil representations of \(W_K\) over \(L\) consists of triples \((\rho, V, N)\), where \((\rho, V)\) is a smooth representation of \(W_K\) over \(L\), and \(N\) is an endomorphism of \(V\) s.t.
\[ \rho(x) N \rho(x)^{-1} = ||x|| N. \]
\[ \rho = (\rho', N) \in \mathfrak{w}b_L(W_K) \) is called \(\varphi\)-semisimple if \(\rho'\) is \(\varphi\)-semisimple (14.1.3.8).
Equivalently, a Deligne-Weil representation is a smooth representation $(\rho, V)$ of $W_K$ together with a $W_K$-map $V \mapsto V(1)$. (14.1.1.4)

We can define the tensor products or duals in $\mathfrak{d}u_L(W_K)$, where $\rho$ transfer as Lie group representations and $N$ transfer as Lie algebra representations.

$N$ is necessarily nilpotent, and for an irreducible Deligne-Weil representation, $N = 0$.

**Proof:** $N$ is nilpotent because $\varphi N \varphi^{-1} = q^{-1} N$, thus its characteristic polynomial equals

$$f(t) = \det(tI - N) = \det(tI - q^{-1} N) = q^{-n} f(qt)$$

thus $f(t) = t^n$.

□

**Remark (14.1.3.12).** Deligne-Weil representations are exactly the continuous representations of $W_K$, as will be illustrated in (14.1.3.16).

**Prop. (14.1.3.13) [Sp$_m(\rho)$].** If $(\rho, V) \in \text{Rep}^\infty(W_K)$ and $m \geq 0$, we can define the a Deligne-Weil representation $\text{Sp}_m(\rho)$ given by $\text{Sp}_m(\rho) = V \oplus V(1) \oplus \ldots \oplus V(m - 1)$ and $N$ maps $V(i)$ isomorphically to $V(i + 1)$ for $i < m - 1$, and trivial on $V(m - 1)$.

Then any representation that

**Prop. (14.1.3.14) [Grothendieck's $\ell$-adic Monodromy Theorem].** Let $\rho$ be a continuous $\ell$-adic representation of $W_K$, then

- There exists an open subgroup $I'_K \subset I_K$ and a uniquely determined nilpotent operator $N \subset \text{End}(V)$ s.t. for all $\sigma \in I'_K$, $\rho(\sigma) = \exp(t_1(\sigma) N)$.
- For any element $\tau = \sigma \varphi^n \in W_K$, $\sigma \in I_K$,

$$\rho(\tau) N \rho(\tau^{-1}) = q^{-n}N.$$  

**Proof:** Cf. [Local Langlands, P7].

□

**Cor. (14.1.3.15) [Potentially Unramified].** If $\rho$ is a semisimple $\ell$-adic continuous representation of $W_K$, then $\rho(I_K)$ is finite, and $\rho(I_K') = 1$ for some finite extension of $K$. In particular, $\rho(I_K)$ is finite.

**Proof:** Choose a finite extension $K'/K$ s.t. $I_{K'} \subset I'_K$, then $\rho|_{I_{K'}}$ is both unipotent and semisimple (15.1.1.23).

□

**Cor. (14.1.3.16) [Continuous Representations and Deligne-Weil Representations].** There is an equivalence of categories

$$WD : \text{Rep}(W_K) \rightarrow \mathfrak{d}b(W_K)$$

$$(\rho, V) \mapsto (\rho_\varphi, V, N), \quad \rho_\varphi(\varphi^n x) = \rho(\varphi^n x) \exp(-t_1(x) N),$$

where $N$ is given in (14.1.3.14).

**Prop. (14.1.3.17) [Integral Deligne-Weil Representation is Galois].** There is an equivalence of categories

$$WD = WD_{\xi, \varphi} : \text{Rep}_L(G_K) \cong \mathfrak{d}b_{L}$$(int)(W_K)$$

$$\rho \mapsto (\rho', N), \quad \rho'(\sigma \varphi^n) = \rho(\sigma \varphi^n) \exp(-t_1(\sigma) N)$$

from the category of $L$-adic $G_K$-representations and the category of $L$-integral where $N$ is given in (14.1.3.14).

Moreover, $\rho$ is semisimple iff $WD(\rho)$ is semisimple, and $\rho$ is irreducible iff $WD(\rho) = (\rho', 0)$, where $\rho'$ is irreducible.
Proof:

Cor. (14.1.3.18). In the above situation, for $\rho \in \text{Rep}_L(G_K)$, the following are equivalent:

- $\rho$ is semisimple.
- $\rho$ is $\varphi$-semisimple and $\rho(I_K)$ is finite.
- $\rho'$ is $\varphi$-semisimple and $N = 0$.

Def. (14.1.3.19) [Dihedral Representation]. A dihedral Weil representation is a representation $W_F \to GL(2, \mathbb{C})$ that is induced from a quasi-character of $W_E$ for some quadratic extension $E/F$.

Prop. (14.1.3.20) [Induced Weil Representations]. If $F$ is a non-Archimedean field of residue characteristic prime to $n$, then any irreducible representation $W_F \to GL(n, \mathbb{C})$ is induced from a quasi-character of $W_E$ (equivalently $E^*$) where $E$ is a $n$-dimensional field extension $E/F$.

Proof: By (10.9.5.4), the class of such induced extensions are stable under twisting by $\omega_s$, thus using (14.1.3.6), we can assume that the representation factors through $G(F/F)$, thus through $G(K/F)$ for some finite extension $K/F$, thus the assertion follows from (14.1.2.6).

Conj. (14.1.3.21) [Fontaine-Mazur]. Let

L-Functions of Weil Representations

Notation as in (15.8.0.1).

Thm. (14.1.3.22) [Weil L-Factors]. For any local field $K$ and a non-trivial character $\psi$ of $K^+$, there exists a group homomorphism

$$\varepsilon(\cdot, \psi) : K_0(\text{Rep}_{W_K}) \to \mathbb{C}^*$$

that satisfy

- For a quasi-character $\chi$, $\varepsilon(\chi, \psi)$ agrees with local factor given by Tate thesis.
- If $E/F$ is a finite extension, and $\rho$ is a representation of $W_E$, then

$$\varepsilon(\text{ind}_{W_F}^{W_E} \rho, \psi_F) = \lambda(E/F, \psi_F)^{\dim \rho} \varepsilon(\rho, \psi_F \circ \text{tr}_{E/F}).$$

Proof: Cf. [Functional Equation for Artin L-Functions, Langlands]

Def. (14.1.3.23) [Deligne-Weil L-Factors]. Let $\rho = (\rho', N)$ be a Deligne-Weil representation of $W_K$, we define

- the conductor $c(\rho) = c(\rho') + \dim V^I_K - \dim \ker(N)^I_K$.
- the local L-factor

$$L(\rho, s) = \det(1 - a^{-s} \varphi | \ker(N)^I_K)^{-1}.$$ 

- the local $\varepsilon$-factor

$$\varepsilon(\rho, s, \psi) = q^{-c(\rho) + n(\psi) \dim V} \det(-\varphi | V^I_K / \ker(N)^I_K)^{\varepsilon(\rho', \psi)}.$$ 

Prop. (14.1.3.24). $\varepsilon(\rho \otimes \omega_s, \psi) = q^{-c(\rho) + n(\psi) \dim V} \varepsilon(\rho, \psi)$.

Proof: □
4 Mod ℓ Local Galois Representations

Notations (14.1.4.1). Use notation as in (14.1.2.1).

Def. (14.1.4.2) [Decomposed Generically]. Let $K \in p$-LField with residue field $F_q$ and $\ell \in P\backslash p$, an unramified representation
$$\overline{\rho} : \text{Gal}_K \to GL(n, \overline{F}_\ell)$$
is called decomposed generically if the eigenvalues $\{\lambda_1, \ldots, \lambda_n\}$ of $\overline{\rho}(\varphi)$ satisfies $\lambda_i / \lambda_j \notin \{1, q\}$ for any $1 \leq i \neq j \leq n$.

5 $p$-adic $p$-Local Representations

6 Representations from Geometry

Prop. (14.1.6.1). Let $k \in \text{Field}$ and $E \in E_{\ell} \backslash k$, then for any $N \in \mathbb{Z}\backslash \text{char} k$, there is an action of $\text{Gal}_k$ on $E[N] \cong (\mathbb{Z}/(N))^2$, giving a representation
$$\rho_{E,N} : \text{Gal}_k \mapsto GL(2, \mathbb{Z}/(N)).$$

Let $\overline{\rho}_{E,N}$ denote the representation $\text{Gal}_k \mapsto GL(2, \mathbb{Z}/(N))/\{\pm 1\}$. Then $\rho_{E,N}$ is surjective iff $\overline{\rho}_{E,N}$ is surjective.

Proof: Notice if $\overline{\rho}_{E,N}$ is surjective, then either $\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$ or $\begin{bmatrix} -1 & 1 \\ -1 & 1 \end{bmatrix}$ is in the image, thus $-1$ is in the image. □

Def. (14.1.6.2) [Tate modules]. For $\ell \in P$, the action of $\text{Gal}_k$ on the Tate module $T_\ell(E)$ (13.5.6.15) is denoted by $\rho_{E,\ell}^\infty$.

Prop. (14.1.6.3) [Determinant of Tate Modules]. If $(K, k)$ be a CDVR and $E \in E_{\ell} / K$, then $\det(\rho_{E,\ell}^\infty)$ is the $\ell$-cyclotomic character $\chi^\infty(14.1.1.4)$, by Weil pairing (13.5.7.6).

Prop. (14.1.6.4) [Serre]. Assume $E \in E_{\ell} / \mathbb{Q}$ is non-CM, then there exists $N_0 \in \mathbb{Z}_+ \text{ s.t. } \rho_{E,N}$ is surjective for any $N \geq N_0$.

Proof: □

Conj. (14.1.6.5) [Serre’s Uniformity Problem]. There exists a number $N_0 \in \mathbb{Z}_+ \text{ s.t. for any } E \in E_{\ell} / \mathbb{Q} \text{ non-CM, } \rho_{E,N}$ is surjective for any $N \geq N_0$.

Proof: □

7 Representation from Automorphic Forms

Prop. (14.1.7.1) [Representation Associated to a Cusp Form].

Conj. (14.1.7.2) [Serre]. Let $\rho : \text{Gal}_\mathbb{Q} \to GL(2, F_q)$ be an odd smooth representation (i.e. $\det(\rho(\sigma_\infty)) = -1$), then there exists a normalized Hecke eigenform in $S_2(N, \chi)$ s.t. $\overline{\rho}_f = \rho$. 
14.2  p-adic Hodge Theory

Main references are [Berger, Galois representations and $(\varphi, \Gamma)$-modules], [Introduction to p-adic Hodge, Xavier Caruso] and [notes on p-adic Hodge, Conrad].

This is a continuation of the section Galois Representations.

1 Intro

Remark (14.2.1.1). Delete this subsection. Cf.[Conrad].

Let $K$ be a $p$-adic field and $K_\infty = K(\mu_{p^{\infty}})$, $\Gamma = \text{Gal}(K_\infty/K)$, then there exists a $E = E_{K_\infty/K} \in p$-Field with a canonical isomorphism

$$\text{Gal}_{K_\infty} \cong \text{Gal}_{E}.$$ 

Thus

$$\text{Rep}_{Z_p}(\text{Gal}_{K_\infty}) \cong \text{Rep}_{Z_p}(\text{Gal}_{E}) \cong \varphi-\text{Mod}_{A_E}.$$ 

Then because a representation of $\text{Gal}_K$ can be viewed as a representation of $\text{Gal}_{K_\infty}$ with certain descent datum, and this induces an equivalence of categories

$$\text{Rep}_{Z_p}(\text{Gal}_K) \cong (\varphi, \Gamma)-\text{Mod}_{A_E}.$$ 

2 $(\varphi, \Gamma)$-modules

Main references are [Fontaine90: Représentations p-adiques des corps locaux],[Fontaine94a: Le corps des périodes p-adiques] and [Fontaine94b: Représentations p-adiques semi-stables] but I cannot understand French so [Foundations of Theory of $(\varphi, \Gamma)$-modules over the Robba Ring] is used and I’m mostly following [Berger, Galois representations and $(\varphi, \Gamma)$-modules].

Def. (14.2.2.1) [\varphi-module]. Let $M$ be an $A$-module and $\sigma : A \to A$ is a ring map. Then an additive map $\varphi : M \to M$ is called $\sigma$-semi-linear iff $\varphi(am) = \sigma(a)\varphi(m)$ for $a \in A$. A \varphi-module over $(A, \sigma)$ is just an $A$-module $M$ with a $\sigma$-semi-linear $\varphi$. The category of $\varphi$-modules over $A$ is denoted by $\varphi-\text{Mod}_A$.

Giving a $A$-module $M$ and a $\varphi : M \to M$, there is a map $\Phi : A \otimes_{\sigma, A} M = \sigma_\ast M \to M : \lambda \otimes m \mapsto \lambda\varphi(m)$, which is an $A$-module map iff $\varphi$ is $\sigma$-semi-linear.

If we define a ring $A_{\mathfrak{r}}[\varphi]$ as the free group $A[X]$ modulo the relation $Xa = \sigma(a)X$ and ring relations in $A$, then it is a ring. Then a $\varphi$-module over $(A, \sigma)$ is equivalent to a left $A_{\mathfrak{r}}[\varphi]$-module.

Thus $\varphi-\text{Mod}_A$ is a Grothendieck Abelian category with tensor products, and moreover, the kernel as $A_{\mathfrak{r}}[\varphi]$-module is the same as the kernel as a $A$-module.

Def. (14.2.2.2). If there is a map $\alpha : (A_1, \sigma_1) \to (A_2, \sigma_2)$ that commutes with $\sigma_i$, then we have a pullback from $\Phi M_1$ to $\Phi M_2$: $\alpha^\ast(M) = (A_2)_{\sigma_2}[\varphi] \otimes (A_1)_{\sigma_1}[\varphi] M(14.2.2.1)$.

Def. (14.2.2.3) [Étale \varphi-Modules]. If $A$ is Noetherian, then a $\varphi$-module $M$ is called étale iff it is f.g and the corresponding $\Phi : \sigma_\ast M \to M$ in(14.2.2.1) is a bijection. The subcategory of étale $\varphi$-modules is denoted by $\varphi-\text{Mod}^\text{et}$. 

In case when $\sigma$ is a bijection, $\Phi$ is a bijection iff $\varphi$ is a bijection.

Proof: Note that in this case $\sigma_\ast M \to M$ is a bijection by $\lambda \otimes m \mapsto \sigma^{-1}(\lambda)m$, so the rest is easy. □
Prop. (14.2.2.4). If \( A \) is Noetherian and \( A_\sigma \) is flat, then \( \varphi\text{-Mod}^{\text{ét}} \) is Abelian category.

Proof: 0 is the zero object, the canonical sum\&product are clearly étale. And we need to check the kernel and cokernel are étale. But we have an exact sequence \( 0 \to \ker \to M \to N \to \Coker \to 0 \) so we tensor with \( A_\sigma \) to get a morphism of sequences that \( \sigma_*M \to M, \sigma_*N \to N \) are both bijective, so by 5-lemma, it is bijection at kernel and cokernel, so they are étale.

Def. (14.2.2.5) [(\( \varphi, \Gamma \))-modules]. If \( A \) has an action of a group \( \Gamma \) that commutes with \( \sigma \), then a (\( \varphi, \Gamma \))-module is a \( \varphi \)-module with a semi-linear action of \( \Gamma \) that commutes with \( \varphi \).

If \( A, \Gamma \) has complete topologies and the action is continuous and \( \sigma \) flat, then a (\( \varphi, \Gamma \))-module \( M \) is called étale iff it is an étale \( \varphi \)-module and it has a topology that the action of \( \Gamma \) is continuous on \( M \).

Similar to \( \varphi \)-modules, (\( \varphi, \Gamma \))-modules forms a Grothendieck Abelian category with tensor products.

3 Isocrystals

Def. (14.2.3.1) [Isocrystals]. We consider a perfect field \( k \) and \( K = W(k)[1/p] \), \( K \) is equipped with the natural \( \sigma \) lifting the Frobenius. Define an isocrystal over \( K \) as a f.d. \( \varphi \)-modules \( V \) over \( K \) with \( \sigma = \sigma^a(14.2.2.1) \), where \( a \in \mathbb{Z}\setminus\{0\} \). We don’t care about this \( a \) much. \( \dim_K V \) is called the height of this isocrystal. The fact that \( k \) is perfect implies that the kernel and image of \( \varphi \) are \( K \)-vector subspaces.

Def. (14.2.3.2) [Hodge-Tate Weight]. For any (complete)\( W(k) \)-lattice \( M \) of \( D \), let \( a_n \) be the maximum integer that \( \varphi^a(M) \subset p^n M \), then we have \( a_{n+m} \geq a_m + a_n \), thus by (20.1.1.1), we have \( a_n/n \) converges to sup \( a_n/n = \lambda \). \( \lambda \) doesn’t depend on \( M \) because of the cofinality of lattices, and it is called the Hodge-Tate weight of \( D \).

Then a \( \varphi \)-module \( D \) over \( K \) is called effective if there is a (complete)\( W(k) \)-lattice \( M \) of \( D \) that \( \varphi(M) \subset M \).

Lemma (14.2.3.3). Let \( M \) be a lattice of \( D \) that \( \varphi^{h+1}(M) \subset p^{-1}M \), where \( h \) is the dimension of \( D \), then \( D \) is effective.

Proof: Let \( M_j = M + \varphi(M) + \ldots + \varphi^j(M) \), then \( M_j/M \subset p^{-1}M/M \), which is a \( k \)-vector space of dimension \( h \), then \( M_j = M_{j+1} \) for some \( j \), hence \( M_j \) is stable under \( \varphi \).

Prop. (14.2.3.4). \( \lambda \geq 0 \) iff \( D \) is effective. And \( \lambda = s/r \), where \( 1 \leq r \leq h \).

Proof: If \( D \) is effective, then \( a_n \geq 0 \), conversely, if \( a_n \geq 1 \), then \( M' = M + \varphi(M) + \ldots + \varphi^{n-1}(M) \) is stable under \( \varphi \), so \( D \) is effective.

For the second assertion, we first notice, if \( \lambda > 0 \), then \( \varphi \) is nilpotent on \( M/pM \), which is a \( k \)-vector space of dimension \( h \), then \( \varphi^h = 0 \) on \( M/pM \), so \( \lambda \geq 1/h \).

Now we find \( s, r \) that \( |r \lambda - s| \leq 1/(h+1) \), and \( \bar{\varphi} = p^{-s}\varphi^r \) has \( |\bar{\lambda}| \leq 1/(h+1) \), so (14.2.3.3) shows that \( \bar{\varphi} \) is effective, hence \( \bar{\varphi} \geq 0 \), and by what we have proved, \( \bar{\varphi} = 0 \), hence it is \( \lambda = s/r \).

Lemma (14.2.3.5). For a \( \varphi \)-stable \( W(k) \)-lattice \( M \) of \( D \), one has \( M = M_0 \oplus M_{>0} \), where \( \varphi \) is bijection on \( M_0 \) and topologically nilpotent on \( M_{>0} \).

Proof: We consider \( M/pM \), then by (2.2.4.5) under slight modification, we have a decomposition for \( M/pM \). This decompositions for different \( n \) are compatible, so taking an inverse limit gives a decomposition of \( M \) it self.
Def.(14.2.3.6)[Isotypical $\varphi$-Modules]. A $\varphi$-module is called pure(isotypical) of slope $\lambda = s/r \in \mathbb{Q}$ if $D$ admits a lattice $M$ on which $p^{-s}\varphi^r$ is a bijection. This is independent of $M$ because $\lambda$ is independent of $M$.

Prop.(14.2.3.7)[Dieudonné-Manin]. If $M$ is a $\varphi$-module over $W(k)[\frac{1}{p}]$ where $k$ is a perfect field, then $M$ is a finite sum of modules pure of slopes $\lambda_i$. This is called the isocrystal decomposition of $M$.

Proof: We use the $\tilde{\varphi}$ as in the proof of(14.2.3.4), we see that $M$ has a decomposition $M_0 \oplus M_{>0}$ by(14.2.3.5), and $M_0 \neq 0$ by definition. Then we use induction to get the result.

Lemma(14.2.3.8). If $k$ is a separably closed field and $V$ is a $\varphi$-module with $a \geq 1$ of slope 0, then $V$ has a basis of elements fixed by $\varphi$, and $1 - \varphi$ is a surjection.

If $A = W(k)$ is a ring with $k$ a separably close field and $V$ is a $\varphi$-module over $A$ with $a \geq 1$ and slope 0, then $V$ has a basis of elements fixed by $\varphi$, and $1 - \varphi$ is a surjection.

Proof: We choose a $e_0 \in V$, and set $e_i = \varphi^i(e_0)$, and suppose $e_d = a_0 e_0 + \ldots + a_d e_{d-1}$, then if we consider the equation $\varphi(b_0 e_0 + \ldots + b_{d-1} e_{d-1}) = b_0 e_0 + \ldots + b_{d-1} e_{d-1}$, then we need to assure $b_{d-1}$ is a zero of
\[
x = a_0^{d-1} x^d + a_1^{d-2} x^{d-1} + \ldots + a_{d-1} x^1
\]
which is separable, so it has a non-zero solution in $k$, so $\varphi$ has a fixed point $v$. By induction, we have $V/k \cdot v$ admits a basis fixed by $\varphi$. We know that $1 - \varphi : k \cdot v \to k \cdot v : x \mapsto (x - x^q)$ is surjective, so we can adjust the coefficient of $v$ to get a basis of $V$ fixed by $\varphi$. And meanwhile we proved $1 - \varphi$ is surjective.

The second assertion follows from successive approximation, as $x^p - x - a$ always has a root in $k$.

Def.(14.2.3.9). When $k$ is alg.closed, for $\lambda = s/r$, we define a $\varphi$-module over $K = W(k)[1/p]$ $E_\lambda = \mathbb{Q}_p^{-1} K e_i$ that $\varphi(e_i) = e_{i+1}$, and $\varphi(e_{r+1}) = p^r e_0$. In this case, $E_\lambda$ is irreducible.

Proof: If $D$ is a $W(k)$-lattice stable under $\varphi$, then we may assume it is pure of slope $d/h$ by(14.2.3.7), and then we find an element $y = \sum y_i e_i$ fixed by $p^{-d} \varphi^h$, then $p^h \varphi^h(y_i) = p^d y_i$, which by valuation is only possible when $sh = rd$, so $h \geq r$, so $D$ generate $E_\lambda$.

Prop.(14.2.3.10)[Dieudonné-Manin]. If $k$ is alg.closed, then any $\varphi$-module over $K$ has a unique decomposition as sums of $E_\lambda (14.2.3.9)$.

Proof: By(14.2.3.7) we assume $D$ is pure, then by(14.2.3.8) we find a basis $y_i$ that $\varphi^r(y_i) = p^r y_i$, then there is a map $E_\lambda \to D$. Since $E_\lambda$ is irreducible, this is injective, and we consider all $y_i$ until $E_\lambda^m \to V$ is surjective, then it is an isomorphism(this is like the case of simple modules).

Def.(14.2.3.11)[Tate Twist]. The Tate object $1(n), n \in \mathbb{Z}$ is the 1-dimensional isocrystal over $K_0$ that $\varphi = p^n \sigma$, so it is of slope $n$. And the Tate twist isocrystal is tensoring by $1(n)$. It preserves rank and shifts Hodge-Tate weight by $n$.

Filtered $(\varphi, N)$-Modules

Def.(14.2.3.12)[$\varphi$-Modules over $K$]. Let $K$ be a finite field extension of $\mathbb{Q}_p$ and $K_0$ be the maximal unramified subextension of $K$, $K_0 = W(k)$ where $k$ is the residue field of $K$, then a $\varphi$-module over $K$ as a $\varphi$-module over $(K_0, \sigma)$ where $\sigma$ is the absolute Frobenius.
Def. (14.2.3.13) [(\(\varphi, N, \text{Gal}(L/K)\))-Modules]. Let \((R, K, k)\) be a CDVR of mixed characteristic \((0, p)\), let \(L\) be a Galois extension of \(K\) with residue field \(k_L\). Let \(L_0\) be the maximal unramified subextension of \(K_0 = W(k)[1/p]\) in \(L\). Let \(\sigma\) be a Frobenius endomorphism of \(L_0\).

Then I define the category of \((\varphi, N, \text{Gal}(L/K))\)-modules as the category of f.d. \(L_0\)-spaces \(V_0\) with
- a \(\sigma\)-semi-linear endomorphism,
- a \(L_0\)-linear endomorphism \(N\),
- a semi-linear continuous action of \(\text{Gal}(L/K)\) (w.r.t the discrete topology).

That satisfies:
- \(N\varphi = p\varphi N\),
- \(N, \varphi\) commutes with \(\text{Gal}(L/K)\)-actions.

The category of all \((\varphi, N)\)-modules is an Abelian category, similar to that of \(\varphi\)-modules (14.2.2.1).

Notice that the condition implies \(N\) maps the subspace of \(\varphi\)-slope \(l\) to the subspace of \(\varphi\)-slope \(l - 1\), in particular, \(N\) is nilpotent.

Def. (14.2.3.14) [Filtered \((\varphi, N, \text{Gal}(L/K))\)-Modules]. A filtered \((\varphi, N, \text{Gal}(L/K))\)-module \((D, \varphi_D, N, \text{Gal}(L/K), \text{Fil})\) is a \((\varphi, N, \text{Gal}(L/K))\)-module \((D, \varphi_D, N, \text{Gal}(L/K)) \in (\varphi, N)\text{-Mod}_{L/K}\) together with a finite filtration \(\text{Fil}\) on \(D_L = D \otimes_{L_0} L\) in the category of vector spaces over \(L\). The category of filtered \((\varphi, N, G_{L/K})\)-modules over \(K\) is denoted by \((\varphi, N)\text{-Fil} \text{Mod}_{L/K}\).

The category \(\varphi\text{-Fil} \text{Mod}_{L/K}\) of filtered \(\varphi\)-modules (isocrystals) \((D, \varphi_D)\) over \(K\) is the sub Abelian category of filtered \((\varphi, N)\)-modules that \(N = 0\).

Prop. (14.2.3.15) [HN-Formalism for Filtered \(\varphi\)-Modules]. The category \(\varphi\text{-Fil} \text{Mod}_{K/K_0}(14.2.3.14)\) is an HN-formalism where \(A\) is the Abelian category of \(\varphi\)-modules (14.2.3.13), the rank is defined as usual and

\[
\deg((D, \varphi_D, \text{Fil})) = t_H(D_K, \text{Fil}) - t_N(D, \varphi_D)
\]

where \(t_H\) is the Hodge-Tate degree (3.2.4.27) and \(t_N = v_p(\det(\varphi_D; D))\). This is an HN-formalism.

Proof: The proof is clear, the same as that of (3.2.4.27). □

Def. (14.2.3.16) [Weakly Admissible \(\varphi\)-Modules]. The category \(\varphi\text{-Fil} \text{Mod}_{K/K_0}^{weak, adm}\) of weakly admissible \(\varphi\)-modules is those that are semistable of slope 0 w.r.t the HN-formalism. It is an Abelian category by (3.2.4.33).

Prop. (14.2.3.17) [Faltings]. The category \((\varphi, N)\text{-Fil} \text{Mod}_{L/K}^{weak, adm} \subset (\varphi, N)\text{-Fil} \text{Mod}_{L/K}\) is stable under tensor products.

Proof: [Tensor Products in p-adic Hodge, Totaro, P9,12]. □

4 Admissible Representations

Def. (14.2.4.1) [Admissible Representations]. Let \(G \in \text{Gr}_B^{top}\) and \(E\) a topological field and \(B\) a topological \(E\)-algebra s.t. \(B \in \text{Rep}_E(G)\). Then \(V \in \text{Rep}_E^{fil}(G)\) is called \(B\)-admissible if the \(B\)-semi-linear representation \(B \otimes_E V\) is trivial.

The category of f.d. \(B\)-admissible \(E\)-representations of \(G\) are denoted by \(\text{Rep}_E^{B, adm}(G)\).
**G\textsubscript{K}-Regularity**

**Def. (14.2.4.2) [G\textsubscript{K}-Regularity]**. We want to establish a numerical criterion for recognizing B-admissible representations. For this goal, suppose B satisfies the following axioms:

- (H1): B is a domain.
- (H2): (\text{Frac}(B))^G = B^G.
- (H3): if b \neq 0 \in B and Eb is stable under G-action, then b \in B^*.

B is called G\textsubscript{K}-regular if it satisfies these three conditions. Notice a field is clearly G\textsubscript{K}-regular.

**Cor. (14.2.4.3)**. Notice that (H3) implies B^G is a field, because for b \in B^G, Eb is clearly stable under G-action, thus b is invertible.

Also the morphism

\[ \alpha_W : B \otimes_{B^G} W^G \to W \]

is injective for all W \in \text{Rep}_B(G) free of finite rank over B. In particular, this is true for W = B \otimes_E V for a f.d. E-linear representation V of G.

**Proof**: To show \( \alpha_W \) is injective, it suffices to show a linear basis \{e_i\} of \( W^G \) over \( B^G \) is linearly independent over \( B \): Suppose \( \sum a_i e_i = 0 \), where \( a_i \in B \), with the number of nonzero coefficients minimal, and \( a_1 \neq 0 \), then dividing \( a_1 \in \text{Frac}(B) \), we assume \( a_1 = 1 \), and then acting by \( g - \text{id} \), we get

\[ \sum (g(a_i) - a_i)e_i = 0 \]

and this has smaller non-zero elements, unless \( a_i \) is fixed by \( g \) for any \( g \in G \), so \( a_i \in \text{Frac}(B)^G = B^G \) by (H2), contradiction.

**Prop. (14.2.4.4) [Galois Extension]**. Let \( L \) be a finite Galois extension of \( E \), then

\[
\text{Rep}_E^d(\text{Gal}(L/E)) \subset \text{Rep}_E^{L-\text{adm}}(\text{Gal}(L/G)).
\]

**Proof**: We prove that the morphism \( \alpha_W : B \otimes_{B^G} W^G \to W \) is an isomorphism: it is an isomorphism by (14.2.4.3), for the surjectivity. Let \( \lambda_i \) be a basis of \( L \) over \( E \), then by (2.2.5.1), \( \lambda_i : G \to K \) are linearly independent, so there are some \( \mu_i \in K \) that \( \sum \mu_i g(\lambda_i) = 1 \) for \( g = \text{id} \) and 0 otherwise. Then \( \sum \mu_i \text{tr}(\lambda_i x) = x \) for all \( x \in W \), showing surjectivity.

**Prop. (14.2.4.5)**. If \( B \) is G\textsubscript{K}-regular (14.2.4.2), \( V \in \text{Rep}_E(G) \) be f.d. and \( W = B \otimes_E V \), then the following are equivalent:

- \( W \) is trivial.
- \( \alpha_W(14.2.4.3) \) is an isomorphism.
- \( \text{dim}_{B^G} W^G = \text{dim}_E V \).

**Proof**: 1, 2 are equivalent by (14.2.4.3), as \( B^G \) is a field. Also 2 \( \implies \) 3 is clear.

3 \( \implies \) 2: \( \alpha_W : B \otimes_{B^G} W^G \to B \otimes_E V \) is a B-linear morphism of two finite free B-modules, then it suffices to show the determinant map is an isomorphism. Let \( v_1, \ldots, v_d \) be an E-basis of \( V \) and \( w_1, \ldots, w_d \) a B\textsuperscript{G}-basis of \( W^G \). Let \( b \) be the unique element of \( B \) that

\[ \alpha_W(v_1) \wedge \ldots \wedge \alpha_W(v_d) = bw_1 \wedge \ldots \wedge w_d \]

then \( gb = \eta b \) for \( g \in G \) where \( \eta \) is determined by the identity \( \alpha_W(gv_1) \wedge \ldots \wedge \alpha_W(gv_d) = \eta \alpha_W(v_1) \wedge \ldots \wedge \alpha_W(v_d) \). Now the E-space of \( v_1, \ldots, v_d \) is \( V \), which is stable under G action, thus \( \eta \in E \), and then by (H3) \( b \in B^* \), so we are done.
Cor. (14.2.4.6) [Category of Admissible Representations]. If $B$ is $\text{Gal}_K$-regular, then the subcategory $\text{Rep}_E^B\text{-adm}(\text{Gal}_K) \subset \text{Rep}_E(\text{Gal}_K)$ is stable under subobjects and quotients.

Proof: Given an exact sequence $0 \to V_1 \to V \to V_2 \to 0$ in the category $\text{Rep}_E(\text{Gal}_K)$, tensoring $B$ and taking $G$-fixed points, we get an exact sequence

$$0 \to (B \otimes_E V_1)^G \to (B \otimes_E V)^G \to (B \otimes_E V_2)^G$$

from which we derive the inequality $\dim_{B,C}(B \otimes_E V)^G \leq \dim_{B,C}(B \otimes_E V_1)^G + \dim_{B,C}(B \otimes_E V_2)^G$.

Now we have $\dim_{B,C}(B \otimes_E V_1)^G \leq \dim_{E} V_1$ by (14.2.4.3), so

$$\dim_{B,C}(B \otimes_E V)^G \leq \dim_{B,C}(B \otimes_E V_1)^G + \dim_{B,C}(B \otimes_E V_2)^G \leq \dim_{E} V_1 + \dim_{E} V_2 = \dim_{E} V.$$

But this is an equality because $V$ is $B$-admissible, thus $V_1, V_2$ are all $B$-admissible. \hfill $\square$

5 $\mathbf{C}_p$-Admissibility and Hodge-Tate Representations

Cohomology of $\text{Gal}_K$-actions on $\mathbf{C}_p(\psi)$

Def. (14.2.5.1) [Notations]. Let $K$ be a $p$-adic number field, $K_\infty$ is an Abelian extension of $K$ that the Galois group $\Gamma$ has a subgroup $\Gamma_0$ of finite index that $\Gamma_0 \cong \mathbb{Z}_p$, and $H_K = G_{K,K_\infty}$. The natural examples is $K_\infty = K(p^{1/\infty})$.

Let $\Gamma_m = \Gamma_0^m$ and $K_m$ the fixed field of $\Gamma_m$.

Decompose $\Gamma = \Sigma \times \Gamma_0$ and let $\gamma$ be a topological generator of $\Gamma_0$, then every element of $\Gamma_0$ can be written as $\gamma^t$ for some $t \in \mathbb{Z}_p$. Denote $\gamma^t = \gamma^p^t$.

$\psi : G_K \to \Gamma \to \mathbb{Z}_p^*$ be a character factoring through $\Gamma$, then we can form a representation $\mathbf{C}_p(\psi)$ of $G_K$ on $\mathbf{C}_p$ that $\rho(\sigma)(x) = \psi(\sigma)\sigma(x)$. This is an action because $G_K$ acts trivial on $\mathbb{Z}_p^*$.

Lemma (14.2.5.2). Given an $\sigma \in G_K/Q_{q_0}$, if $x, y \in m_{C_p}$ that $x \equiv y \mod \pi_n^k$, then $[\pi_K]^\sigma(\pi^k) \equiv [\pi_K]^\sigma(\pi_n^k)$ mod $\pi_n^{k+1}$, where $f^\sigma$ is given by action of $\sigma$ on the coefficients.

Proof: This is because the coefficients of $[\pi_K]^\sigma$ are divisible by $\pi_K$ except for degree $q$, where it is $x^q - y^q = (x - y)(x^{q-1} + x^{q-2}y + \ldots + y^{q-1})$ which is divisible by $\pi_n^{k+1}$ because the residue field of $K$ is of order $q$. \hfill $\square$

Prop. (14.2.5.3). If we let the action of $\sigma \in G(K/Q_{q_0})$ on the residue field giving by $\overline{\sigma} : k_K \to \mathbb{F}_p : x \mapsto x^{q_0}$, where $q_0 = p^\alpha$ is a $p$-power, given an element $\eta = (\eta_0, \eta_1, \ldots) \in TG$, we have $\eta^{q^\sigma} \equiv [\pi_K]^\sigma(\eta_n^{q^\sigma}) \mod \pi_K$, hence the above lemma (14.2.5.2) shows that $[\pi_K]^\sigma(\eta_n^{q^\sigma}) \equiv [\pi_K]^{q^\sigma}(\eta_n^{q^\sigma}) \mod \pi_K$, so $[\pi_K]^{q^\sigma}(\eta_n^{q^\sigma})$ is a Cauchy sequence, converging to an element $\mu_\sigma$ (don’t care about $\eta$).

If $g \in G_K$, then $g(\eta_n) = [\chi_K(g)](\eta_n)$, hence take $q_0$-th power, $g(\eta_n^{q^\sigma}) \equiv [\chi_K(g)]^{q^\sigma}(\eta_n^{q^\sigma}) \mod \pi_K$, then

$$[\chi_K(g)]^{q^\sigma}[\pi_K]^{q^\sigma}(\eta_n^{q^\sigma}) \equiv [\pi_K]^{q^\sigma}g(\eta_n^{q^\sigma}) = g([\pi_K]^{q^\sigma}\eta_n^{q^\sigma}) \mod \pi_K,$$

hence by limiting, $g(\mu) = [\chi_K(g)]^{q}(\mu)$. \hfill $\square$

Lemma (14.2.5.4).

$$v_p(\mu_\sigma) = \begin{cases} \frac{q_0}{e_K(q-1)} + \frac{1}{e_K} & n(\sigma) \neq 0 \\ \frac{1}{e_K(q-1)} + v_p(\sigma(\pi_K) - \pi_K) & n(\sigma) = 0 \end{cases}$$
14.2. P-ADIC HODGE THEORY

1434

Proof: By (7.5.3.27), we know the Newton polygon of $[\pi^n_K]^\sigma$. When $n(\sigma) \neq 0$, $v(\eta_1^n) = \frac{q_\sigma}{\varepsilon_K(q-1)} > \frac{1}{\varepsilon_K(q-1)}$, so the valuation of $[\pi_k]^\sigma(\eta_1^n)$ equals the valuation of its degree 1 term, which is $v(\pi_K\eta_1^n) = \frac{1}{\varepsilon_K(q-1)} + \frac{1}{\varepsilon_K}$.

Now we have by (14.2.5.3), we have $[\pi_k]^\sigma \eta_1^n \equiv \left[\frac{\pi_k}{\eta_1^n} \right] \mod \pi_2^n$, and $\frac{q_\sigma}{\varepsilon_K(q-1)} + \frac{1}{\varepsilon_K} < 2/\varepsilon_K$, so valuation already stable at degree 1, and $v(\mu_\sigma) = v([\pi_k]^\sigma(\eta_1^n)).$

If $q_\sigma = 1$, it’s more delicate, because degree 1 and degree $q$ term has the same minimal valuation, so they may jump to higher valuations. Notice $[\pi_k]^\sigma(\eta_n) = 0$, so $[\pi_k]^\sigma(\eta_n) = ([\pi_k]^\sigma - [\pi_k]^\sigma)(\eta_n)$. And we have by (12.2.2.26), for $x \in \mathcal{O}_K$, $v(\sigma(x) - x) \geq v(x) + v(\pi(\pi_k - 1) + \delta_{v(\sigma(x) - 1)}^v(\pi_k)$, with equality when $v_p(x) = q/\varepsilon_K$. So by the Newton polygon, the minimum valuation of the coefficient of $[\pi_k]^\sigma - [\pi_k]^\sigma$ appear at degree $p^n - 1$ and possibly $p^n$. The valuation of $\eta_n$ is too small $(\frac{1}{\varepsilon_K(p^n - 1)})$ that we don’t need to consider other degrees but can assure that degree $p^n - 1$ is of minimum valuation, which is $v(\eta_1^{n-1}) + v(\pi(\pi_k - \pi_k) = \frac{1}{\varepsilon_k(q-1)} + v_p(\pi(\pi_k - \pi_k)).$

\[\square\]

Prop. (14.2.5.5). For any $\sigma \in \text{Gal}(K/Q_p)\setminus\{\text{id}\}$, there is an element $\alpha_\sigma \in C_\sigma^*$ that $\sigma \circ \chi_K(g) = g(\alpha_\sigma)/\alpha_\sigma$ for all $g \in G_K$, where $\chi_K$ is the Lubin-Tate character.

Proof: We let $\alpha_\sigma = \log F_n(\mu_\sigma)$, by (14.2.5.4), $1/\varepsilon_K < \mu_\sigma < \infty$, so by the Newton polygon analysis of $\log F_n(7.5.3.28)$, $\alpha_\sigma$ has the same valuation of $\mu_\sigma$, in particular, $\alpha_\sigma \neq 0$. Then

$$g(\alpha_\sigma) = \log F_n(\mu_\sigma)) = (\log F(\chi_K(\sigma)))^\sigma(\mu_\sigma) = (\chi_K(\sigma) \cdot \log F^n(\sigma)^\sigma(\mu_\sigma) = \sigma(\chi_K(\sigma)) \cdot \alpha_\sigma.$$

\[\square\]

Cor. (14.2.5.6). $\log p(\sigma(\chi_K(\sigma))) = g(\log(\alpha)) - \log p(\alpha_\sigma).$

Prop. (14.2.5.7). Now we compute $H^1(G_K, C_\sigma(p))$. There is an inf-res exact sequence

$$0 \to H^1(\Gamma_K, K_\infty(\psi)) \to H^1(G_K, C_\sigma(p)) \to H^1(H_K, C_\sigma(p))$$

Then $H^1(H_K, C_\sigma(p)) = 0$. The first two vanish iff $\psi$ is of infinite order, and is a $K$-vector space of dimension 1 if $\psi$ is of finite order.

Proof: For the first assertion, $\psi$ is trivial on $H_K$, so $C_\sigma(p(\psi)) \cong C_\sigma$ as $H_K$-representation, so it suffice to show for $\psi = \text{id}$. Let $f$ be a cocycle, as $H_K$ is compact, $f(H_K) \in \tilde{\mathcal{O}}_C$, for some integer $k$. So the lemma below (14.2.5.8) shows that we can move $f$ cohomologically to higher valuation, i.e.

$$f(g) = \sum x_i - g(\sum x_i),$$

so $f$ is a coboundary.

For the second assertion, we assume $\Gamma_K \neq Z_p$, for this case, see remark (14.2.5.9) below.

Let $\gamma$ be a topological generator of $\Gamma_K = 1 + p^kZ_2^k$, $k \geq 0$, because $Z_p$ are all topological cyclic groups except for $Z_2^k \cong Z/2^kZ \oplus Z_2$, and $\gamma_\sigma$ be a topological generator of $\Gamma_{F_n}$ which is also a power of $\gamma$. By (10.1.3.22) we know $H^1(\Gamma_K, K_\infty(\psi)) = K_\infty(\psi)/1 - \gamma$.

For $n$ large, we have a decomposition $K_\infty(\psi) = K_n(\psi) \oplus X_n(\psi)$ by (12.2.3.27), and $1 - \gamma_n$ is invertible on $X_n(\psi)$. Now $1 - \gamma_n = (1 - \gamma)(1 + \gamma + \ldots + \gamma^{k-1})$, so $1 - \gamma$ is also invertible in $X_n(\psi)$. And on $K_n(\psi)$, if $\psi$ is of infinite order, then $1 - \gamma$ is injective, otherwise $\psi = \psi(x)^{N} = \psi(x)^{N\gamma}$.

So it is also surjective because it is a $K$-linear mapping of $K_n$. So $K_\infty(\psi)/1 - \gamma = 0$. If $\psi$ is of finite order then $K_n(\psi) \cong K_n$ as $K$-module when $n$ is large enough that $\gamma$ factors through $K_n$, by (10.1.3.1). So $K_n/1 - \gamma = K_n/\ker(tr_{K_n/K}) = K$.

\[\square\]

Lemma (14.2.5.8). If $f : H_K \to p^n\mathcal{O}_C_\psi$ is a continuous cocycle, then there exists an $x \in p^{n-1}\mathcal{O}_C_\psi$, that the cohomological cocycle $g \mapsto f(g) - (x - g(x))$ has values in $p^{n+1}\mathcal{O}_C_\psi$.  

Proposition (14.2.5.10). For all $p > 2$, the ring $\mathcal{O}_{C_p}$ is open in $\mathcal{O}_p$, so there is a finite extension $L/K$ that $f(H_L) \in p^{n+2}\mathcal{O}_{C_p}$.

Proof: $p^{n+2}\mathcal{O}_{C_p}$ is open in $p^n\mathcal{O}_{C_p}$, so there is a finite extension $L/K$ that $f(H_L) \in p^{n+2}\mathcal{O}_{C_p}$.

By (12.2.3.21), there is a $z$ that $f_L/z_{K_\infty} = p$, so there is a $y \in p\mathcal{O}_{L_\infty}$ such that $f_L/y_{K_\infty} = 1$.

Now for a set of representatives $Q$ of $H_K/H_L$, denote $x_Q = \sum_{h \in Q} h(y)f(h)$, then for $g \in H_K$, $g(Q)$ is also a set of representative, and $g(x_Q) = \sum_{h \in Q} gh(y)gfh(h) = \sum_{h \in Q} gh(y)(f(g) - f(h)) = x_g(Q) - x_Q$, as $h(y) = 1$. So $f(g) - (x_g - g(x_Q)) = x_g(Q) - x_Q$. The RHS is in $p^{n+2}\mathcal{O}_{C_p}$, because:

- if we let $gh_i = g(h_i)a_i$, where $a_i \in H_L$, then $x_g(Q) - x_Q = \sum_{i} h_i(gh_i(a_i) - \sum_{i} h_i(g_i))f(h_i(i))h_i(g_i(i)h_i(g_i(i)) = \sum_{i} h_i(g_i(i))$, which is in $p^{n+1}$ because $h_i(g_i(i)) \in p^{-1}\mathcal{O}_{C_p}$ and $f(a_i) \in p^{n+2}\mathcal{O}_{C_p}$ by the choice of $L$.

Remark (14.2.5.9). In case $\Gamma = \mathbb{Z}_2$,

$$0 \to H^1(\{ \pm 1 \}, K(\psi)) \to H^1(\mathbb{Z}_2^*, \mathbb{K}_\infty(\psi)) \to H^1(\mathbb{Z}_2^*, \mathbb{C}_p(\psi))$$

$H^1(\{ \pm 1 \}, K(\psi)) = 0$ whether $\psi(-1) = 1$ or $-1$. And by the same proof as above, possibly replace $X_n$ with $X_{n+1}$, to remedy the singularity of $p = 2$, $H^1(1 + 2\mathbb{Z}_2^*, \mathbb{C}_p(\psi)) = K$, with generator $[g \mapsto \chi(g)^{-1}\tau^{-1}(a)]$ for some $a$. This cocycle extends to a cocycle of $\mathbb{Z}_2^*$, so the map is surjective.

Proposition (14.2.5.10). The 1-dimensional $K$-vector space $H^1(G_K, \mathbb{C}_p)$ is generated by the cocycle $[g \mapsto \log_p \chi(g)]$.

Proof: By the proof of (14.2.5.7), we know that $H^1(\Gamma, K_n) \to H^1(G_K, \mathbb{C}_p)$ is an isomorphism. For $\alpha \in K$, if $\chi(g) = \gamma^k$, then $f(\alpha)(g) = (1 + \gamma + \cdots + \gamma^{k-1})(\alpha) = \log_p(\chi(g))/\log_p(\gamma)$. So by continuity, $f$ is a multiple of $[g \mapsto \log_p(\chi(g))]$.

Lemma (14.2.5.11). And $f \in \text{Hom}(U_K^b, \mathbb{Q}_p)$ is of the form $f(g) = \text{tr}_{K/\mathbb{Q}_p}(\beta_f \log_p \chi(g))$ for some $\beta_f \in K$.

Proof: By (12.4.2.23), $\chi_K$ is a canonical isomorphism $I_K^b \cong \mathcal{O}_K^*$. Any $f \in \text{Hom}(\mathcal{O}_K^*, \mathbb{Q}_p)$ is of the form $f(g) = \text{tr}_{K/\mathbb{Q}_p}(\beta_f \log_p(g))$ for some $\beta_f \in K$, because: by (12.2.3.8), when $n$ is large, $\log_p$ is a bijection between $U_K^n$ and $\pi_K^n \mathcal{O}_K$.

$\pi_K^n \mathcal{O}_K \to \mathbb{Q}_p$ can be extended to a map $K \to \mathbb{Q}_p$ as $\mathbb{Q}_p$ is divisible. Now trace is an invertible bilinear form on $K$, so the assertion is true on $U_K^n$ for some $n$, and because $U_K^n$ is of finite index in $\mathcal{O}_K^*$ and $\mathbb{Q}_p$ is of char 0, this is true for all $\mathcal{O}_K^*$.

Proposition (14.2.5.12). The map $H^1(G_K, \mathbb{Q}_p) \to H^1(G_K, \mathbb{C}_p)$ is given as follows: $f \in H^1(G_K, \mathbb{Q}_p)$ must factor through $G_K^b$, if the restriction of $f$ to $I_K^b$ corresponds to $\beta_f$, then $f$ maps to $\beta_f[g \mapsto \log_p \chi(g)]$.

Proof: $f(g) = \text{tr}_{K/\mathbb{Q}_p}(\beta_f \log_p \chi(g))$ on $I_K$, but this map extends to map on $G_K$. So $f(g) = \text{tr}_{K/\mathbb{Q}_p}(\beta_f \log_p \chi(g)) + c(g)$ for a unramified map $c$ on $G_K$.

Now by (10.1.3.21), $H^1(G, \mathbb{Q}_p^*)/\mathbb{Q}_p$ vanish because $H^1(G, \mathbb{F}_p)$ vanish (10.1.3.1), so there is a $z \in \mathbb{Q}_p^*$ that $c(g) = g(z) - z$. And

$\text{tr}_{K/\mathbb{Q}_p}(\beta_f \log_p \chi(K(g))) = \sum_{\sigma} \sigma(\beta_f \log_p \chi(K(g))) = \beta_f \text{tr}_{K/\mathbb{Q}_p}(\log_p \chi(K(g))) + \sum_{\sigma} (\beta_f) - \beta_f) \sigma(\log_p \chi(K(g)))$.

Notice (14.2.5.5) gives a $\beta_f$ that $\sigma(\log_p \chi(K(g))) = g(\beta_f) - \beta_f$, and $\text{tr}_{K/\mathbb{Q}_p}(\log_p \chi(K(g))) = \log_p \chi(g)$ because $(N_K/\mathbb{Q}_p \chi(K(g)))^{-1} = (\chi(g))^{-1}$, as they both correspond via local CFT to the element in $G_K^b$ which acts by $g$ on $L_\pi$ and id on $K^ur$. Thus the result.
14.2. \textit{P-Adic Hodge Theory}

\textbf{C}_p\text{-Admissibility}

\textbf{Prop.}(14.2.5.13)[\textit{Variant of Hilbert’s Theorem90}]. Any f.d. \(\widehat{K}_{ur}\)-semi-linear representation of \(\text{Gal}(K_{ur}/K)\) is trivial.

\textit{Proof:} Denote by \(\mathcal{O}\) the ring of integers of \(\widehat{K}_{ur}\) and \(m\) the maximal ideal, Let \(W\) be a f.d. \(\widehat{K}_{ur}\)-semi-linear representation, \((v_{1,0}, \ldots, v_{d,0})\) a basis of \(W\) over \(\widehat{K}_{ur}\) and \(\mathcal{O}_W\) the \(\mathcal{O}\)-span of \((v_{1,0}, \ldots, v_{d,0})\), then we are going to construct a sequence of tuples \((v_{1,n}, \ldots, v_{d,n})\) that \(v_{i,n+1} \equiv v_{i,n} \mod m^n\) and \(\text{Frob}_q(v_{i,n}) \equiv v_{i,n} \mod m^n\) for all \(i\) and \(n\).

Use induction on \(n\): the case \(n = 1\) follows from the fact \(\mathcal{O}_W/m\mathcal{O}_W\) is trivial as a \(\widehat{k}\)-semi-linear representation of \(G(\widehat{k}/k)\). To prove this, notice there is a finite extension \(l\) of \(k\) and an \(l\)-semi-linear representation \(W_L\) of \(G_{l/k}\) that \(\widehat{k} \otimes_l W_L \cong \mathcal{O}_W/m\mathcal{O}_W\), then the assertion follows from Hilbert’s theorem90(10.1.3.16).

For general \(n\), we are looking for vectors \(w_1, \ldots, w_d\) in \(\mathcal{O}_W\) that \(\text{Frob}_q(v_{i,n} + \pi^n w_i) \equiv v_{i,n} + \pi^n w_i \mod m^{n+1}\), which is equivalent to \(\text{Frob}_q w_i - w_i = \frac{\text{Frob}_q v_{i,n} - v_{i,n}}{\pi^n} \in \mathcal{O}_W/m\mathcal{O}_W\). To prove this, notice \(\text{Frob}_q - \text{id}\) is surjective on \(\mathcal{O}_W/m\mathcal{O}_W\), which follows from the fact \(\mathcal{O}_W/m\mathcal{O}_W\) is trivial as proved above and \(\text{Frob}_q - \text{id}\) is surjective on \(\widehat{k}\).

Now \(v_i, n\) are Cauchy sequences and they converge to a tuple \(v_i\) that \(G_{K_{ur}/K}\) acts trivially and it is an \(\mathcal{O}\)-basis of \(\mathcal{O}_W\), as its reduction modulo \(m\) is a basis of \(\mathcal{O}_W/m\mathcal{O}_W\), so it is a \(\widehat{K}_{ur}\)-basis of \(W\).

\textbf{Remark}(14.2.5.14). Note that this proposition implies that any unramified f.d. representation of \(\text{Gal}_K\) is \(\widehat{K}_{ur}\)-admissible hence \(C_p\)-admissible, which is a special case of(14.2.5.15).

\textbf{Prop.}(14.2.5.15)[\textit{C}_p\text{-Admissibility}]. Let \(K\) be a finite extension of \(\mathbb{Q}_p\) and \(G_K = G_{\widehat{k}/k}\), then a f.d. \(\mathbb{Q}_p\)-representation of \(G_K\) is \(C_p\)-admissible iff the inertia group \(I_K\) acts on \(V\) through a finite quotient.

\textit{Proof:} Cf.\([p\text{-adic Period Rings Intro, P18}].\) ?

\textbf{Cor.}(14.2.5.16)[\(H^0\)]. \(H^0(\text{Gal}_K, C_p(\psi)) = (C_p(\psi))^{\text{Gal}_K} = K\) if \(\psi\) is of finite order, and vanish if \(\psi\) is of infinite order.

\textit{Proof:} The cyclotomic extension of \(K\) thus also the cyclotomic character of \(G_K\) is infinitely unramified, thus \(\chi_{cycl}^s\) factors through a finite quotient iff \(s = 0\). And \(H^0(G_K, C_p(\psi)) = K\) iff \(\mathbb{Q}_p(\psi)\) is admissible, by Ax-Sen-Tate(12.1.3.9), so we are done.

\textbf{Cor.}(14.2.5.17)[\textit{Potentially Unramified}]. If \(\eta : G_K \to \mathbb{Z}_p^*\) is a character and there is \(y \in C_p^*\) that \(\eta(g) = g(y)/y\), then there exists a finite Abelian extension \(L\) of \(K\) that \(\eta|_{G_L}\) is unramified, i.e. \(\eta\) is potentially unramified.

6 Sen’s Theory and Hodge-Tate Representations

\textbf{Remark}(14.2.6.1). Sen’s theory is to go further than \(C_p\)-admissible representations and classify all \(C_p\)-semi-linear representations.

\textbf{Prop.}(14.2.6.2)[\textit{Hilbert’s Theorem90 for Gal(\(\overline{K}/K_{\infty}\))}]. Any \(W \in \text{Rep}_{C_p}(G_K)\) is trivial as a \(C_p\)-semi-linear representation of \(\overline{K}/K_{\infty}\). In particular, there is an isomorphism \(\mathcal{C}_p \otimes_{\widehat{K}_{\infty}} \overline{K}/K_{\infty} \cong W\).
Proof: The proof is similar to that of (14.2.5.13).

Let \( \mathcal{O}_W \) be any \( \mathcal{O}_{G_{\infty}} \)-lattice in \( W \). Firstly we construct a \( \mathbb{C}_p \)-basis \( w_1, \ldots, w_d \) of \( W \) that \( w_i \in \mathcal{O}_W \) and \( gw_i \equiv w_i \mod p^2 \mathcal{O}_W \) for all \( g \in G_{\overline{K}/K_{\infty}} \) and \( p \mathcal{O}_W \subset \mathcal{O}_{\mathbb{C}_p} w_1 \oplus \cdots \oplus \mathcal{O}_{\mathbb{C}_p} w_d \).

By continuity there is a finite Galois extension \( L/K \) that \( ? \) \( \text{Cf.}[p\text{-adic Hodge Intro, P23}]. \)

Prop. (14.2.6.3). The next step in Sen’s theory is to study the \( \hat{K}_{\infty} \)-semi-linear representation of \( \Gamma_K \). To this attempt, Sen considers the subspace of \( \Gamma_K \)-finite vectors in \( W \), they form a vector space over \( K_{\infty} \).

Then for any \( \hat{K}_{\infty} \)-semi-linear representation \( W \) of \( \Gamma_K \), there exists an integer \( r \) and a basis \( (v_1, \ldots, v_d) \) of \( W \) that the \( K_r \)-span of \( v_i \) are stable under \( \Gamma_K \)-actions. Obviously, these \( v_i \) are \( \Gamma_K \)-finite.

Proof: \( \text{Cf.}[p\text{-adic Hodge Intro, P25}]. ? \)

Cor. (14.2.6.4) [Sen’s Operator]. Combining the previous two propositions, let \( W \in \text{Rep}_{\mathbb{C}_p}(\Gamma_K) \), denote \( \hat{W}_\infty = W^{G_{\overline{K}/K_{\infty}}} \) and \( W_\infty \) the set of finite vectors of \( \hat{W}_\infty \), then \( \mathbb{C}_p \otimes_{K_{\infty}} W_\infty \to W \) is an isomorphism. Let \( v_1, \ldots, v_d \) be given by (14.2.6.3), \( W_r = \oplus K_r v_i \). For \( g \in \Gamma_K \), let \( \rho_W(g) \) be the endomorphism of \( W_r \) given by action of \( g \), then \( \rho_W(\gamma_s) \) is linear when \( s \geq r \), and because \( \gamma_s \) converges to id, \( \log \rho_W(\gamma_s) \) is defined for \( s \) large. Then Sen’s operator \( \Phi_W \) is defined to be \( \Phi_W = \frac{\log \rho(\gamma_s)}{p^s} \), or equivalently \( \Phi_W(v) = \lim_{t \to 0} \left( s(t) - v \right) \).

Sen’s operator is defined over \( K \), as it commutes with \( \Gamma_K \) seen from the limit form, and its kernel is the \( \mathbb{C}_p \)-subspace of \( W \) generated by elements invariant under \( \Gamma_K \).

Proof: It is evident that fixed points of \( \Gamma_K \) are killed by \( \Phi_W \). Conversely, the kernel of \( \Phi_W \) on \( W_\infty \) is stable under action of \( \Gamma_K \), thus is a sub-representation of \( \Gamma_K \) in \( W_\infty \), and because \( W_\infty \) consists of finite vectors, the \( \Gamma_K \)-action is continuous w.r.t the discrete topology, and Hilbert’s theorem90(10.1.3.16) shows this subspace is generated by elements invariant under \( \Gamma_K \).

Prop. (14.2.6.5) [Sen’s Category]. Let \( \text{Sen}(K, K_{\infty}) \) be the category of f.d. \( K_{\infty} \)-vector spaces equipped with an endomorphism defined over \( K \), then the construction sending \( W \) to \( (W_\infty, \Phi_W) \) induces a functor \( S : \text{Rep}_{\mathbb{C}_p}(\Gamma_K) \to \text{Sen}(K, K_{\infty}) \). This functor commutes with direct sums, and also under tensor products, with the Sen’s operator given by

\[
\Phi_{W \otimes W'} = \Phi_W \otimes \text{id}_{W'} + \text{id}_W \otimes \Phi_{W'}.
\]

This functor is faithful, but in general not full. However, it reflects isomorphisms.

Proof: This functor is faithful because \( W_\infty \) generates \( W \) as a \( \mathbb{C}_p \)-vector space. To show it reflects isomorphism, Let \( f : W_\infty \to W'_\infty \) be an isomorphism commuting with Sen’s operator, then it extends by linearity to an isomorphism of \( \mathbb{C}_p \)-vector spaces \( W \to W' \), and \( f \) is \( \Gamma_s \)-equivariant for some \( s \) by the definition of Sen’s operator. Then considering the space of \( \Gamma_s \)-equivariant \( \mathbb{C}_p \)-linear morphisms from \( W \) to \( W' \), Hilbert’s theorem90 shows there is a basis \( f_i \) consisting of \( \Gamma_K \)-equivariant morphisms. Then it remains to show there exists a linear \( K \)-combination of \( f_i \) that is invertible. This is possible because it is true for \( \Gamma_s \), as \( f \) is invertible, and \( K \) is an infinite field.

Cor. (14.2.6.6). \( W \in \text{Rep}_{\mathbb{C}_p}(\text{Gal}_K) \) is trivial iff \( \Phi_W = 0 \).

Proof: As \( S \) reflects isomorphisms, compare with the trivial representation \( \mathbb{C}_d \).
Def. (14.2.6.7) [Hodge-Tate Representations]. Let $B_{H-T} = \mathbb{C}_{p}[t, t^{-1}], B'_{H-T} = \mathbb{C}_{p}(t)$, and let $G_{K}$ acts on it by $g(at^{i}) = g(a)\chi_{cycl}(g)^{it}$. In addition, there is a filtration on $B'_{H-T}$ given by $\text{Fil}^{m}B'_{H-T} = t^{m}\mathbb{C}_{p}[[t]]$, then the graded ring of $B'_{H-T}$ is isomorphic to $B_{H-T}$. (14.2.5.16) shows that $B'_{H-T}^{Gal_{K}} = B'_{H-T} = \mathbb{K}$.

$B_{H-T}$ and $B'_{H-T}$ are $\text{Gal}_{K}$-regular (14.2.4.2), and a $\mathbb{Q}_{p}$-linear representation of $G_{K}$ is $B_{H-T}$-admissible iff it is $B'_{H-T}$-admissible iff it is $V$ decomposes as
\[ \mathbb{C}_{p} \otimes \mathbb{Q}_{p} V \cong \mathbb{C}_{p}(\chi_{cycl}^{n_{1}}) \oplus \cdots \oplus \mathbb{C}_{p}(\chi_{cycl}^{n_{d}}) \]

And such a representation is called a **Hodge-Tate representation**.

**Proof:** $B'_{H-T}$ is $G_{K}$-regular because it is a field. For $B_{H-T}, B'_{H-T} \subset \text{Frac}(B_{H-T}) \subset B'_{H-T}$, taking $\text{Gal}_{K}$-fixed points shows (H2). For (H3), if $\mathbb{Q}_{p}x$ is stable under $\text{Gal}_{K}$ and $x$ is not of the form $at^{i}$, then we can get a non-trivial $G_{K}$-fixed point of $\mathbb{C}_{p}(\chi_{cycl}^{j})$, which is impossible by (14.2.5.16).

Notice $B_{H-T} \cong \bigoplus_{m \in \mathbb{Z}} \mathbb{C}_{p}(\chi_{cycl}^{m})$ as $\mathbb{C}_{p}$-semi-linear representations, then
\[ (V \otimes \mathbb{Q}_{p} B_{H-T})^{Gal_{K}} \cong \bigoplus_{m \in \mathbb{Z}} (V \otimes \mathbb{C}_{p}(\chi_{cycl}^{m}))^{Gal_{K}}. \]

Now if $V$ is Hodge-Tate, then clearly $(V \otimes \mathbb{Q}_{p} B_{HT})^{G_{K}}$ has dimension $\dim_{\mathbb{Q}_{p}}(V)$ thus $V$ is $B_{H-T}$-admissible. Conversely, $(V \otimes \mathbb{Q}_{p} B_{H-T})^{Gal_{K}}$ has dimension $\dim_{\mathbb{Q}_{p}}(V)$ implies there are $d \mathbb{C}_{p}(\chi_{cycl}^{m})$ contained in $V \otimes \mathbb{Q}_{p} \mathbb{C}_{p}$, and they are non-intersecting by (14.2.6.8), thus $V$ is Hodge-Tate.

**Prop. (14.2.6.8).** For any two integers $n, m$,
\[ \text{Hom}_{\text{Rep}_{\mathbb{C}_{p}}(\text{Gal}_{K})}(\mathbb{C}_{p}(\chi_{cycl}^{n}), \mathbb{C}_{p}(\chi_{cycl}^{m})) \]

is of one-dimensional if $n = m$, and vanishes otherwise.

This implies the decomposition for a Hodge-Tate representation (14.2.6.7) is uniquely determined up to a permutation.

**Proof:** Let $W = \text{Hom}_{\mathbb{C}_{p}}(\mathbb{C}_{p}(\chi_{cycl}^{n}), \mathbb{C}_{p}(\chi_{cycl}^{m})) = \mathbb{C}_{p}(\chi_{cycl}^{m-n})$, then the desired space is $W^{Gal_{K}}$, and the assertion follows from (14.2.5.16).

**Prop. (14.2.6.9) [Sen’s Operator and Hodge-Tate Representations].** A representation $V \in \text{Rep}_{\mathbb{Q}_{p}}^{f}(G_{K})$ is Hodge Tate iff the Sen’s operator $\Phi_{\mathbb{C}_{p} \otimes \mathbb{Q}_{p} V}$ is semisimple with eigenvalues in $\mathbb{Z}$. For a general $V$, the eigenvalue of $\Phi_{\mathbb{C}_{p} \otimes \mathbb{Q}_{p} V}$ is called the **generalized Hodge-Tate weights** of $V$.

**Proof:** If $V$ is a Hodge-Tate representation, then clearly $\Phi_{W}(v) = \lim_{t \to 0} \frac{\gamma'(t) - v}{t}$ acts by $k$ on $\mathbb{C}_{p}(\chi_{cycl}^{k})$, thus it is semisimple with eigenvalues in $\mathbb{Z}$. Conversely, on the $i$-eigenspace of $\Phi$, tensoring $\chi_{cycl}^{-i}$, $\Phi$ acts trivially, then because the kernel of $\Phi$ are the fixed points of $\Gamma_{K}(14.2.6.4)$, thus this eigenspace is isomorphic to $\mathbb{C}_{p}(\chi_{cycl}^{i})^{d}$, so $V$ is Hodge-Tate.

**Fontaine-Wintenberger Theory of Norm Fields**

Cf.[notes on p-adic Hodge, Conrad]intro.
7 Admissible Representations

**Lemma (14.2.7.1).** Let $V$ be a finite $\mathbb{Q}_p$-vector space with an action of $\text{Gal}_K$, then the action is continuous iff the induced action on $V \otimes_{\mathbb{Q}_p} B_{\text{dR}}^+$ is continuous.

**Proof:** This is because the action of $G_K$ on $B_{\text{dR}}^+$ is continuous, and $V$ has the induced topology in $V \otimes_{\mathbb{Q}_p} B_{\text{dR}}^+$. \hfill $\Box$

**Prop. (14.2.7.2).**
- $K = B^{\text{Gal}_K}$
- $K_0 = B_{\text{crys}}^{\text{Gal}_K}$, and the canonical morphism $K \otimes_{K_0} B_{\text{crys}} \to B_{\text{dR}}$ is injective.
- $Q_p = B_{e}^{\text{Gal}_K}$.

**Proof:**
1: Use the filtration $t^{-n}B_{\text{dR}}^+$ on $B_{\text{dR}}$, then the graded is just $C_p(\chi_{\text{cycl}})$, the $p$-adic closure twisted by $\chi_{\text{cycl}}$-action. Then by (14.2.5.16) $H^0(G_K, C_p(n)) = K$ iff $n = 0$ because $\chi_{\text{cycl}}^n$ has finite order iff $n = 0$. Hence induction this implies $K = B^{G_K}$.

2: The injectivity of $K \otimes_{K_0} B_{\text{crys}} \to B_{\text{dR}}$ Cf.[Laurent Fargues and Jean-Marc Fontaine Prop10.2.8].

3: From 2 and notice $B_e = B_{\text{crys}}^{e=\text{id}}$. \hfill $\Box$

**Def. (14.2.7.3) [Admissible Representations].** Let $K$ be a finite extension of $\mathbb{Q}_p$ with residue field $k$, $K_0 = W(k)[\frac{1}{p}]$ its maximal unramified extension. Let $B$ be a $\mathbb{Q}_p$-algebra that $G_K$ acts continuously that $F = B^{G_K}$ is a field. Given a finite $G_K$-module $V$, consider $D_B(V) = (V \otimes_{\mathbb{Q}_p} B)^{\text{Gal}_K}$, then $V$ is called $B$-admissible iff $\dim_F D_B(V) = \dim_{\mathbb{Q}_p} V$, equivalently,

$$D_B(V) \otimes_F B \to V \otimes_{\mathbb{Q}_p} B$$

is an isomorphism.

In particular, if $B = B_{\text{dR}}$ or $B_{\text{crys}}$, then the representation is called deRham representations or crystalline representations. The category of deRham or Crystalline representations of $G$ are denoted by $\text{Rep}_{\mathbb{Q}_p}^{\text{dR}}(G)$ or $\text{Rep}_{\mathbb{Q}_p}^{\text{crys}}(G)$

**Def. (14.2.7.4) [Rep$^l_{B_e}(\text{Gal}_K)$].** Denote by $\text{Rep}^l_{B_e}(\text{Gal}_K)$ the category of finite locally free $B_e$-modules $M$ with a semi-linear $\text{Gal}_K$-action that there exists a $\text{Gal}_K$-invariant $B_{\text{dR}}^+$-lattice $\Gamma \in M \otimes_{B_e} B_{\text{dR}}$ that $G_K$ acts continuously.

**Prop. (14.2.7.5) [Crystalline Representation].** The functor

$$\mathcal{D}: \text{Rep}_{B_e} G_K \to \varphi\text{-Mod}_{K_0}: W \mapsto (W \otimes_{B_e} B_{\text{crys}})^{\text{Gal}_K}$$

are left adjoint to the functor

$$\mathcal{V}: \varphi - \text{Mod}_{K_0} \to \text{Rep}_{B_e} G_K: (D, \varphi_D) \mapsto (D \otimes_{K_0} B_{\text{crys}})^{\varphi_D \otimes \varphi = \text{id}}$$

Moreover, $\mathcal{V}$ is fully faithful, $\text{id} \cong \mathcal{D} \circ \mathcal{V}, \mathcal{V} \circ \mathcal{D} \cong \text{id}$, and $M \in \text{Rep}_{B_e}(\text{Gal}_K)$ is in the image of $\mathcal{V}$ iff $\mathcal{V}(\mathcal{D}(M)) \cong M$.

**Proof:** Cf.[Laurent Fargues and Jean-Marc Fontaine Prop10.2.12]. \hfill $\Box$

**Cor. (14.2.7.6).** In particular, a $B_e$-representation is crystalline iff it is in the image of $\mathcal{V}$. Now we define a Vector bundle $\mathcal{E}$ on $X$ to be crystalline iff the $H^0(X \setminus \{\infty\}, \mathcal{E})$ is crystalline.
Lemma (14.2.7.7). Let $W$ be a f.d. $K$-vector space, then the map:

$$\{\text{Filtrations on } W\} \rightarrow \{G_K\text{-stable } B_{dR}^+\text{-lattice in } W \otimes_K B_{dR}\} : \text{Fil} \mapsto \text{Fil}^0(W \otimes_K B_{dR})$$

is bijective and the inverse is given by $\Gamma \mapsto \{(t^n \Gamma)^{\text{Gal}_K} \subset (B_{dR} \otimes_{\mathcal{O}_{\mathcal{K}}} \mathcal{O}_{\mathcal{K}}^+) \text{Gal}_K = W\}_{n \in \mathbb{Z}}$.

Proof: Cf.[Laurent Fargues and Jean-Marc Fontaine Prop10.4.3]. □

Comparison Theorems

Prop. (14.2.7.8) [C_{dR}-Theorem]. Let $X$ be a proper smooth variety over $K$, then for any $r$, there exists a canonical isomorphism

$$\gamma_{dR}(X) : B_{dR} \otimes_K H^r_{dR}(X) \cong B_{dR} \otimes_{\mathbb{Q}_p} H^r_{\text{et}}(X_{\overline{K}}, \mathbb{Q}_p).$$

which respect filtrations and $G_K$-actions on both sides. Moreover $\gamma_{dR}$ is functorial in $X$.

Proof: □

Cor. (14.2.7.9). The $\mathbb{Q}_p$-representation $H^r_{\text{et}}(X_{\overline{K}}, \mathbb{Q}_p)$ is de Rham, and

$$H^r_{dR}(X) \cong (B_{dR} \otimes_{\mathbb{Q}_p} H^r_{\text{et}}(X_{\overline{K}}, \mathbb{Q}_p))^\text{Gal}_K.$$

Also by taking the gradation there is a Hodge-like decomposition

$$C_p \otimes_{\mathbb{Q}_p} H^r_{\text{et}}(X_{\overline{K}}, \mathbb{Q}_p) \cong \bigoplus_{a+b=r} C_p(\chi_{\text{cycl}}^{-a}) \otimes_K H^b(X, \mathcal{O}_X).$$

Conj. (14.2.7.10) [Fontaine-Mazur]. $C_{dR}$-theorem (14.2.7.8) implies any representation of $G_K$ of the form $H^r_{\text{et}}(X_{\overline{K}}, \mathbb{Q}_p)$ is de Rham, thus it is natural to consider the converse.

Let $F$ be a number field and $V$ a f.d. $\mathbb{Q}_p$-representation of $G_F$ that satisfies:

- For almost all prime ideal $p$ of $\mathcal{O}_F$, the representation is unramified at $p$.
- For all primes above $p$, the representation $V|_{\text{Gal}_p}$ is de Rham.

Then $V$ appears as a subquotient of some $H^r_{\text{et}}(X_{\overline{K}}, \mathbb{Q}_p)(\chi_{\text{cycl}}^m)$ where $X \in \text{Var}_{\text{sm,proper}} / \text{Spec } F$.

Proof: □

Emerton and Kisin proved the two-dimensional case, Cf.[The Fontaine-Mazur conjecture for GL2, Kisin]. □

Prop. (14.2.7.11). $B_{H-T}$ is identified with the graded ring of $B_{dR}$, so any deRham representation of $G$ is Hodge Tate. □

8 Crystalline Representations

References are [Crystalline Representations and $F$-crystals, Kisin].
14.3 p-adic Modular Forms

Main references are [p-adic Modular Forms]
14.4 $\mathbb{F}_p$-Schemes

1 Perfect Schemes

**Def. (14.4.1.1) [Perfect Schemes].** An $\mathbb{F}_p$-scheme is called **perfect** if the Frobenius is an isomorphism on it. Equivalently, this means every affine subscheme is the spectrum of a perfect scheme.

Let Perf be the category of perfect qcqs $\mathbb{F}_p$-schemes endowed with the V-topology (5.1.4.43).

**Def. (14.4.1.2) [Perfection].** There is a **perfection** functor $X \mapsto X_{\text{perf}}$ from the category of schemes to the category of perfect schemes, it is defined as the glueing of the perfection $R \rightarrow R_{\text{perf}}$ as it commutes with colimits.

**Prop. (14.4.1.3) [Perfection and Properties].** Let $f : X \rightarrow Y$ be a morphism of $\mathbb{F}_p$-schemes, then the following properties holds true for $f$ iff it holds true for $f_{\text{perf}}$:
1. Qco.
2. Quasiseparated.
3. Affine.
4. Separated.
5. Integral.
6. Universally closed.
7. Universal homeomorphism.

The following properties holds for $f_{\text{perf}}$ if it holds for $f$:
1. Closed immersion.
2. Open immersion.
3. immersion
4. Étale
5. (Faithfully) Flat.

**Proof:** Cf. [Projectivity of Witt Vectors Affine Grassmannian, 3.4]. □

**Prop. (14.4.1.4).** If $X$ is an $\mathbb{F}_p$-scheme and $\mathcal{L}$ is a line bundle on $X$, then $\mathcal{L}$ is ample iff the pullback to $X_{\text{perf}}$ is ample.

**Proof:** Cf. [Projectivity of Witt Vectors Affine Grassmannian, 3.6]. □

**Prop. (14.4.1.5).** If $X$ is an $\mathbb{F}_p$-scheme, then $X_{\text{ét}} \rightarrow X_{\text{perf}, \text{ét}} : Y \rightarrow Y_{\text{perf}}$ is an equivalence of sites.

**Proof:** □

**Prop. (14.4.1.6) [Perfectly Finitely Presented Morphisms].** Let $f : X \rightarrow Y$ be a morphism in Perf(14.4.1.1), then $f$ is called a **perfectly finitely presented morphism** if it satisfies the following equivalent conditions:
- Any open affine subscheme $\text{Spec } B \subset X$ mapping to an open affine subscheme $\text{Spec } A \subset Y$, $A \rightarrow B$ is perfectly f.p. (4.5.1.6).
- There is an open affine covering $\text{Spec } A_i \rightarrow X$ mapping to an open affine covering $\text{Spec } B_i \rightarrow Y$ that $B_i \rightarrow A_i$ are all perfectly f.p.
• For any cofiltered system \( \{Z_i\} \in \text{Perf}_Y \) with affine transition maps, there is a bijection 
\[ \text{colim} \ \text{Hom}_Y(Z_i, X) \cong \text{Hom}_Y(\lim Z_i, X). \]
In particular, perfectly finitely presented is local on the base and target.

**Proof:** Cf.[Projectivity of Witt Vectors Affine Grassmannian, 3.11].

**Prop. (14.4.1.7) [Perfect Base Change].** If 
\[
\begin{array}{ccc}
X' & \xrightarrow{g'} & X \\
\downarrow f' & & \downarrow f \\
Y' & \xrightarrow{g} & Y \\
\end{array}
\]
is a pullback diagram of perfect \( \mathbb{F}_p \)-schemes, then for any complex \( K^\bullet \) of \( \mathbb{Q}\text{-co} \) sheaves on \( X \), the base change map (5.3.3.18) 
\[
Lg^*Rf_*K \rightarrow Rf'_*Lg^!K
\]
is an isomorphism.

**Proof:** It is clearly we need only check for the affine case, then let \( X = \text{Spec} \ B, Y = \text{Spec} \ A, Y' = \text{Spec} \ A' \), and \( X' = \text{Spec} \ B \otimes_A A' \), then it suffices to prove that 
\[
K \otimes^L_A A' \cong K \otimes^L_B B'.
\]
This follows from the fact \( B \otimes_A A' = B \otimes^L_A A' \), by (4.5.1.8).

**Prop. (14.4.1.8) [Cartier Isomorphism].** If 

**Proof:**

**Cor. (14.4.1.9) [Affine Line case].** Let \( R \) be an \( \mathbb{F}_p \)-algebra and
14.5 Formal and Rigid Geometry

Main references are [Bos15] and [BGR84], but there are other approaches, such as given by Berkovich, or given by Huber, and used in Scholze’s work, which is most natural because it behaves well w.r.t. the formal model.

1 Affinoid $K$-Spaces

Def. (14.5.1.1) [Affinoid $K$-Space], an affinoid algebra $A$ can be viewed as the function ring on the space $\text{Sp} A$ of maximal ideals of $A$ with the usual Zariski topology called the **affinoid $K$-space associated to** $A$. A morphism of affinoid algebras induce a map on their $\text{Sp} A$. This is because residue fields of maximal ideals are finite over $K$. So we define the category of affinoid $K$-spaces as the opposite category of affinoid $K$-algebras.

Cor. (14.5.1.2). The category of affinoid spaces admits fiber products, because of (10.3.4.30).

Prop. (14.5.1.3). By the properties of a Jacobson space (3.8.3.24)(3.8.3.21), the affinoid $K$-space has good properties w.r.t. closed, open hence irreducible compared to $\text{Spec} A$ in Zariski topology. In particular, it is a Noetherian space.

Def. (14.5.1.4) [Canonical Topology]. The affinoid $K$-space has another topology, called the **canonical topology**, generated by $X(f, \varepsilon) = \{ x | f(x) \leq \varepsilon \}$ as a subbasis. And this topology is in fact generated by $X(f) = X(f, 1)$ as a subbasis.

Proof: For the last assertion, notice $f(x)$ assume value in $|K|$, which is dense in $\mathbb{R}_+$, so we can assume $\varepsilon \in |K|$ (by approximation from below), hence $\varepsilon^n = |c|$, where $c \in K$, so $X(f, \varepsilon) = X(f^n, c) = X(c^{-1} f^n)$.

Prop. (14.5.1.5). $\{ x | f(x) = \varepsilon \}$ is open in $\text{Sp} A$.

Proof: We let $f(x) = \varepsilon$ and $k = A/\mathfrak{m}_x$, let the minipoly of $f$ in $A/\mathfrak{m}_x$ be $P$ of degree $n$, and let $g = P(f)$, then $g(x) = 0$, and if $|g(y)| < \varepsilon^n$, then $|f(y)| = \varepsilon$, otherwise $|f(y) - \alpha_i| \geq |\alpha_i| = \varepsilon$ for every root $\alpha_i$ of $P$, hence $|P(f(y))| \geq \varepsilon^n$, contradiction.

Cor. (14.5.1.6). By the proof, we have, $X(f_1, \ldots, f_r)$, $f_i \in \mathfrak{m}_x$ forms a basis of $x$ in $\text{Sp} A$. (Replace every $X(f_i) \text{ by } \{ y | f_i(y) = \varepsilon \}$, then by some $X(g_i)$ for $g_i \in \mathfrak{m}_x$.

Def. (14.5.1.7) [Affinoid Subdomain]. For an affinoid $K$-space $X$, a subset $U$ is called a **affinoid subdomain of** $X$ if there is an closest affinoid space map $X' \to X$ with image in $U$, i.e. any other these maps factor through it. The definition is weird but the situation is clarified by the following proposition.

Prop. (14.5.1.8). For an affinoid subdomain $i: X' \to X$,

- $i$ is injective and $\text{Im} i = U$.
- $i^*$ induce an isomorphism $A/\mathfrak{m}_{i(x)}^k \cong A'/\mathfrak{m}_{i(x)}^k$.
- $\mathfrak{m}_x = \mathfrak{m}_{i(x)} A'$.
Proof: Consider a point \( y \in U \), there is a commutative diagram

\[
\begin{array}{ccc}
A & \xrightarrow{i^*} & A' \\
\downarrow & & \downarrow \\
A/m^n_y & \xrightarrow{\sigma} & A'/m^n_y A'
\end{array}
\]

there is a map \( \alpha : A' \to A/m^n_y \) that makes the upper diagram commutative by universal property of subdomain, and the lower triangle is commutative by universal properties again. Then we see \( \sigma \) is surjective and notice the kernel of the projection is \( m_y A' \) is in the kernel of \( \alpha \), thus \( \sigma \) is injective.

Now the case \( n = 1 \) shows \( m_y A' \) is maximal, hence \( i \) is surjective and the inverse image is just one point. \( \square \)

Prop.(14.5.1.9)[Special Subdomains]. There are three special affinoid subdomain of \( X \): Weierstrass domain \( X(f_1, \ldots, f_r) \), Laurent domain \( X(f_1, \ldots, f_r, g_1^{-1}, \ldots, g_s^{-1}) \), rational domain \( X(\frac{L_0}{f_0}, \ldots, \frac{L_r}{f_0}) = \{ x | |f_i(x)| \leq |f_0(x)| \} \) for \( (f_0, \ldots, f_r) = (1) \). They are all open by (14.5.1.5).

Proof: The Weierstrass domain corresponds to \( A \to A\langle X_1, \ldots, X_r \rangle/(X_i - f_i) \).

The Laurent domain corresponds to \( A \to A\langle X_1, \ldots, X_{r+s} \rangle/(X_i - f_i, 1 - X_{r+j}g_j) \).

The rational domain corresponds to \( A \to A\langle X_1, \ldots, X_r \rangle/(f_i - f_0 X_i) \).

They are affinoid subdomains in fact, easily checked. \( \square \)

Lemma(14.5.1.10). Weierstrass domain are Laurent, and Laurent domain are rational, this is because intersection of rational domains are rational.

Any rational domain is a Weierstrass domain of a Laurent domain.

Proof: Notice a Laurent subdomain is a finite intersections of \( X(\frac{L}{1}) \) and \( X(\frac{L}{g}) \), so it is rational.

For a rational domain \( U \), \( f_0 \) is a unit in \( O(U) \), hence its inverse has a bounded value, then \( |c f_0| > 1 \) for some \( c \in K^* \). Hence \( U \) is Weierstrass in \( X((c f_0)^{-1}) \). \( \square \)

Cor.(14.5.1.11)[Pullback & Composition of Affinoid Subdomain]. The pullback(hence intersections) of affinoid subdomains is affinoid subdomain and it is just the set-theoretic inverse image, and specialness is preserved.

The affinoid subdomain of an affinoid subdomain is affinoid subdomain, and Weierstrassness and rationalness is preserved(while Laurentness not).

Proof: Pullback: fiber product exist in the category of affinoid \( K \)-spaces, then the universal property is checked. The set-theoretic property follows from (14.5.1.8).

Speciality: Clear.

Transitivity: Clear by universal property.

For the speciality, if \( V = X(f_i), U = V(g_j) \) is Weierstrass, then because by (10.3.4.26) \( A \) is dense in \( A\langle f_i \rangle \), we can replace \( g_j \) by elements from \( A \), by adding elements of small sup-norm, because valuation is non-Archimedean. Then \( U = X(f_i, g_j) \). For the rational subdomain \( V = X(\frac{L_0}{f_0}, \ldots, \frac{L_r}{f_0}) \), use (14.5.1.10), it suffices to prove for \( U = V(g) \) or \( U = V(g^{-1}) \). For this, notice the image of \( A[f_0^{-1}] \) is dense in \( A\langle \frac{L_0}{f_0}, \ldots, \frac{L_r}{f_0} \rangle \), by (10.3.4.26), so as before, we change \( g \) that it \( g_0 f_0^n g \in A \) for some \( n \). Now

\[
V(g) = V \cap \{ x \in X ||g_0(x)|| \leq |f_0^n(x)| \}, \quad V(g^{-1}) = V \cap \{ x \in X ||g_0(x)|| \geq |f_0^n(x)| \}.
\]

But now \( f_0^n \) is a unit in \( A\langle \frac{L_0}{f_0}, \ldots, \frac{L_r}{f_0} \rangle \), so \( |f(x)|_{sup} \geq |c| \) for some \( c \in K^* \), so

\[
V(g) = V \cap X(\frac{g_0}{f_0}, \frac{c}{f_0}), \quad V(g^{-1}) = V \cap X(\frac{f_0}{g_0}, \frac{c}{g_0}).
\]

is rational in \( X \). \( \square \)
Cor. (14.5.1.12). For a special subdomain $U$ of $X$, the canonical topology induces the canonical topology of $U$, by the transitivity property of affinoid subdomains and (14.5.1.10). In fact, by (14.5.1.14), any affinoid subdomain is open and the topology coincides.

Prop. (14.5.1.13). Let $\varphi : Y = \text{Sp} B \to X = \text{Sp} A$ be a morphism, if $x$ is a point of $X$ that $A/\mathfrak{m}_x \to B/\mathfrak{m}_x B$ is a surjection, then there is an affinoid nbhd $U$ of $x$ that $\varphi$ restricts to a closed immersion on $\varphi^{-1}(U)$. If $A/\mathfrak{m}_x^n \cong B/\mathfrak{m}_x^n$ for all $n$, then there is an affinoid nbhd $U$ of $x$ that $\varphi$ restricts to an isomorphism $\varphi^{-1}(U) \cong U$.

Proof: Cf. [Rigid And Formal Geometry P79].

Cor. (14.5.1.14). Every affinoid subdomain of $X$ is open and has the restriction topology of $X$ (canonical topology), because it satisfies the second condition of (14.5.1.13), by (14.5.1.8).

Lemma (14.5.1.15). If $f \subset A(X_1, \ldots, X_n)$ is $X_n$-distinguished of order $\leq s$ for each element of $\text{Sp} A$, then the set of elements that $f$ is $X_n$-distinguished of exact order $s$ is a rational subdomain of $A$.

Proof: Let $f = \sum f_i X_i^s$, let the constant coefficient of $f_i$ be $a_i$, then the set is in fact $U = \{ x \in \text{Sp} A | |a_i(x)| \leq |a_i(x)| \}$. This is because, if $f$ is distinguished of order $s_x$ at $x$, then $a_{s_x} \neq 0$ because $f_{s_x}$ is a unit, and $|a_{s_x}| \leq |f_{s_x}| = |a_{s_x}|^2$ for $v \leq s_x$ and strict inequality holds for $v > s_x$. In particular, $a_0, \ldots, a_s$ cannot have a common zero, so it is truly a rational subdomain.

Prop. (14.5.1.16). If $f \subset A(X_1, \ldots, X_n)$ is $X_n$-distinguished of order $s$ for each element of $\text{Sp} A$, then the map
\[ A(X_1, \ldots, X_{n-1}) \to A(X_1, \ldots, X_n)/(f) \]
is finite.

Proof: Cf. [Rigid And Formal Geometry P79].

Presheaf of Affinoid Functions

Def. (14.5.1.17). The weak Grothendieck category (affine topology) on an affinoid space $X$ has coverings defined by the finite cover by affinoid subdomains, called **affinoid covering**.

The strong Grothendieck category (fpqc topology) on an affinoid space $X$ is defined by: objects are unions of affinoid subdomains $U = \bigcup U_i$ that for any morphism from an affinoid space $\varphi : Z \to U \subset X$, the pullback covering $\bigcup \varphi^{-1}(U_i)$ has a finite subcover by affinoid subdomains. A covering is defined by the same finiteness property.

The strong Grothendieck topology satisfies completeness conditions $G_0, G_1, G_2$ defined in (5.1.1.10), as easily verified.

The weak Grothendieck topology is a temporary notion, it will be obsolete after Tate’s acyclicity theorem is proved. Admissible opens and admissible covers are notions w.r.t. the strong Grothendieck topology.

Proof: The weak Grothendieck category is a Grothendieck category by (14.5.1.11). The strong Grothendieck category is a Grothendieck category because: the finiteness condition lifts along base change, and also for base change, because we can first choose a finite subcover, then choose a finite subcover of the base change covering of that finite covering.

Def. (14.5.1.18). For $n$ functions $f_1, \ldots, f_n$ without common zeros, the rational subdomains $U_i = X(\sum_{j=1}^n f_i f_j)$ is an affinoid covering, called the **rational covering**. For $n$ functions $f_1, \ldots, f_n$, there is a **Laurent covering** $X(\prod_{i=1}^n f_i), \varepsilon_i = \pm 1$. 
Prop. (14.5.1.19). Morphisms of affinoid spaces are continuous in weak Grothendieck topology by (14.5.1.11). It is also continuous in the strong Grothendieck topology, as one can check the finiteness conditions.

Prop. (14.5.1.20). Let $X$ be an affinoid $K$-space, for any $f \in \mathcal{O}_X(X)$, consider the following sets:

$$U_1 = \{x | |f(x)| < 1\}, \quad U_2 = \{x | |f(x)| > 1\}, \quad U_3 = \{x | |f(x)| > 0\}.$$

Then any finite union of sets of the form is admissible, and any finite cover by finite union of sets of the form is an admissible covering.

Proof: We first show that $U_1$ is admissible open, the others are similar. Let $\varepsilon_n$ be an ascending sequence of elements in $\sqrt{|K^*|}$ converging to 1, then $U_1 = \bigcup_n X(\varepsilon_n^{-1}f)$ is a union of open subsets because $\varepsilon_n \in \sqrt{|K^*|}$. Now for any affinoid space $Z$ mapping into $U_1$, $|\varphi^*(f)(z)|_{\sup} < 1$ for all $z \in Z$, thus by maximal principle (10.3.4.21), $|f|_{\sup} < 1$, thus the cover $U_1 = \bigcup_n X(\varepsilon_n^{-1}f)$ can be refined by a finite cover, thus it is admissible open.

For the admissibility of covering, the proof is similar, but use the following lemma (14.5.1.21).

Lemma (14.5.1.21). For any affinoid $K$-algebra $A$, if $f_i, g_j, h_k$ are system of functions on $A$ that: for every $x \in A$, either $|f_i(x)| < 1$, $|g_j| > 1$ or $h_k(x) > 0$, then we can replace $>,< by \geq, \leq$ and elements in $\sqrt{|K^*|}$ that the same condition is true.

Proof: Cf. [Rigid and Formal Geometry P97].

Cor. (14.5.1.22). The strong Grothendieck category is finer than the Zariski category, because any standard affine open set is of the form $U_3$ and also Zariski covering is open covering because $\text{Sp}(A)$ is Noetherian (10.3.4.16).

Def. (14.5.1.23) [Presheaf of Affinoid Functions]. There is a presheaf of affinoid functions defined on the weak Grothendieck topology because of the universal property of the affinoid subdomains.

Then the stalk $\mathcal{O}_{X,x}$ are local ring with maximal ideal $m_x \mathcal{O}_{X,x}$. Hence let $X = \text{Sp} A$, the stalk map factor thorough $A \to A_m \leftrightarrow \mathcal{O}_{X,x}$, and

$$A/m^n_x \cong A_{m_x}/m^n_x A_{m_x} \cong \mathcal{O}_{X,x}/m^n_x \mathcal{O}_{X,x}$$

so it induces isomorphisms between their $m_x$-adic completions.

Proof: By (14.5.1.8), there is an isomorphism $K' = \mathcal{O}_X(X)/m_x \cong \mathcal{O}_X(U)/m_x \mathcal{O}(U)$. Take the converse and pass to direct colimit (it is exact), $\mathcal{O}_{X,x}/m_x \mathcal{O}_{X,x} \cong K'$. This map will be regarded as evaluation at $x$. The kernel $m_x \mathcal{O}_{X,x}$ is a maximal ideal. There are no other maximal ideals in $\mathcal{O}_{X,x}$ because if $f$ in not in the kernel, then $f(x) \neq 0$, and multiply by an element in $K^*$, it can be made $|f(x)| \geq 1$, and then $U(f^{-1})$ is an affinoid subdomain containing $x$ that $f$ is invertible in it.

For the second assertion, for an affinoid subdomain $\text{Sp} A'$, there are maps

$$A/m^n \to A'/m^n \to \mathcal{O}_{X,x}/m^n \mathcal{O}_{X,x}.$$
Cor. (14.5.1.24). \( f \in A = \mathcal{O}_X(X) \) vanish iff it vanish at every stalk, this is because \( A \to \prod \mathfrak{m}_A \to \prod \mathcal{O}_{X,x} \) is injective.

Cor. (14.5.1.25). Giving a covering of affinoid subdomain of an affinoid space \( X_i \to X \), then \( \mathcal{O}_X(X) \to \prod \mathcal{O}_{X_i}(X_i) \) is an injection. (This is because the kernel vanishes at each stalk.)

Cor. (14.5.1.26). For a subdomain of an affinoid space \( X \), the corresponding ring map is flat.

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]

\[ \text{} \]}
Prop. (14.5.1.33) [Equivalent Definition of Runge Immersions]. For a morphism \( \sigma : A \to A' \), \( \text{Sp } A' \to \text{Sp } A \) is a Runge immersion if \( \sigma(A) \) is dense in \( A' \) iff \( \sigma(A) \) contains a set of affinoid generator of \( A' \) over \( A \).

Proof: For a Runge immersion, \( \sigma(A) \) is dense in \( A' \), because this is true for Weierstrass subdomain and closed immersion.

If \( \sigma(A) \) is dense in \( A' \), then by (10.3.4.28), we can modify a set of affinoid generators by a set of affinoid generators in \( \sigma(A) \).

If \( h_i \) is a set of affinoid generators in \( \sigma(A) \), then \( A \to A\langle h_i \rangle \to A' \) is a Runge immersion. \( \square \)

Cor. (14.5.1.34). Runge immersion is stable under composition.

Prop. (14.5.1.35). An open and Runge immersion is an immersion of Weierstrass subdomain.

Proof: By localizing on this Weierstrass subdomain, and notice Weierstrass subdomain is stable under composition (14.5.1.11), we reduce to clopen immersion case, and result follows by (14.5.1.31). \( \square \)

Lemma (14.5.1.36) [Extension of Runge Immersion]. For a morphism of affinoid spaces \( X' \to X = \text{Sp } A \), if \( f_1, \ldots, f_n, g \) generate \( A \), for \( \varepsilon \in \sqrt{K^*} \), denote \( X_\varepsilon = \{ x \mid |f_i(x)| \leq \varepsilon |g| \} \), this is a rational subdomain. The inverse image of \( X_\varepsilon \) is \( X'_\varepsilon \), then if \( X'_\varepsilon \to X_\varepsilon \) is a Runge immersion for some \( \varepsilon_0 \), then there is a \( \varepsilon > \varepsilon_0 \) that \( X'_\varepsilon \to X_\varepsilon \) is also a Runge immersion.

Proof: Cf. [Rigid and Formal Geometry P73]. \( \square \)

Prop. (14.5.1.37) [Gerritzen-Grauert]. For a locally closed immersion \( \varphi : X' \to X \), there is a finite cover of \( X \) of rational subdomains \( X_i \) that \( \varphi^{-1}(X_i) \to X_i \) are Runge immersions.

Proof: Cf. [Formal and Rigid Geometry P79]. \( \square \)

Cor. (14.5.1.38) [Gerritzen-Grauert]. Any affinoid subdomain is equivalent to a finite union of rational subdomains.

Proof: An affinoid subdomain is an open immersion by (14.5.1.28), so \( \varphi^{-1}(X_i) \to X_i \) is open and Runge, so it is Weierstrass by (14.5.1.35). In particular, \( X \cap X_i \) is rational in \( X \) by transitivity, thus the result. \( \square \)

Tate’s Acyclicity

Lemma (14.5.1.39) [Reduction of Weak Grothendieck Topology].

- Every affinoid covering has a refinement of rational covering.

- For every rational covering, there is a Laurent covering \( \{V_i\} \) that restriction on each \( V_i \) is rational covering generated by units.

- Every rational covering generated by units has a refinement of Laurent covering.

Proof: 1: By (14.5.1.38), we can assume the covering consists of rational subdomains \( U_i = X(f_{i1}, \ldots, f_{in}) \), then consider the elements \( f_{v_1 \cdots v_n} = \prod_{i=1}^{n} f_{iv_i} \), where at least some \( v_i = 0 \). Denote the set of these elements by \( I \).

Firstly, these elements has no common zero on \( X \), thus generating a rational covering of \( X \): for any \( x \in U_i \), \( f_{00} \) doesn’t vanish at \( x \), thus the product \( \prod_{j \neq i} f_{jv_j} \) vanishes for all choices of \( v_j \), but this is impossible because for each \( j \), \( \{f_{ik}\}_k = (1) \).
Secondly, this is a refinement of $U_j$: We show $X_{f_{v_1\ldots v_n}} \subset U_k$ where $v_k = 0$. For this, consider $x \in X_{f_{v_1\ldots v_n}}$, then $x \in U_j$ for some $j$. If $j = k$, we are done, otherwise,

$$|f_{v_1\ldots v_n}(x)| \leq |f_{v_1\ldots v_n}(x)| \leq |f_{v_1\ldots v_n}(x)|.$$  

Where the last inequality is because $(v_1, \ldots, v_n)$ has a 0, thus $f_{v_1\ldots v_n} \in I$.

2: For a rational covering, $f_i$ is invertible in the ring of $U = X(\frac{f_0}{f_1}, \ldots, \frac{f_n}{f_1})$, thus it has a inverse that attains maximum value on $U(10.3.4.21)$. Hence there is a $c \in k^*$ that $|c|^{-1} < \inf\max\{|f_i(x)|\}$.

I claim the Laurent covering w.r.t. the elements $c(f_0), \ldots, c(f_n)$ satisfies the requirement. Because for example, on $V = X((c_0) \cdots (c_n)(c_{s+1})^{-1} \cdots (c_n)^{-1})$, $|f_i(x)| < |f_j(x)|$ for $i \leq s < j$, so the covering restricted to $V$ is just the rational covering generated by $f_{s+1}, \ldots, f_n$, and they are all invertible in $\mathcal{O}(V)$.

3: In fact the Laurent covering generated by the element $f_i f_j^{-1}$ for $i < j$ is a refinement of the rational covering generated by $f_1, \ldots, f_n$, because in any one of this Laurent subdomains $V$, for any two $i, j$, either $|f_i(x)| < |f_j(x)|$ or $|f_j(x)| < |f_i(x)|$ for all $x \in V$, so there is a maximal one $f_s$, then $V \subset X(\frac{f_0}{f_s}, \ldots, \frac{f_n}{f_s})$.

\[\Box\]

**Prop. (14.5.1.40)** [Tate’s Acyclicity Theorem]. The presheaf of affinoid functions on an affinoid space $X = \text{Sp} A$ is a sheaf w.r.t. the weak Grothendieck category. In fact, for any $A$-module $M$, the presheaf $\tilde{M} = M \otimes_A \mathcal{O}_X$ is a sheaf w.r.t. the weak Grothendieck topology, called the quasi-coherent sheaf on $X$.

Moreover, for any finite cover of affinoid subdomains, the Čech cohomology group $\check{H}^q(\text{Sp} A, \tilde{M})$ vanish for $q \neq 0$.

**Proof:** It suffices to prove the last assertion. First reduce to the case of Laurent covering by(14.5.1.39) and(5.3.2.10)(5.3.2.11). Notice the base change invariance of the specialities of affinoid subdomains(14.5.1.11). Even more, by(5.3.2.12) and an induction process, it suffices to prove for the simple Laurent covering $X(f), X(f^{-1})$.

It suffices to prove for the sheaf of affinoid functions $\mathcal{O}_X$, because for any Qco sheaf $\tilde{M}$, choose a free resolution of $M$, then use dimension shifting, notice the covering is finite(the flatness of the algebra map(14.5.1.26) is used to deduce the long exact sequence).

For the sheaf $\mathcal{O}_X$, the main tool is the following commutative diagram:

\[
\begin{array}{ccc}
0 & 0 \\
\downarrow & \downarrow \\
(X-f)A(X) \times (1-fY)A(Y) & \delta''(X-f)A(X,X^{-1}) \rightarrow 0 \\
\downarrow & \downarrow \\
0 & A \xrightarrow{\varepsilon'} A(X) \times A(Y) \xrightarrow{\delta'} A(X,X^{-1}) \rightarrow 0 \\
\downarrow & \downarrow \\
0 & A \xrightarrow{\varepsilon} A(f) \times A(f^{-1}) \xrightarrow{\delta} A(f,f^{-1}) \rightarrow 0
\end{array}
\]

where $\delta'$ is given by $(h_1(X), h_2(Y)) \mapsto h_1(X) - h_2(X^{-1})$, and $\delta''$ is induced by $\delta'$. The columns are all exact, and the first row and the second row are exact. $\varepsilon$ is injective by(14.5.1.25). Then the last row is also exact, by spectral sequence. \[\Box\]
Prop. (14.5.1.41) [Strong/Weak Topos The same]. If \( X \) is an affinoid \( K \)-space, the category of sheaves w.r.t. the strong Grothendieck topology is equivalent to the category of sheaves w.r.t. the weak Grothendieck topology by pushforward and pullback of sheaves by (5.1.2.24) because the strong and weak Grothendieck category satisfies the conditions.

In particular, this applies to the case \( O_X \) by (14.5.1.40), the resulting sheaf is called the sheaf of rigid analytic functions on \( X \), also denoted by \( O_X \).

2 Rigid Analytic Spaces

Def. (14.5.2.1). A \( G \)-ringed \( K \)-space is a pair \((X, O_X)\) where \( X \) is a \( G \)-topological space and \( O_X \) is a sheaf of \( K \)-algebras. It is called local \( G \)-ringed \( K \)-space if the stalks are all local rings. Their morphisms are defined routinely.

Prop. (14.5.2.2) [Morphisms Between Affinoid Spaces]. An affinoid \( K \)-space with the sheaf of analytic functions \((X, O_X)\) (14.5.1.41) is an example of local \( G \)-ringed \( K \)-space (14.5.1.23).

A continuous homomorphism of rings induces a local \( G \)-ringed morphism. And all morphisms come from these.

Moreover, an affinoid \( K \)-space is a complete \( G \)-ringed \( K \)-space (i.e. rigid) (5.1.1.10).

Proof: It is a \( G \)-space by (14.5.1.40), (14.5.1.41), morphisms by (14.5.1.19), notice the \( m_x \) generate the maximal ideal of \( O_{X,x} \) (14.5.1.23), so the morphism is local.

To show all morphisms are like these, we need to show a morphism \( \sigma : A \to B \) gives at most one \( \text{Sp} B \to \text{Sp} A \): the morphism is local, so it maps \( m_{\varphi(x)} \) to \( m_x \), and from the commutative diagram

\[
\begin{array}{ccc}
A / m_{\varphi(x)} & \longrightarrow & B / m_x \\
\downarrow \cong & & \downarrow \cong \\
O_{\varphi(x), \text{Sp} A} / m_{\varphi(x)} O_{\varphi(x), \text{Sp} A} & \longrightarrow & O_{x, \text{Sp} B} / m_x O_{x, \text{Sp} B}
\end{array}
\]

(14.5.1.23) shows \( m_{\varphi(x)} \) is mapped into \( m_x \), so \( m_{\varphi(x)} = (\sigma^*)^{-1} m_x \), which shows \( \varphi \) is unique set-theoretically, and on the level of structure sheaf, the uniqueness of \( O_{\text{Sp} A}(V) \to O_{\text{Sp} B}(\varphi^{-1}(V)) \) is unique by the definition of affinoid subdomain (14.5.1.7).

Def. (14.5.2.3) [Rigid Spaces]. The category of rigid (analytic) space is a full subcategory of local \( G \)-ringed \( K \)-spaces that it is complete \( G_0, G_1, G_2 \), and it has an admissible covering \( \{X_i \to X\} \) that \((X_i, O_X|_{X_i})\) are affinoid \( K \)-spaces.

It follows easily that an admissible open subset of a rigid space is again rigid.

Prop. (14.5.2.4) [Glueing Rigid Spaces]. Glueing rigid analytic spaces is legitimate, so does glueing morphisms on the source.

Proof: First glue the set, then use (5.1.1.12) to glue \( G \)-topology, finally the glue of structure sheaf is similar to (5.1.5.3).

Cor. (14.5.2.5) [Spectrum Adjointness]. If \( X \) is rigid and \( Y \) is affinoid, then \( \text{Hom}(X, Y) \cong \text{Hom}(O_Y(Y), O_X(X)) \). This follows from (14.5.2.2) and glue (14.5.2.4).

Prop. (14.5.2.6) [Fiber Products]. Fiber products exist in the category of rigid analytic space. This is fiber product of affinoid spaces are affinoid so we can glue them by universal property, the same as (5.2.7.15).
Prop. (14.5.2.7). An affinoid space is connected in the weak Grothendieck topology iff it is connected in the strong Grothendieck topology iff it is connected in the Zariski topology.

Proof: Firstly the weak and strong are equal because any strong covering of \( X \) has a refinement of weak covering, and a weak covering is a strong covering. So it suffices to prove the equivalence of the last two.

One direction is trivial, for the other direction, use Tate’s acyclicity, if \( X_1, X_2 \to \text{Sp}A \), \( X_1 \cap X_2 = 0 \), then \( A = \mathcal{O}_X(X_1) \times \mathcal{O}_X(X_2) \), so Spec \( A \) is not connected, neither do Spec \( A \).

\( \Box \)

Prop. (14.5.2.8). We can define the connected components of \( X \) as the equivalence classes of elements that can be reached using connected admissible open subsets of \( X \). Then the connected components are admissible and forms an admissible cover of \( X \).

Proof: Notice that there exists a finite covering consisting of connected Zariski subsets, by (14.5.2.7) and the fact \( \text{Sp}A \) has f.m. connected components because Spec \( A \) does as \( A \) is Noetherian (10.3.4.12) and (14.5.1.3).

Thus we are done, because by (14.5.1.22), a Zariski covering is admissible, and clearly the connected components of \( X \) are just this Zariski covering.

\( \Box \)

Rigid GAGA

Lemma (14.5.2.9). Let \( Z \) be an affine scheme algebraic over \( K \), and \( Y \) a rigid \( K \)-space, then the set of morphisms of local \( G \)-ringed spaces \( (Y, \mathcal{O}_Y) \to (Z, \mathcal{O}_Z) \) corresponds to \( K \)-algebra morphisms from \( \mathcal{O}_Z(Z) \) to \( \mathcal{O}_Y(Y) \).

Proof: Cf. [Formal and Rigid Geometry P111].

Def. (14.5.2.10) [Rigid Analytification]. There is a partial functor \( X^{\text{rig}} \) from the category of schemes \( X \) locally algebraic over a valued field \( K \) to the category of rigid \( K \)-spaces that are right adjoint to the forgetful functor from the category of rigid \( K \)-spaces to local ringed \( K \)-space, called the GAGA functor.

The existence of this functor is proven in (14.5.2.14).

Def. (14.5.2.11) [Analytification of Affine Schemes]. Let \( T_n(r) \) be the elements \( \sum a_v \zeta^v \in T_n \) that \( \lim a_v r^{|v|} = 0 \). Then choose a \( c \in K, |c| > 1 \), define \( T_n^{(i)} = T_n(|c|^i) \). Then \( T_n^{(i)} = K\langle c^{-i}X_1, \ldots, c^{-i}X_n \rangle \), so clearly Spec \( (T_n^{(i)}) \) is an affinoid subdomain of Spec \( (T_n^{(i+1)}) \) by (14.5.1.9). Thus there is a chain of inclusions of affinoid subdomains:

\[ B^n = \text{Sp}(T_n^{(0)}) \hookrightarrow \text{Sp}(T_n^{(1)}) \hookrightarrow \text{Sp}(T_n^{(2)}) \hookrightarrow \ldots \]

Then we can use (14.5.2.4) to glue them together as \( \mathbb{A}_K^{n,\text{rig}} \).

Prop. (14.5.2.12). The maximal spectrum Max\( (K[X_i]) = \cup_n \text{Sp}(T_n^{(i)}) \) as sets.

Proof: It suffices to show the following two.

- For any maximal ideal \( m \subset T_n \), \( m' = m \cap K[X_i] \) is maximal.
- For any maximal ideal \( m' \subset K[X_i] \), there is some \( N \) that \( m'T_n^{(i)} \) is maximal in \( T_n^{(i)} \) for all \( i > N \).
For 1: Consider the $K \subset K[X_i]/m' \subset T_n/m$, $T_n/m$ is a finite extension of $K$ by (10.3.4.10), then so does $K[X_i]/m'$, by (4.2.1.3). To prove $m' = m \cap K[X_i]$, consider the following diagram:

$$
\begin{array}{ccc}
K[X_i]/m' & \twoheadrightarrow & T_n/m'T_n \\
\| & & \downarrow \\
K[X_i]/m' & \longrightarrow & T_n/m
\end{array}
$$

As $K[X_i]/m'$ is finite over $K$, it is complete, but $K[X_i]$ is dense in $T_n$, thus the horizontal maps are surjective. But then the lower horizontal is isomorphism, then the upper horizontal is also isomorphism, and then the vertical map is isomorphism, thus we are done.

For 2, $K[X_i]/m'$ is a finite extension of $K$, thus has a unique valuation, let $N$ be large that $|X_i| \leq |c|^N$, then for $i > N$, the quotient map factors uniquely as $K[X_i] \to T_n^{(i)} \to K/m'$. Then the kernel $m$ of $T_n^{(i)}$ is a maximal ideal (same reason as before) that satisfies $m \cap K[X_i] = m'$. Then we finish by item 1. □

Cor. (14.5.2.13) [Analytification for Affine Schemes]. Similarly, for an affine scheme $Z = \text{Spec} K[X_i]/a$ of f.t over $K$, we construct its analytification $Z^{rig}$ as the glue of the inclusions:

$$\text{Sp}(T_n^{(0)}/a) \leftarrow \text{Sp}(T_n^{(1)}/a) \leftarrow \ldots$$

Then $Z^{rig}$ is the analytification of $K[X_i]/a$.

And we see from the proof of (14.5.2.12) the maximal spectrum $\text{Max}(K[X_i]/a) = \cup_n \text{Spa}(T_n^{(i)}/a)$ as sets.

Proof: The canonical map $K[X_i]/a \to T_n^{(i)}/a$ glue together to be a morphism $\mathcal{O}_Z(Z) \to \mathcal{O}_Z^{rig}(Z^{rig})$, which by (14.5.2.9) corresponds to a map $Z^{rig} \to Z$ of local ringed spaces.

Now any other morphism $Y \to Z$ from a rigid $K$-space $Y$ to $Z$, choose an affinoid $K$-space covering $Y_i$ of $Y$, then the map $Y_i \to Z$ corresponds by (14.5.2.9) to a morphism $\sigma : K[X_i]/a \to \mathcal{O}_{Y_i}(Y_i)$, thus if we choose $i$ large enough that $|\sigma(X_i)| \leq |c|^i$, then $\sigma$ can be extended uniquely to $K[X_i]/a \to T_n^{(i)}/a \xrightarrow{\sigma} \mathcal{O}_{Y_i}(Y_i)$, by the universality of affinoid subdomains. This $\sigma$ corresponds to a morphism $Y_i \to \text{Sp}(T_n^{(i)}) \to Z^{rig}$, and these clearly glue together to give a morphism $Y \to Z^{rig}$, thus proving the universal property. □

Prop. (14.5.2.14) [General Analytification]. For any locally algebra scheme $X$ over $K$, choose an affine covering $Z_i$, consider the analytification of $Z_i$ by (14.5.2.13), then $Z_i \cap Z_j$ obviously has the inverse image as the rigid analytification by universal property, thus unique, so the analytifications of $Z_i$ can be glued to an analytification of $X$.

Moreover, the underlying set of $X^{rig}$ is identified with the closed pts of the scheme $X$, because this is the case of $Z_i$(14.5.2.11).

Prop. (14.5.2.15). Rigid analytification preserves fiber products.

Proof: This follows from the construction of fibered product of schemes (5.2.7.15), so we only need to prove the affine case. For this, Cf.[U. Köpf, Über eigentliche Familien algebraischer Varietäten über affinoiden Räumen. Schriftenr., Satz 1.8]. □

Prop. (14.5.2.16) [Stalks]. For a point $z \in Z^{rig}$, the completion of $\mathcal{O}_{Z^{rig},z}$ and $\mathcal{O}_{Z,z}$ are the same.

3 Coherent Sheaves on Rigid Spaces

Prop. (14.5.3.1). For an affinoid $K$-space $X$, there is a $\mathcal{O}_X$ module construction $M \to M \otimes_A \mathcal{O}_X$ as in (14.5.1.40) in the weak Grothendieck topology, and it extends uniquely to a sheaf w.r.t. the strong Grothendieck topology by (14.5.1.41), also denoted by $M \otimes_A \mathcal{O}_X$. This is a faithfully exact, fully faithful functor between Abelian categories from $\mathcal{A}$ to $\mathcal{O}_X$-modules, and it preserves tensor product and direct sums.

Proof: Because $\Gamma(X, M \otimes_A \mathcal{O}_X) = M$ and obviously fully faithful, this map is fully faithful, and it is exact because the restriction map of an affinoid subdomain is flat (14.5.1.26), and shiffification is exact.

Def. (14.5.3.2) [Coherent Sheaves]. For an $\mathcal{O}_X$-module $\mathcal{F}$ on a rigid space $X$, finite type, of finite presentation, coherence are defined w.r.t the strong topology as $X$ is a ringed site. All these notions are stable under passing to an admissible open subspaces.

Proof: For the passing of coherence to admissible open subspaces, use the fact that restriction maps are flat (14.5.1.26).

Cor. (14.5.3.3). Notice $\mathcal{O}_X^n = A^n \otimes_A \mathcal{O}_X$, by (14.5.3.1) and the fact $A$ is Noetherian, passing to a refinement covering, $\mathcal{F}$ is coherent iff there is an admissible affinoid covering $\mathcal{U}: X_i \to X$ that $F^1|_{X_i}$ is associated to a finite $\mathcal{O}_{X_i}$-module. In this case, $\mathcal{F}$ is said to be $\mathcal{U}$-coherent. Thus the coherent sheaves form a weak Serre subcategory of $\mathcal{O}_X$-modules.

In particular, $\mathcal{O}_X$ is coherent.

Prop. (14.5.3.4). If $\mathcal{F}, \mathcal{G}$ are all $\mathcal{U}$-coherent modules, then:

- $\mathcal{F} \otimes_{\mathcal{O}_X} \mathcal{G}$ and $\mathcal{F} \oplus \mathcal{G}$ are $\mathcal{U}$-coherent,
- if $\mathcal{T} \to \mathcal{G}$ is a $\mathcal{O}_X$-module morphism, then the kernel and image are all $\mathcal{U}$-coherent.
- If $\mathcal{I}$ is a $\mathcal{U}$-coherent sheaf of ideal of $\mathcal{O}_X$, then $\mathcal{I}\mathcal{F}$ is $\mathcal{U}$-coherent.

Proof: The first and the second are consequences of (14.5.3.1), noticing $A_i$ is Noetherian. The third is an image of $\mathcal{I} \otimes_{\mathcal{O}_X} \mathcal{F}$.

Lemma (14.5.3.5). If $\mathcal{F}$ is $\mathcal{U}$ coherent for a simple Laurent covering $\mathcal{U}$, then $H^1(\mathcal{U}, \mathcal{F}) = 0$.

Proof: The goal is to show any element in $\mathcal{F}(U_1 \cap U_2)$ can be represented by $u_1 + u_2$, where $u_i \in \mathcal{F}(U_i)$. Let $U_1 = \text{Sp} A(f), U_2 = \text{Sp} A(f^{-1}), U_1 \cap U_2 = \text{Sp} A(f, f^{-1})$. Now $A(f) = A(X)/(X - f), A(f^{-1}) = A(Y)/(Yf - 1), A(f, f^{-1}) = A(X, Y)/(X - f, Yf - 1)$, and we endow them with the residue norm.

Now we want to give norms to $M_1 = \mathcal{F}(U_1), M_2 = \mathcal{F}(U_2), M_{12} = \mathcal{F}(U_1 \cap U_2)$. $M_i$ are finite $\mathcal{O}_X(U_i)$-modules, so there are elements $v_i, w_j, i \leq m, j \leq n$ that generate $M_1, M_2$ respectively. So there are attached morphisms

\[(A(f))^m \to M_1, \quad (A(f^{-1}))^n \to M_2, \quad (A(f, f^{-1}))^m \to M_{12}\]

And endow them with the residue norm, which is complete.

Notice that to prove the assertion, it suffice to show for each $\varepsilon > 0$, there is an $\alpha$ that for each $u \in \mathcal{U}$, there are $u_1$ and $u_2$ in $M_i$ respectively that $|u_i| < \alpha |u|$ and $|u - u_1 - u_2| < \varepsilon |u|$, because then we can use iteration and completeness to get the result.
Giving $\beta > 1$, any $g \in A(f, f^{-1})$ can be lifted to an element $\sum c_{ij} X^i Y^j$ that $|c_{ij}| \leq \beta |g|$. Then by regrouping terms that $i = j$ or $i < j$, there are two element $g^+ \in A(f)$ and $g^- \in A(f^{-1})$ that $g^+ + g^-$ restricts to $g$ on $U_1 \cap U_2$, and $|g^+|, |g^-| \leq \beta |g|$.

Now that $\mathcal{F}$ is coherent, so $v_i$ and $w_j$ both generate $M_{12}$ separately. Then there are equations $v_i = \sum c_{ij} w_j$ and $w_i = \sum d_{ij} v_j$, where $c_{ij}, d_{ij} \in A(f, f^{-1})$. The image of $A(f)$ is dense in $A(f, f^{-1})(10.3.4.26)$, so there are elements $c'_{ij} \in A(f^{-1})$ s.t. $\max |c_{ij} - c'_{ij}| |d_{ij}| < \beta^{-2} \varepsilon$.

Now I claim the above approximation process is true for $\alpha = \beta^2 \max(|c'_{ij}| + 1)$. For this, notice for any $u = \sum a_i v_i$ with $a_i \in A(f, f^{-1})$, which we may assume $|a_i| \leq \beta |u|$ by the definition of the norm on $M_{12}$, then $a_i = a_i^+ + a_i^-$, that $|a_i^+| \leq \beta |a_i|$. Consider the following element

$$u^+ = \sum a_i^+ v_i \in M_1, \quad u^- = \sum a_i^- \sum c'_{ij} w_j \in M_2$$

Then it is easily verified that $|u^*| < \alpha |u|$, and

$$u - u^- - u^+ = \sum a_i^- (c_{ij} - c'_{ij}) w_j = \sum \sum a_i^- (c_{ij} - c'_{ij}) d_{ij} v_i,$$

which has norm smaller than $\max |a_i^- (c_{ij} - c'_{ij})| |d_{ij}| \leq \beta^2 |u| \cdot \beta^{-2} \varepsilon = \varepsilon |u|$, finishing the proof. \qed

**Prop. (14.5.3.6)[Kiehl]**. An $\mathcal{O}_X$-module $\mathcal{F}$ on an affinoid $K$-space $\text{Sp} A$ is coherent iff it is associated to a finite $A$-module.

**Proof**: The converse is obvious, for the other direction, by (14.5.1.39), it suffices to prove for $\mathcal{U}$ a Laurent covering, and further, it suffices to prove for the simplest Laurent covering $X(f), X(f^{-1}) \to X$ because: $U(f, g) \cup U(f, g^{-1}) \cup U(f^{-1}, g) \cup U(f^{-1}, g^{-1}) = (U(f, g) \cup U(f, g^{-1})) \cup (U(f^{-1}, g) \cup U(f^{-1}, g^{-1}))$.

Thus the above lemma shows that $H^1(\mathcal{U}, \mathcal{F}) = 0$. Now I prove that for any finite affinoid covering $\mathcal{U} = \sqcup \text{Sp} A_i$, if $H^1(\mathcal{U}, \mathcal{F}) = 0$ for any coherent sheaf $\mathcal{F}$, then any $\mathcal{U}$-coherent sheaf $\mathcal{F}$ is associated to a finite $A$-module, this will finish the proof.

Consider any maximal ideal $m_x$ of $A$, $m_x \otimes_A \mathcal{O}_X$ is a coherent sheaf as $m_x$ is finite because $A$ is Noetherian, so there is a short exact sequence

$$0 \to m_x \mathcal{F} \to \mathcal{F} \to \mathcal{F}/m_x \mathcal{F} \to 0$$

of $\mathcal{U}$-coherent sheaves, because $A/m_x$ is a field, thus flat.

Now for any affinoid space $U'$ in $U_i$ for some $i$, the section of this exact sequence is exact, because the ring morphism associated to an affinoid subdomain is flat (14.5.1.26). In particular, this can be applied to any intersections of $U_i$, in particular the Čech complex of these sheaves. Then the long exact sequence and the fact $H^1(\mathcal{U}, m_x \mathcal{F}) = 0$ shows

$$0 \to m_x \mathcal{F}(X) \to \mathcal{F}(X) \to \mathcal{F}/m_x \mathcal{F}(X) \to 0$$

Next we want to show $\mathcal{F}/m_x \mathcal{F}(X) \to \mathcal{F}(U') \to \mathcal{F}/m_x \mathcal{F}(U_i)$ is isomorphism for any $x \in U_i$. To prove this, first for any affinoid subspace $U' = \text{Sp} B$ contained in some $U_j$, let $U' \cap U_i = \text{Sp} B_i$, $\mathcal{F}|_{U'} = M' \otimes_A \mathcal{O}_{U'}$, we show $\mathcal{F}/m_x \mathcal{F}(U') \cong \mathcal{F}/m_x \mathcal{F}(U' \cap U_i)$, this is equivalent to

$$M'/m_x M' \to M'/m_x M' \otimes_B B_i = M'/m_x M' \otimes_B/m_x B B_j/m_x B_j$$

is an isomorphism. But $B/m_x B \cong B_j/m_x B_j$: This is true when $x \in U'$ by (14.5.1.8), and they are both trivial ring if $x \notin U'$. Then look at the morphism of Čech complex induced by $\mathcal{F}/m_x \mathcal{F} \to$
\( \mathcal{F}/\mathfrak{m}_x \mathcal{F}|_{U_i} \), then it is an isomorphism, by what we just proved, so its \( H^0 \) is also isomorphism, which is \( \mathcal{F}/\mathfrak{m}_x \mathcal{F}(X) \cong \mathcal{F}/\mathfrak{m}_x \mathcal{F}(U_i) \).

Finally, by the commutative diagram

\[
\begin{array}{ccc}
\mathcal{F}(X) & \longrightarrow & \mathcal{F}/\mathfrak{m}_x \mathcal{F}(X) \\
\downarrow & & \downarrow \\
\mathcal{F}(U_i) & \longrightarrow & \mathcal{F}/\mathfrak{m}_x \mathcal{F}(U_i)
\end{array}
\]

 morphism, so if denote \( \mathcal{F}(U_i) \) by \( M_i \), then \( \mathcal{F}(X) \) generate \( M_i/\mathfrak{m}_x M_i \) for every \( x \), then consider \( L = M_i/\mathcal{F}(X) \), then \( \mathfrak{m}_x L = L \) for every \( x \), then by Nakayama, for each maximal ideal \( \mathfrak{m} \), there is a \( m \in \mathfrak{m} \) that \( (1 + m)L = 0 \), so \( \text{Ann}(L) = (1) \), so \( L = 0 \), i.e. \( \mathcal{F}(X) \) generate \( M_i \) for each \( i \).

Now choose \( f_i \) in \( \mathcal{F}(X) \) that generate \( M_i \) simultaneously, then the map \( \mathcal{O}^n_X \to \mathcal{F} \) is a surjection of \( \mathfrak{u} \)-coherent sheaves, its kernel \( G \) is also coherent by (14.5.3.4), now all the above argument works for \( G \), so there is a surjection \( \mathcal{O}^n_X \to G \), so \( \mathcal{O}^n_X \to \mathcal{O}^n_X \to \mathcal{F} \to 0 \), so \( \mathcal{F} \) is associated to the cokernel of the map \( A^n \to A^n \).

\[ \square \]

Cor. (14.5.3.7). Coherence for a \( \mathcal{O}_X \)-module on a rigid \( K \)-space is affinoid local on the target.

**Cohomology on Rigid Analytic Spaces**

**Lemma (14.5.3.8).** The category of \( \mathcal{O}_X \)-modules on a rigid \( K \)-space is a Grothendieck category by (3.3.2.28).

**Def. (14.5.3.9)[Derived Cohomologies].** Consider the right derived functor for \( \Gamma \) and more general \( f_* \), these are left exact by (5.1.2.9). Then \( R^p f_* \mathcal{F} = (f_* \mathcal{H}^p(\mathcal{F}))^\delta \) by Grothendieck spectral sequence.

The Cech-to-Derived spectral sequence (5.3.2.13) is applied: \( H^p(\{U_i \to U\}, \mathcal{H}^q(F)) \Rightarrow H^{p+q}(U, F) \) and \( H^1(U, F) \cong H^1(U, F) \).

In particular, if \( H^q(U_{i_0i_1 \ldots i_r}, \mathcal{F}) = 0 \), then \( H^p(\{U_i \to U\}, \mathcal{F}) = H^p(U, \mathcal{F}) \) (5.3.2.15).

And it is enough to have \( H^q(U_{i_0i_1 \ldots i_r}, \mathcal{F}) = 0 \), then \( p > 0 \) by (5.3.2.16).

**Cor. (14.5.3.10).** A Qco sheaf on an affinoid space has vanishing higher sheaf cohomology by Tate’s acyclicity (14.5.1.40) and (5.3.2.16).

**Properties of Rigid \( K \)-Spaces**

This subsubsection is strongly suggested to read after reading the parallel part of schemes.

**Def. (14.5.3.11).** A morphism is called a **closed immersion** if there is an admissible affinoid covering that it restricts to a closed immersion of affinoid spaces (It is compatible with definition (14.5.1.28) before by (14.5.3.15)). It is called an **open immersion** iff it is injective and the corresponding stalk maps are isomorphisms. The **(quasi-)separatedness**, **(quasi-)compactness**, **finiteness** are defined similarly as for schemes.

**Lemma (14.5.3.12)[Nike’s Trick].** In a rigid analytic \( K \)-space \( X \) and \( \text{Sp} A, \text{Sp} B \) be affinoid subspaces, then there is an admissible affinoid covering of \( \text{Sp} A \cap \text{Sp} B \).

**Proof:** This is analogous to the scheme case (5.4.1.1), but the proof is different: \( X \) has an admissible covering, this restricts to an admissible covering of \( \text{Sp} A \cap \text{Sp} B \), and any admissible covering can be refined by an affinoid admissible covering. \[ \square \]
Prop.(14.5.3.13) [Affinoid Communication Theorem]. A property $P$ of affinoid open subsets of $X$ is called **affinoid local** if: $\text{Sp} A$ has $P \Rightarrow$ all affinoid subdomains of $\text{Sp} A$ has $P$, and any admissible affinoid cover of $\text{Sp} A$ has $P \Rightarrow \text{Sp} A$ has $P$. Notice a stalk-wise property is obviously affine-local.

Now if we call $X$ has $\tilde{P}$ if there is an admissible affinoid covering $A_i \to X$ that $A_i$ has $P$. Then the following are equivalent:

- all open affinoid subsets of $X$ has $P$.
- all open subspace of $X$ has $\tilde{P}$.
- $X$ has a cover of open subspaces that has $\tilde{P}$.
- $X$ has $\tilde{P}$.

*Proof:* The proof is the same as the scheme case(5.4.1.2).

Prop.(14.5.3.14). Separated morphism is quasi-separated because closed immersion is affinoid hence quasi-compact(14.5.1.3).

Prop.(14.5.3.15)[Finite Morphism]. For a morphism $\varphi : X \to Y$ of rigid $K$-spaces

- It is finite iff the inverse image of any affinoid space is affinoid, and $\varphi_\ast \mathcal{O}_Y$ is a coherent $\mathcal{O}_X$-module. In particular, finiteness is local on the target because coherence do.
- It is closed immersion iff it is finite and $\mathcal{O}_Y \to \varphi_\ast \mathcal{O}_X$ is surjective, this shows the definition of closed immersion is compatible with before.

*Proof:* Coherence is affinoid local on the target by Kiehl’s theorem, so it suffices to prove the inverse image of any affinoid space is affinoid for a finite morphism: Consider any affinoid subdomain $U \subset X$ with inverse image $\varphi^{-1}(U)$, by Kiehl’s theorem, $B = \mathcal{O}_X(f^{-1}(U))$ is finite over $A = \mathcal{O}_Y(U)$, thus can be given an affinoid $K$-algebra structure(10.3.4.33). Now

$$\varphi^{-1}(U) \xrightarrow{\chi} \text{Sp} B \xrightarrow{\rho'} \text{Sp} A$$

$\chi$ is locally an isomorphism, as $\rho$ is finite, so $\chi$ is an isomorphism.

The second assertion is because locally $\mathcal{O}_Y, \varphi_\ast \mathcal{O}_X$ are both Qco so surjectivity is equivalent to the global section is surjective(14.5.3.1).

Prop.(14.5.3.16). Closed/Open immersion, quasi-compactness, (quasi-)separatedness are all local on the target, and stable under base change.

*Proof:* Closed immersion is local on the target because finiteness do and surjectiveness of $\mathcal{O}_Y \to \varphi_\ast \mathcal{O}_X$ is checked locally. Open immersion is local on the target because stalk and injectivity are all checked locally.

Then Closed/Open immersion are stable under base change because the affinoid case is true(14.5.1.29).

Quasi-compact is easily seen local on the target and stable under base change.

(Quasi-)Separateness is local on the target because closed immersion and quasi-compact do.

(Quasi-)Separateness is stable under base change because closed immersion and quasi-compact do, because diagonal commutes with base change(3.1.1.48).

Prop.(14.5.3.17). Morphisms between affinoid $K$-spaces are separated. Moreover, because of local-ness, any finite morphism is separated.
4 Proper Mapping Theorem

Def.(14.5.4.1). For a rigid space $X$ over affinoid space $Y$, if $U \subset U' \subset X$ be affinoid subspaces, $U$ is called relatively compact in $U'$ iff there is a set of affinoid generators $f_i$ of $\mathcal{O}_X(U')$ over $\mathcal{O}_Y(Y)$ that $|f_i(x)| < 1$ on $U$. This is denoted by $U \Subset Y U'$.

Prop.(14.5.4.2). If $X_1, X_2$ are affinoid spaces over an affinoid space $Y$, and $U_i$ are affinoid space of $X_i$, then

- if $U_1 \Subset Y X_1$, then $U_1 \times_Y X_2 \Subset X_2 X_1 \times_Y X_2$.
- if $U_i \Subset Y X_i$, then $U_1 \times_Y U_2 \Subset Y X_1 \times_Y X_2$.
- If $U_i \Subset Y X_i$, and $X_i$ are affinoid subspaces of a rigid space separable over $Y$, then $U_1 \cap U_2 \Subset Y X_1 \cap X_2$.
- If $U_1 \Subset Y X_1$, and $i : T \to X_1$ is a closed immersion, then $i^{-1}(U_1) \Subset Y i^{-1}(X_1)$.

The proof is easy. For the last one, should notice $|f(x)| = |f(i(x))|$, because it is closed immersion, so the residue field is the same.

Def.(14.5.4.3) [Proper Morphism]. A proper morphism $\varphi : X \to Y$ of rigid $K$-spaces is a separated morphism that there is an admissible affinoid covering $Y_i$ of $Y$ that there are two admissible affinoid coverings $X_{ij}, X'_{ij}$ of $\varphi^{-1}(Y_i)$ that $X_{ij} \Subset Y_i X'_{ij}$ for any $i, j$.

Prop.(14.5.4.4). Properness is stable under base change and composition

Proof: The base change follows directly from(14.5.4.2).

For the composition, Cf.[Formal and Rigid Geometry P131](difficult).

Prop.(14.5.4.5). Properness is local on the target.

Proof: This is because separatedness is local on the target(14.5.3.16) and the second condition of properness is itself local.
Prop. (14.5.4.6). If \( g \circ f : X \to Y \to Z \) is proper and \( g \) is separated, then \( f \) is proper.

Proof: By (14.5.3.18), \( \tau : X \to X \times_Z Y \) is closed immersion, and \( f \) is separated by (14.5.3.21). Now proper is local, so we may assume \( Z \) is affinoid, so there are two admissible covering \( X_i, X'_i \) of \( X \) that \( X_i \subseteq Z \subseteq X'_i \), and choose an admissible affinoid covering \( Y_i \to Y \), then \( X_j \times_Z Y_i, X'_j \times_Z Y_i \) are admissible coverings of \( Y_i \) that is \( X_j \times_Z Y_i \subseteq Y_i, X'_j \times_Z Y_i \). And it can be pulled back to an affinoid admissible coverings of \( f^{-1}(Y_i) \) that \( \tau^{-1}(X_j \times_Z Y_i) \subseteq Y_i, \tau^{-1}(X'_j \times_Z Y_i) \), because \( \tau \) is closed immersion. So \( X \to Y \) is proper.

Prop. (14.5.4.7). Finite morphism is proper, in particular, closed immersion is proper.

Proof: Finite morphism is separated by (14.5.3.17), and locally, assume both space are affinoid, \( X = \text{Sp} B \to \text{Sp} A = Y \), then \( B \) is a finite \( A \)-module, in priori a f.g. \( A \)-algebra, so there is a set of generators \( f_i \) of \( B \) over \( A \) that (by multiplying a constant in \( K^* \)) \( |f_i|_{\text{sup}} < 1(10.3.4.21) \), so \( X \subseteq_Y X \), hence it is proper.

Prop. (14.5.4.8) [Proper and Analytification]. For a morphism between schemes locally of f.t. over \( K \), it is proper iff its rigid analytification is proper.


For the following: Cf.[Formal and Rigid Geometry P132].

Prop. (14.5.4.9) [Proper Mapping theorem, Kiehl]. The higher direct images of a proper map of rigid analytic spaces takes coherent sheaves to coherent sheaves.

Proof:

Prop. (14.5.4.10). For a scheme \( X \) locally of f.t. over \( K \), an \( \mathcal{O}_X \)-module \( \mathcal{F} \) on \( X \) gives rise to an \( \mathcal{O}_{X^{\text{rig}}} \)-module on \( X^{\text{rig}} \), and it is coherent iff \( \mathcal{F} \) is coherent.

Proof:

Prop. (14.5.4.11). For a proper scheme over \( K \), \( H^q(X, \mathcal{F}) \cong H^q(X^{\text{rig}}, \mathcal{F}^{\text{rig}}) \) for \( \mathcal{F} \) coherent.

Proof:

Prop. (14.5.4.12). When \( X \) is proper, coherent sheaves on \( X^{\text{rig}} \) corresponds to coherent sheaves on \( X \). This gives an analog of Chow’s theorem when applied to \( X = \mathbb{P}^n_K \) and \( \mathcal{F} \) is a sheaf of ideals in \( \mathcal{O}_{X^{\text{rig}}} \).

Proof:

5 Formal Geometry

Main references for this subsection is [Bos15], [Hartshorne] and [Topics in Algebraic Geometry, Illusie].

Def. (14.5.5.1) [Formal Spectrum \( \text{Spf} A \)]. Let \( A \) be a complete adic ring (10.3.1.8) with an ideal of definition \( \alpha \) that the \( A \) is \( \alpha \)-adically complete and separated. Then we let \( \text{Spf} A \) be the topological space \( \text{Spec}(A/\alpha) \) (open primes of \( A \)), and there is a structure sheaf \( \mathcal{O} \) on \( \text{Spf} A \) that \( \mathcal{O}(\text{D}(f)) = \text{A}(f^{-1}) \).
14.5. FORMAL AND RIGID GEOMETRY

Proof: To construct this sheaf, we first check that $\mathcal{O}(D(f)) = A(f^{-1}) = \lim_{\leftarrow n} (A/\alpha^n[f^{-1}])$ defines a sheaf on the site of subspaces of $\text{Spf} \ A$ of the form $D(f)$: For any open covering $\{D(f_i)\}$ of $D(f)$, there are exact sequences:

$$0 \to (A/\alpha^n)_f \to \prod_i (A/\alpha^n)_{f_i} \to \prod_{i,j} (A/\alpha^n)_{f_i f_j}$$

by (4.4.2.3). Then we take inverse limit, which is exact by Mittag-Leffler (4.6.3.2), to get an exact sequence, which is just the sheaf condition of $\mathcal{O}$. Then, we can use (5.1.2.24) to extend this sheaf to a sheaf on $\text{Spf} \ A$.

$\square$

Prop. (14.5.5.2) [Stalks of $\text{Spf} \ A$]. Let $x \in \text{Spf} \ A$ correspond to a prime $\mathfrak{p}_x$ in $A$. Then the stalk of $\text{Spf} \ A$ at $x$ is just $\mathcal{O}_x = \lim_{\leftarrow x \in D(f)} A(f^{-1})$, which is a local ring with maximal ideal $\mathfrak{m}_x$ containing $\mathfrak{p}_x \mathcal{O}_x$. Moreover, $\mathfrak{m}_x = \mathfrak{p}_x \mathcal{O}_x$ iff $\alpha$ is f.g.. So $\text{Spf} \ A$ is a local ringed space, called the affine formal scheme of $A$.

Proof: Cf. [Bos15]P159.$\square$

Remark (14.5.5.3). In many case, for example in Scholze’s treatment of the $p$-adic geometry, the ideal of definition $\alpha$ is assumed to be f.g., because we need this to show that the $\alpha$-adic completion of $A[f^{-1}]$ is $(\alpha)$-adically complete (4.2.3.6), so that we can interpret $D(f) \subset \text{Spf} \ A$ as an affine formal scheme $\text{Spf}(A(f^{-1}))(10.3.1.11)$.

Another way to get around this finiteness condition is to consider formal spectrum for a larger class of rings, called the admissible rings, which is a complete and separated topological ring with a basis consisting of open ideals, and with an ideal of definition $\alpha$ that $\alpha^n \to 0$ for $n \to 0$.

Prop. (14.5.5.4) [Affine Formal Adjointness]. Morphisms between local topologically ringed spaces $\text{Spf} \ B \to \text{Spf} \ A$ corresponds to continuous homomorphisms $A \to B$.

Def. (14.5.5.5) [Formal Schemes]. The category of formal schemes is the full subcategory of the category of local topologically ringed topological spaces $(X, \mathcal{O}_X)$ consisting of objects that is locally isomorphic to an affine formal scheme $\text{Spf} \ A$.

The category of formal schemes contains the category of schemes, by mapping $\text{Spec} \ A$ to $\text{Spf} \ A$, where $A$ is endowed with the discrete topology.

Prop. (14.5.5.6) [Glueing and Fiber Products]. Formal Schemes can easily be glued, and also spectrum adjointness holds as in (14.5.2.5). Finally there are fibered products, constructed as in (5.2.7.15), where the affine case corresponds to completed tensor product (10.3.1.12).

Def. (14.5.5.7) [Formal Completion of Schemes Along a Closed Subscheme]. Let $X$ be a scheme and $Y$ a closed subscheme of $X$ defined by a Qco ideal $\mathcal{I} \subset \mathcal{O}_X$, then consider the sheaf $\mathcal{O}_Y$ defined by restricting the projective limit $\lim_{\leftarrow n} \mathcal{O}_X/\mathcal{I}^n$ to $Y$, then $(Y, \mathcal{O}_Y)$ is a locally topologically ringed space, called the formal completion of $X$ along $Y$.

Noetherian Adic Formal Schemes

Cf. [Hartshorne Chap 2.9] and [Sta]30.23. and Illusie.

Def. (14.5.5.8) [Noetherian Formal Adic Schemes].

Def. (14.5.5.9) [Coherent Sheaves on Noetherian Formal Adic Schemes].
**Prop. (14.5.5.10).** Let $A$ be a Noetherian ring and $I$ an ideal, let $X$ be a proper scheme over $A$ and $\mathcal{F}$ a coherent sheaf on $X$, then for any $p \geq 0$, the inverse systems $\left( H^p(X, I^n \mathcal{F}) \right)$ and $\left( I^n H^p(X, \mathcal{F}) \right)$ are isomorphic pro-$A$-modules.

*Proof:* Cf. [Sta]02OA.

**Thm. (14.5.5.11) [Theorem of Formal Functions].** Let $A$ be a Noetherian ring with an ideal $I$, $X$ be a proper scheme over $A$ and $\mathcal{F}$ a coherent scheme on $X$. Then for any $p \geq 0$, the system of maps

$$H^p(X, \mathcal{F})/I^n H^p(X, \mathcal{F}) \to H^p(X, \mathcal{F}/I^n \mathcal{F})$$

induce an isomorphism of limits

$$H^p(X, \mathcal{F}) \cong \lim_{\leftarrow n} H^p(X, I^n \mathcal{F}).$$

*Proof:* Cf. [Sta]02OC.

**Prop. (14.5.5.12) [Grothendieck’s Existence Theorem].** Cf. [Sta]0883.

**Prop. (14.5.5.13) [Grothendieck’s Algebrization Theorem].** Cf. [Sta]089A.

### 6 Admissible Formal Schemes

**Remark (14.5.6.1) [Setup].** For a good theory of Admissible formal schemes, let the base ring $R$ be an adic ring with an ideal of definition $I$ that satisfies either one of the following situation:

- $R$ is an adic valuation ring with a principal ideal of definition.
- $R$ is Noetherian and has no $I$-torsion.

**Def. (14.5.6.2) [Admissible Formal Schemes].** Let $R$ be an adic ring, then a formal $R$-scheme $X$ is called **locally of topologically finite type/finite presentation/admissible** if there is an open affine covering $\text{Spf} A_i$ of $X$ that $A_i$ satisfies those properties (10.3.1.13).

$X$ is called **topologically of finite type** if it is locally of topologically finite type and quasi-compact. It is called **topologically of finite presentation** if it is locally of topologically finite presentation, quasi-compact and quasi-separated.

**Prop. (14.5.6.3) [Induced Admissible Formal Subscheme].** Let $X$ be a formal $R$-scheme that is locally of topologically finite type, and let $\mathcal{O}_X$ be its structure sheaf. Then we can look at the ideal sheaf $\mathcal{I} \subset \mathcal{O}_X$ consisting of all elements locally killed by a power of $I^n$. This is a qco sheaf, as $\mathcal{I}(U) = \{ f \in \mathcal{O}(U) | I^n f = 0 \text{ for some } n \}$, because the quotient by the RHS is locally topologically of finite type and has no $I$-torsion, thus admissible, by (10.3.1.15), and admissibility is local (10.3.1.16).

In particular we can take the closed subscheme $X_{adm} \subset X$ corresponding to $\mathcal{I}$, then it is an admissible formal scheme, called the **induced admissible formal subscheme** of $X$.

### 7 Formal Models

**Prop. (14.5.7.1) [Generic Fiber Functor].** Let $R$ be a complete valuation ring of height 1 with field of fraction 1 with field of fraction $K$, then the functor $A \mapsto A \otimes_R K$ from the category of $R$-algebras topologically of finite type to the category of affinoid $K$-algebras

Def. (14.5.7.2) [Formal Models]. In view of (14.5.7.1), one would like to describe all formal $R$-schemes that the generic fiber $X_{\text{rig}}$ is isomorphic to a given rigid $K$-space $X_K$. But first notice $A \mapsto A \otimes_R K$ kills all $R$-torsion, in particular the generic fiber functor only depends on the induced admissible formal scheme $X_{\text{adm}}$ (14.5.6.3). So given any rigid $K$-space $X_K$, any admissible formal $R$-scheme $X$ satisfying $X_{\text{rig}} \cong X_K$ is called a formal $R$-model of $X_K$.

Def. (14.5.7.3) [Admissible Formal Blowing-up].
14.6 $p$-adic Uniformizations

1 Mumford Curves

References are [Schottky Groups and Mumford Curves, 1980], [Mihran Papikian, Nonarchimedean uniformization and monodromy pairing].

Def. (14.6.1.1) [$p$-adic Schottky Groups]. For $p \in \mathbb{P}$, a $p$-adic Schottky group is a discrete, f.g. free subgroup $\Gamma \subset \text{PGL}_2(\mathbb{Q}_p)$.

Prop. (14.6.1.2). A subgroup $\Gamma \subset \text{PGL}(2, \mathbb{Q}_p)$ is a $p$-adic Schottky group if it is discrete, f.g. and torsion-free.

Proof: $\Gamma$ acts on the Bruhat-Tits building $\Delta$ of $\text{PGL}(2, \mathbb{Q}_p)$, and the stabilizer is $\Gamma \cap \text{PGL}(2, \mathbb{Z}_p)$, which is a finite group as $\Gamma$ is discrete and $\text{PGL}(2, \mathbb{Z}_p)$ is compact. Thus it is trivial as $\Gamma$ is torsion-free. Thus $\Gamma$ acts freely on $\Delta$, so $\Gamma$ must be a free group. $\square$

Def. (14.6.1.3). A $p$-adic Schottky group $\Gamma$ acts on $\mathbb{P}^1(\mathbb{C}_p)$. Denote $\mathcal{L}_\Gamma$ is the set of limit points of this action, $\Omega_\Gamma = \mathbb{P}^1(\mathbb{C}_p) - \mathcal{L}_\Gamma$.

Thm. (14.6.1.4) [Mumford]. Let $\Gamma$ is a $p$-adic Schottky group of rank $g$, then there is a smooth complete curve $X_\Gamma/\mathbb{Q}_p$ of genus $g$ with an analytic isomorphism $\Omega_\Gamma/\Gamma \cong X_\Gamma(\mathbb{C}_p)$. Such a curve $X_\Gamma$ is called a $p$-adic Mumford curve.

Proof: $\square$

Thm. (14.6.1.5) [Mumford]. Let $\Gamma$ is a $p$-adic Schottky group of rank $g \geq 2$, then the corresponding Mumford curve $X_\Gamma$ has split degenerate stable reduction. Conversely, and smooth complete curve over $\mathbb{Q}_p$ with split degenerate stable reduction is a Mumford curve.

Where split degenerate reduction means that the normalization of all components of $\bar{X}$ are $\mathbb{F}_p$-rational, and all nodes are $\mathbb{F}_p$-rational with two $\mathbb{F}_p$-rational branches.

Proof: $\square$

Prop. (14.6.1.6) [Herrlich]. Suppose $p \in \mathbb{P}$ and $X/\mathbb{Q}_p$ is a Mumford curve with genus $g \geq 2$, then

$$\# \text{Aut}(X) \leq \begin{cases} 84(g-1) , & p = 2 \\ 24(g-1) , & p = 3 \\ 30(g-1) , & p = 5 \\ 12(g-1) , & p = 3 \end{cases}$$

Proof: $\square$
14.7 Rapoport-Zink Spaces

1 Isocrystals with Additional Structures

Main references are [Period Spaces for p-Divisible Groups, Rapoport/Zink] and [Isocrystals with Additional Structures, Kottwitz].

Def. (14.7.1.1) [Isocrystals with G-structures over $K_0$]. An isocrystal with $G$-structures over $K_0$ is an exact faithful $\otimes$-functor $\text{Rep}_{Q_p}(G) \to \varphi - \text{Mod}_{K_0}$.

Prop. (14.7.1.2) [Associated Isocrystals]. Let $L$ be a perfect field of char $p$ and $K_0 = W(L)[\frac{1}{p}]$ and let $b \in G(K_0)$, then to every $Q_p$-linear representation $V$ of $G$, we can associate an isocrystal

$$\text{Rep}_{Q_p}(G) \to \varphi - \text{Mod}_{K_0} : V \mapsto (V \otimes_{Q_p} K_0, b \circ (\text{id} \otimes \sigma)).$$

This is an isocrystal with $G$-structures over $K_0$ associated to $b$.

If $g \in G(K_0)$ and $b' = gb\sigma(g)^{-1}$, then multiplying by $g$ implies a natural isomorphism between $T_b$ and $T_{b'}$.

Prop. (14.7.1.3) [Associated Filtered Isocrystals]. Let $K$ be a field extension of $K_0$, $G$ be an algebraic group over $Q_p$, and $\mu : G_{m,K} \to G_K$ be a cocharacter over $K$, then the associated isocrystal over $K_0$ upgrades to a filtered isocrystal over $K$

$$\text{Rep}_{Q_p}(G) \to \varphi - \text{Fil Mod}_{K} I : V \mapsto (V \otimes_{Q_p} K_0, b \circ (\text{id} \otimes \sigma), \text{Fil}^*)$$

where the filtration comes from $\mu$ by weight-filtrations($G_m$ is diagonalizable).

Def. (14.7.1.4) [Admissible Pair]. Let $G$ be a reductive group, then a pair $(\mu, b)$ in (14.7.1.3) is called a (weakly)admissible pair if for any $Q_p$-representation of $G$, the filtered isocrystal $I(V)$ is (weakly)admissible.

It suffices to check this condition for any faithful representation $V$.

Proof: This is because for a faithful representation $V$, any $Q_p$-representation appears as a direct summand of $V_{\otimes n} \otimes \Hat{V}^{\otimes m}$ (15.3.1.16). Then the assertion follows from the fact direct summands and tensor products of (weakly)admissible filtered isocrystals is (weakly)admissible. □

Prop. (14.7.1.5) [Slope Morphism]. Let $D = \text{Spec} Q_p[\{T^{1/k}\}_{k \in \mathbb{Z}}] = D(Q)_Q$ be the pro-algebraic torus over $Q_p$ with character group $Q$, and $b \in G(K_0)$, then there is a morphism $\nu : D_{K_0} \to G_{K_0}$, called the slope morphism associated to $b$, which is defined as follows:

For any f.d. representation $\rho : G \to GL(V)$, there is an associated isocrystal defined in (14.7.1.2), then there is a morphism $\nu_\rho \in \text{Hom}_L(D, GL(V))$ that $D$ acts on the isotypical component $V_\lambda$ of $V$ by the character $\lambda \in Q = X^*(D)$. Then for any $x \in G(R)$, the mapping $\rho \mapsto \mu_\rho$ gives an automorphism of the standard fiber functor on $\text{Rep}(G)$, so by Tannakian duality corresponds to a unique element $x \in G(R)$ that $\rho(y) = \nu_\rho(x)$ for any $\rho$. The homomorphism $x \mapsto y$ is functorial in $R$ and thus defines an element $\nu \in \text{Hom}_L(D, G)$.

Notice the group $Q^*$ acts on $D$, and for $s \in Q^*$ and $v \in \text{Hom}(D, G)$, denote by $sv$ the composite $D \xrightarrow{v} D \xrightarrow{s} G$, and $D \to G_m$ the natural morphism, then for any $v$, there is a suitable $s$ that $sv$ factors through a morphism also denoted by $sv : G_{m,K_0} \to G_{K_0}$, as $G$ is algebraic.

Prop. (14.7.1.6) [Characterizing Slope Morphism]. The slope morphism can be characterized intrinsically to be the unique morphism $\nu \in \text{Hom}_L(D, G)$ that there exists some $s > 0, c \in G(L)$ that
• \( s\mu \in \text{Hom}_L(G_m, G) \),
• \( c(s\mu)c^{-1} \) is defined over \( \mathbb{Q}_p^s \),
• \( c(b\sigma)^n c^{-1} = c(n\nu)(p)c^{-1}\sigma^n \).

Proof: Cf.[Kottwitz, P13]. \( \square \)

Cor. (14.7.1.7) [Conjugate of Slope Morphism]. Now we can define the \( \sigma \)-conjugate of the slope morphism \( \nu \), and we have the identity

\[
bb' = \nu
\]

To check this, replace \( \nu \) by some \( s\nu \) to assume \( \nu \) factors through \( G_m \), then it suffices to show for any \( a \in K_0^s \),

\[
bs(\nu(\sigma^{-1}(a))) = \nu(a)b\sigma
\]

It suffices to check for any \( G \)-representation \( Q \), and it is true as \((V \otimes_{\mathbb{Q}_p} K_0, b\sigma)\) is a \( \varphi \)-module for \( \sigma \) and \( \nu(a) \) acts on the isotypical part of slope \( r \) by \( a^r \).

More generally, any \( g \in G(L) \) commuting with \( b\sigma \) also commutes with \( \varphi(a), a \in K_0^s \), as it preserves the isotypical decomposition for any isocrystal, and on the isotypical component \( V_\lambda \), the \( a \) acts by \( a^r \).

Def. (14.7.1.8) [Descent Conditions]. A \( \sigma \)-conjugacy class \( \bar{b} \) in \( G(\overline{K}) \) is called a descent if there is some \( s \geq 0 \) and some \( b \in \bar{b} \) that \( s\nu \) factors through \( D \to G_m \) and

\[
(b\sigma)^s = \nu(p)\sigma^s
\]

as an identity in \( G(K_0) \times \langle \sigma \rangle \).

Prop. (14.7.1.9). If \( G \) is connected and \( L \) is alg.closed, then any \( \sigma \)-conjugacy class is descent (14.7.1.8).

Proof: Cf.[Kottwitz]. \( \square \)

Prop. (14.7.1.10). Let \( \bar{b} \) be a descent and \( b \) satisfies the descent condition for \( s \) in (14.7.1.8), then if \( \mathbb{Q}_p^s = W(\mathbb{F}_p)[[\frac{1}{p}]], b \in G(\mathbb{Q}_p^s) \) and \( \nu \) is defined over \( \mathbb{Q}_p^s \).

Proof: Set \( b_s = b\sigma^s \), then iterating (14.7.1.7), \( b_s \nu(b_\sigma)^{s-1} = \nu \). And we have \( b_s = s\nu(p) \), so \( \nu^s = \nu \), so \( \nu \) is defined over \( \mathbb{Q}_p^s \).

To show the first assertion, notice \((b\sigma)(b\sigma)^s = (b\sigma)^s(b\sigma)\) shows

\[
s\nu(p)\sigma^s b\sigma = b\sigma s\nu(p)\sigma^s = s\nu(p)b\sigma^{s+1}(14.7.1.7).
\]

and then \( b\sigma^s = \sigma^s b \). \( \square \)

Cor. (14.7.1.11). If \( b_1, b_2 \in \bar{b} \) are descent w.r.t the same \( s \), then they are conjugate w.r.t. \( G(K_0 \cap \mathbb{Q}_p^s) \).

In particular, for any descent \( b \in G(\mathbb{Q}_p^s) \) and any \( \mathbb{Q}_p \)-representation \( V \) of \( G \), the induced isocrystal is defined over the field \( K_s = W(\mathbb{F}_p \cap L)[[\frac{1}{p}]] \), and it only depends on \( \bar{b} \) up to isomorphism.

Proof: Suppose \( b_2 = gb_1 \sigma(g)^{-1} \), then \( \nu_2 = g\nu_1 g^{-1} \), and the descent equations are

\[
(b_1\sigma)^2 = s\nu_1(p)\sigma^s, \quad (b_1\sigma)^{s+1} = g s\nu_1(p)g^{-1}\sigma^s.
\]

Comparing these two, \( g \) commutes with \( \sigma^s \), so \( g \in G(K_0 \cap \mathbb{Q}_p^s) \). \( \square \)
Prop. (14.7.1.12). Let $b \in G(K_0)$, then the following functor on the category of $\mathbb{Q}_p$-algebras is representable by a smooth affine group scheme:

$$J(R) = \{g \in G(R \otimes \mathbb{Q}_p, K_0)| g(b \sigma) = (b \sigma)g\}.$$ 

Moreover, if $b \in G(W(L)[\frac{1}{p}])$ where $L'$ is an alg.closed subfield of $L$, and $J'$ be the corresponding functor defined with $L'$, then the canonical morphism $J' \to J$ is an isomorphism.

Proof: Choose an embedding $G \subset GL(V, \mathbb{Q}_p)$, consider the functor:

$$F(R) = \{g \in \text{End}(V_{K_0}) \otimes R | g = b \sigma(g)b^{-1}\},$$

then it is representable by an affine space by the lemma (14.7.1.13) applied to the $\sigma$-linear map $g \mapsto b \sigma(g)b^{-1}$.

More precisely, there is a f.d. $\mathbb{Q}_p$-vector space $W \subset \text{End}(V_{K_0})$ that $F(R) = W \otimes \mathbb{Q}_p R$. Choose a basis $A_i$ of $W$, then $J(R)$ is just the subfunctor of $r_i \in R$ that $f_i(\sum r_i A_i) = 0$, and $\det(\sum r_i A_i) \neq 0$. Taking a basis of $K_0$ over $\mathbb{Q}_p$, then these are polynomials with coefficients in $\mathbb{Q}_p$. It is automatically smooth by Cartier’s theorem (7.1.4.2).

The last assertion follows from the proof of (14.7.1.13). □

Lemma (14.7.1.13). Let $N$ be a f.d. isocrystal over $K_0 = W(L)[\frac{1}{p}]$ w.r.t. $\sigma^s$ for some $s \neq 0$, then the following functor on the category of $\mathbb{Q}_p$-algebras

$$F(R) = \{n \in N \otimes \mathbb{Q}_p R | \varphi(n) = n\}$$

is representable by an affine space over $\mathbb{Q}_p$.

Proof: $F(R)$ is just $N^s \otimes \mathbb{Q}_p R$, so it suffices to show $\dim_{\mathbb{Q}_p} N^s < \infty$. Firstly assume that $L$ is alg.closed, then this is a consequence of Dieudonné-Manin classification (14.2.3.10). This functor $F$ doesn’t depend on $L$ once $L$ reaches its alg.closure: if $L$ is alg.closed and $L'$ is a field extension, then the corresponding functor $F'$ defined by $N \otimes W(L)[\frac{1}{p}]/W(L')[\frac{1}{p}]$ coincide with $F$. (This is also by Dieudonné-Manin classification.) □

Cor. (14.7.1.14). Assume $b$ satisfies a descent condition for $s(14.7.1.8)$, then $J$ is a $G_{\text{st}(p)}/\mathbb{Q}_p$-inner form of the centralizer $G_{\text{st}(p)}(14.7.1.10)$.

Proof: The descent equation shows $b_s = s\nu(p)$, so the adjoint $b_{ad} : g \mapsto (b \sigma)g(b \sigma)^{-1} = b \sigma(g)b^{-1}$ defines an element in $H^1(G(\mathbb{Q}_p)/\mathbb{Q}_p, \text{Aut}(G_{\text{st}(p)}(\mathbb{Q}_p^s)))$, because

$$\sigma^k b_{ad} : g \mapsto \sigma((b \sigma)^{-1}(g)b^{-1})) = \sigma^k(b)\sigma(g)\sigma^k(b)^{-1}.$$ 

so

$$b_{ad} \circ \sigma(b_{ad}) \circ \ldots \circ \sigma^{-1}(b_{ad}) : g \mapsto b_s g b_s^{-1} = s\nu(p)g(s\nu(p))^{-1} = g.$$ 

So it defines an inner form, which is just

$$J'(R) = G_{\text{st}(p)}(\mathbb{Q}_p^s)^{b_{ad}^\sigma} = \{g \in G_{\text{st}(p)}(R \otimes \mathbb{Q}_p \mathbb{Q}_p) | g(b \sigma) = (b \sigma)g\}$$

Now it suffices to show $J'(R)$ is just $J(R)$ defined in (14.7.1.12). For this, notice any $g \in J(R)$ commutes with $b \sigma$ thus commutes with $s\nu(p)$ by (14.7.1.7), and the descent condition $(b \sigma)^n = s\nu(p)\sigma^n$ shows it commutes with $\sigma^n$, so $g \in J'(R)$. □
Prop. (14.7.1.15). Let $G$ be a connected reductive group and $L$ be alg.closed, then the following are equivalent for $b \in G(K_0)$:

- The slope morphism $\nu$ factors through the center of $G$.
- $b$ is $\sigma$-conjugate to an element in $T(K_0)$ where $T$ is an elliptic maximal torus of $G$.
- The algebraic group $J$ of (14.7.1.12) is an inner form on $G$.

In this case, $b$ and its conjugacy class $\overline{b}$ are called basic.

Proof: Cf. [Kottwitz]. □

Prop. (14.7.1.16) [Conjugacy Classes and Base Change]. Let $b_1, b_2$ be two elements of $G(W(L)[\frac{1}{p}])$, then the functor

$$J(R) = \{g \in G(R \otimes_{Q_p} W(L)[\frac{1}{p}]) \mid g(b_1 \sigma) = (b_2 \sigma)g\}$$

is representable by a smooth affine scheme over $Q_p$.

Assume $b_1, b_2 \in G(W(L')[\frac{1}{p}])$ where $L'$ is an alg.closed field of $L$, and $J'$ the corresponding functor, then $J' \to J$ is an isomorphism. In particular, the map from the set of $\sigma$-conjugacy classes in $G(W(L')[\frac{1}{p}])$ to the set of $\sigma$-conjugacy classes in $G(W(L)[\frac{1}{p}])$ is injective, and it is surjective iff $L$ is also alg.closed and $G$ is connected.

Proof: The surjectivity follows from the fact that every conjugacy class is descent (14.7.1.9), and those descent elements are in $G(Q_s)$ for some $s \geq 0(14.7.1.10)$, so in $G(W(L')[\frac{1}{p}])$. □

2 Period Domain

Def. (14.7.2.1) [Associated Partial Flag Variety]. Let $G$ be an algebraic group over $Q_p$ and $\mu : G_m \to G$ is a conjugacy class of cocharacters defined over a finite extension field $E/Q_p(15.3.2.5)$, then there is associated a faithful $\otimes$-functor

$$\text{Rep}_{Q_p} \to \mathbb{Z} \text{-graded } R \text{-vector spaces} \to \text{filtered } E\text{-spaces}$$

Now call two cocharacters equivalent if their associated functor are isomorphic. Consider the functor

$$R \mapsto \{\text{the equivalence classes in the conjugacy class of } \mu_R \text{ under } G(R)\}$$

in the category of $E$-algebras, and also consider the closed algebraic subgroup $P(\mu) \subset G$ over $E$:

$$P(\mu)(R) = \{g \in G(R) \mid g\mu_R g^{-1} \text{ is equivalent to } \mu_R\}$$

then the functor above is representable by the homogenous variety $\mathcal{F} = G_E/P(\mu)$ defined over $E$.

Prop. (14.7.2.2). $\mathcal{F}$ is a projective variety.

Proof: If $V$ is a faithful representation in $\text{Rep}_{Q_p}(G)$, we denote $\text{Flag}(V)$ the partial flag variety over $Q_p$ which associates to any $Q_p$-algebra $R$ the filtration $\text{Fil}^i$ of $V \otimes_{Q_p} R$ s.t. $\text{gr}^i(R)$ are direct summands and rank $\text{Fil}^i = \dim_E \text{Fil}^i(\text{Fil}^i(\text{Fil}^{i-1}(V_E))$. Then $\text{Flag}(V)$ is a projective variety, by classical results, and there is a closed immersion

$$\mathcal{F} \hookrightarrow \text{Flag}(V)_E$$

because the isocrystal on other representations are determined by this faithful representation. □
14.7. RAPOPORT-ZINK SPACES

**Def. (14.7.2.3) [p-adic Period Space]**. Let \( \hat{E} = E K_0(F_p)^\wedge \) be the completion of the maximal unramified extension of \(E\), then there is a rigid-analytic structure on \( \hat{E} = \mathcal{F}_E\). Define the **p-adic period space** \( (\hat{F}_b^{wa})^{rig} \subset \hat{F}^{rig} \) associated to \((G,b\{\mu\})\) the set of points \(\xi\) conjugate to \(\mu\) that \((\xi, b)\) is weakly admissible.

Let \( J_b \) be the algebraic group associated to \(b\) as in\((14.7.1.12)\), then \(J_b(Q_p) \subset G(K_0)\) acts on \(\hat{F}^{rig}\), and it preserves the set \((\hat{F}_b^{wa})^{rig}\).

\((\hat{F}_b^{wa})^{rig}\) has a natural structure of an admissible open subset of \(\hat{F}^{rig}\). if \(b' = gb\sigma(g)^{-1}\), then \(\mu \mapsto g^{-1}\mu g\) induces an isomorphism from \((\hat{F}_b^{wa})^{rig}\) to \((\hat{F}_{b'}^{wa})^{rig}\). Moreover, if \(b\) satisfies descent condition w.r.t. \(s > 0\), then this admissible open subset is defined over \(E.Q_p^s\).

**Proof:** Cf.[Rapoport Zink, P26].

\[\square\]

### 3 Algebraic Groups of EL/PEL Types

**Def. (14.7.3.1) [Algebraic Groups of EL/PEL Types]**. Let \(F\) be a finite étale algebra over \(Q_p\), \(B\) a finite central algebra over \(F\), and \(V\) is a f.g. \(B\)-module.

An **algebraic group of EL type** over \(Q_p\) is an algebraic group of the form \(GL_B(V)\). They are related to the classification of \(p\)-divisible groups with an endomorphism and level structures.

Let \((-,-)\) be a non-degenerate alternating \(Q_p\)-bilinear form on \(V\) together with a formal involution \(*\) on \(B\) that

\[
(bv, w) = (v, b^*w).
\]

Let \(F_0\) be the field of elements of \(F\) fixed by \(\ast\).

An **algebraic group of PEL type** over \(Q_p\) is an algebraic group over \(Q_p\) given by

\[
G(R) = \{g \in GL_B(V \otimes_{Q_p} R) \mid \exists c \in X(G), \quad (gv, gw) = c(g)(v, w), \quad \forall v, w\}
\]

**Prop. (14.7.3.2) [Setups]**. If \(G\) is an algebraic group of EL/PEL type, \(K_0 = W(F)\cdot [\frac{1}{p}]\), \(b \in G(K_0)\), then we associate to \(b\) and the natural representation of \(G\) on \(V\) the isocrystal

\[
(N(V), \Phi) = (V \otimes_{Q_p} K_0, b(1 \otimes \sigma)).
\]

This isocrystal is equipped with an action of \(B\), and in the PEL case an alternating bilinear form

\[
\psi : N(V) \otimes N(V) \to 1(n).
\]

where \(n = v_p(c(b))\). In fact, we can find some unit \(u\) that \(c(b) = p^n u \sigma(u)^{-1}\), then the pairing is defined as

\[
\psi(v, v') = u^{-1}(v, v'),
\]

any other choices of \(u\) multiplies \(\psi\) by an element in \(Z_p^\times\).

We will fix in addition a conjugacy class of cocharacters \(\mu : G_m \to G\) defined over a field \(E\), and the associated homogenous algebraic variety \(\mathcal{F}\) defined over \(E\) of filtrations (14.7.2.1). \(\mathcal{F}\) is equipped with a \(B\)-action, as \(G \in GL_B(V)\).

Notice in the PEL case, these filtrations satisfy \(\mathcal{F}^i = (\mathcal{F}^{m-i+1})^\perp\), where \(m = c \circ \mu \in \text{Hom}(G_m, G_m) \cong \mathbb{Z}\). This is due to the fact \((kv, kw) = k^m(v, w)\) and the fact the pairing is non-degenerate.
Prop. (14.7.3.3) [Shimura Field]. Fix a conjugacy class of cocharacters $\{\mu\}$ defined over $E$ and $\mu_0 \in \{\mu\}$, its corresponding filtration $\mathcal{F}_0^\bullet$. The field $E$ in (14.7.3.2) can be described as the field of definition of the isomorphism class of $\mathcal{F}_0^\bullet$ as a $B$-invariant filtration, or equivalently as the finite extension of $\mathbb{Q}_p$ generated by the traces

$$\text{tr}(d; \text{gr}^i_{\mathcal{F}_0}(V \otimes_{\mathbb{Q}_p} \overline{\mathbb{Q}_p})), d \in B, i \in \mathbb{Z}.$$ 

And the filtration $\mathcal{F}$ is described as the functor that for any $E$-algebra $R$, $\mathcal{F}(R)$ is the set of filtrations $\mathcal{F}^\bullet$ of $V \otimes_{\mathbb{Q}_p} R$ by $R$-modules that are direct summands that

$$\text{tr}(d; \text{gr}^i_\mathcal{F}(V \otimes_{\mathbb{Q}_p} R)) = \text{tr}(d; \text{gr}^i_{\mathcal{F}_0}(V \otimes_{\mathbb{Q}_p} \overline{\mathbb{Q}_p})).$$

and moreover in the PEL case satisfies $\mathcal{F}^i = (\mathcal{F}^{m-i+1})^\perp$.

Proof: 1: The field of definition $E$ of the conjugacy class $\{\mu\}$ is determined by Tannakian duality, so it suffices to check over which field these two filtrations are isomorphic as $G$-filtrations, but $G$ is just the group fixing the $B$-module structure, so it suffices to show they are equivalent as $B$-modules, which is then determined by the traces, by (2.4.1.27).

2: It suffices to show $\mathcal{F}$ is a homogenous space under $G$. We restrict to the PEL case, the EL case is simpler. After base change from $\mathbb{Q}_p$ to $\overline{\mathbb{Q}_p}$, the data decomposes to the following types:

- $(A): B = \text{End}(W) \times \text{End}(W^\vee)$ where $W$ is a f.d. $\overline{\mathbb{Q}_p}$-vector space and $(u,v)^* = (v^t, u^t)$.

And $V = W \otimes V' \oplus W^\vee \otimes V'^\vee$ where the pairing is natural and makes the sum orthogonal.

$$G = \{(1 \otimes g, c \cdot (1 \otimes g^{-1})| g \in \text{GL}(V'), c \in X(G)\}$$

- $(C): B = \text{End}(W)$ where $W$ is a f.d. $\overline{\mathbb{Q}_p}$-vector space equipped with a symmetric bilinear form $(-,-)_W$ and $*$ is the transposition w.r.t it.

And $V = W \otimes V'$ where $V'$ is equipped with an alternating form $(-,-)_{V'}$ that $(-,-)_{V'} = (-,-)_W \otimes (-,-)_{V'}$.

$$G = \{cg| g \in \text{Sp}(V'), c \in X(G)\}$$

- $(BD)$: As in $(C)$, except that $(-,-)_W$ is skew-symmetric and $(-,-)_{V'}$ is symmetric.

$$G = \{cg| g \in \text{SO}(V'), c \in C(G)\}$$

Under this decomposition, the functor $\mathcal{F}$ in the proposition is represented by products of partial flags of $V$:

- $(A): \mathcal{F}^i = W \otimes (\mathcal{F}')^i \oplus W^\vee \otimes ((\mathcal{F}')^{m+1-i})^\perp$ and the correspondence $\mathcal{F}^\bullet \mapsto (\mathcal{F}')^\bullet$ identifies $\mathcal{F}$ with the partial flag variety of $V'$ with fixed dimensions $\dim((\mathcal{F}')^i)$.

- $(B, CD): \mathcal{F}^\bullet = W \otimes (\mathcal{F}')^\bullet$ and $\mathcal{F}$ is identified with the partial flag variety of $V'$ of fixed dimensions $\dim((\mathcal{F}')^i)$ and $((\mathcal{F}')^{m+1-i})^\perp$.

The $(A)$ case $G$ clearly acts transitively on $\mathcal{F}$, and the $(B, CD)$ case $(\mathcal{F}')^i$ is isotropic for $i \geq (m + 1)/2$, and it determines all other components, so $G$ acts transitively, by Witt’s theorem (12.3.2.3).

The reason is (2.4.3.26) and the fact representations of $B$ is semisimple, then contemplating on the pairing condition. \qed
Prop. (14.7.3.4) [Examples of PEL Type]. Let $B = D$ be the quaternion algebra over $\mathbb{Q}_p$ and $*$ be the involution, i.e.

$$D = \mathbb{Q}_p[\Pi], \quad \Pi^2 = p, \quad \Pi a = \sigma(a)\Pi$$

and

$$a^* = \sigma(a), a \in \mathbb{Q}_p^2, \quad \Pi^* = \Pi.$$ 

Let $(V, \iota)$ be a free $D$-module of rank $n$ with a non-degenerate bilinear form satisfying the conditions in (14.7.3.1). Then $G$ is a non-trivial inner form of the group $GSp_{2n}$ of symmetric similitudes:

Firstly $Q_{p^2} \otimes K_0 \cong K_0 \oplus K_0$, then $Q_{p^2}$ acts on $K_0 \oplus K_0$ by $a(x, y) = ax, \sigma(a)y$. As $V$ is a $Q_{p^2}$-vector space, there is a decomposition

$$V = V_0 \oplus V_1$$

where $Q_{p^2}$ acts on $V_i$ by $a(v) = v.\sigma^i(a)$, then $G_{K_0}$ is just $GSp_{2n,K_0}$, and $G \neq GSp_{2n}$ as the Galois action $\sigma$ on $Q_{p^2} \otimes K_0$ and $K_0 \cong K_0 \oplus K_0$ are different.

Take $b \in G(K_0)$ the element with $c(b) = p$ and the corresponding isocrystal $(N, \Phi)$ is isotypical of slope $1/2$. $N$ decomposes as $N_0 \oplus N_1$. Notice now $\Pi$ and $\Phi = b\sigma$ interchanges $N_i$, and $\Pi\Phi = \Phi\Pi$. Also $N_i$ is isotropic: For $v, w \in N_i, a \in \mathbb{Q}_p^2$,

$$a(v, w) = (av, w) = (v, \iota(\iota^i(a)v, w)) = (v, \sigma(a)w) = \sigma(a)(v, w)$$

so $(v, w) = 0$.

We can define a new non-degenerate alternating form

$$\langle -, - \rangle : N_0 \times N_0 \to K_0 : \langle v, v' \rangle = \langle v, \Pi v' \rangle$$

and also a $\sigma$-linear endomorphism of $N_0$: $\Phi_0 = \Pi^{-1} \circ \Phi|_{N_0}$. From the condition, $v_p(\det \Phi_0) = 0$, and $\Phi$ has all the slopes $0$. Also $\langle \Phi_0 v, \Phi_0 w \rangle = \sigma(\langle v, w \rangle)$, as

$$\langle \Phi_0 v, \Phi_0 w \rangle = (\Pi^{-1} \Phi v, \Phi w) = (\Pi^{-1} b\sigma v, b\sigma w) = \sigma(v, \Pi w) = \sigma(\langle v, w \rangle).$$

so this alternating form is defined over $\mathbb{Q}_p$, denoted by $(V_0, \langle -, - \rangle)$, and $\Phi_0$ corresponds to $\sigma$. Then $J_b = GSp(V_0, \langle -, - \rangle)$.

Next we consider

$$(0) = \mathcal{F}_0^2 \subset \mathcal{F}_0^1 \subset \mathcal{F}_0^0 = V \otimes \overline{\mathbb{Q}_p}$$

be a filtration where $\mathcal{F}_0^i$ be a $D$-invariant Lagrangian subspace. This corresponds to a cocharacter $\mu \to G$, and $\mathcal{F}$ is just the $Q_{p^2}$ variety of $D$-invariant Lagrangian subspaces of $V_{Q_{p^2}}$. By (14.7.3.3), the Shimura field is $Q_{p^2}$.

Let $\mathcal{F} \subset \mathcal{F}(K)$ where $K/K_0$ is a field extension, then

$$\mathcal{F} = \mathcal{F}_0 \oplus \mathcal{F}_1$$

where $\mathcal{F}_i \in N_0 \otimes_{K_0} K$, as $\mathcal{F}$ is $\Pi$-invariant. Now $\mathcal{F}_0$ is also a Lagrangian subspace of $(V_0, \langle -, - \rangle)$. $\mathcal{F}(K)$ identifies the $K$-points of the Grassmannian of Lagrangian subspaces of $(V_0, \langle -, - \rangle)$.

Cor. (14.7.3.5). Under the above identification, the subset $\mathcal{F}^{\text{iso}}(K)$ of the Grassmannian of Lagrangian spaces $\mathcal{F}$ of $(V_0 \otimes K, \langle -, - \rangle)$ is characterized by $\mathcal{F}$ satisfying the following conditions:

For all totally isotropic subspaces $W_0 \subset V_0$, we have $\dim_K \mathcal{F} \cap (W_0 \otimes K) \leq 1/2 \dim W_0$. 
Proof: It’s clear $\mu(N, \Phi, \mathcal{F}) = 0$, so weakly-admissibility is equivalent to semi-stability. The uniqueness of the HN-filtration of $\mathcal{F}$ implies its $D$-invariance, thus semi-stability is equivalent to the fact that for any subspace $P \subset N$ stable under $\Phi$ and $D$-action, we have

$$\dim_K(\mathcal{F} \cap (P \otimes_{K_0} K)) \leq v_p(\det(\Phi; P)).$$

Now $\Phi$ is isotypical with slope $1/2$, $v_p(\det(\Phi; P)) = \frac{1}{2} \dim P$, and the $D$-invariance of $P$ is equivalent to $P = P_0 \oplus P_1$ and the $\Phi$-invariance of $P$ is equivalent to the $\Phi_0$-invariance of $P_0$, i.e. $P_0$ is a $\mathbb{Q}_p$-rational subspace $W_0 \subset V_0$.

Finally we show it suffices to check for totally isotropic subspaces: Let $W'_0$ be the radical of $W_0$, then there is a non-singular alternating form on $W_0/W'_0$, then the image of $\mathcal{F}_0' \cap (P \otimes_{K_0} K)$ in this quotient is a totally isotropic space, thus has dimension $\leq \frac{1}{2} \dim(W_0/W'_0)$. then it suffices to check the condition for $W'_0$. \qed
14.8 Adic Spaces and Perfectoid Spaces (Scholze)

Main References are [Hub93], [Hub96], [Mor19], [Bha17], [Wed14], [S-W20], and [Sch12].

1 (Continuous) Valuation Spectra

Main references are [Mor19]. Notice this should be prior to the definition of adic spaces.

Def. (14.8.1.1) [Riemann-Zariski Space]. Let $K$ be a field and $A$ be a subring, the Riemann-Zariski space $RZ(K, A)$ is defined to be the set of all valuation subrings of $K$ containing $A$ that has the topology generated by

$$ U(x_1, \ldots, x_n) = \{ P \in RZ(K, A) | x_1, \ldots, x_n \in P \}. $$

$RZ(K, 0)$ is also denoted by $RZ(K)$. $RZ(K, A)$ is just isomorphic to $Spa(K, A_{ic})$, so it is spectral by (14.8.2.24).

Cor. (14.8.1.2). Clearly the specialization relations of $RZ(K, A)$ is identical to inclusion relations.

Def. (14.8.1.3) [Valuation Spectrum]. Let $A$ be a ring, the valuation spectrum $Spv(A)$ is the set of equivalent classes of valuations on $A$, topologized by the open subsets

$$ Spv(A)(\frac{f}{g}) = \{ x \in Spa(A) | |f(x)| \leq |g(x)| = 0 \}. $$

$Spv(A)$ is spectral, with sub-basis generated by $Spv(\frac{f}{g})$

There is a kernel map $ker : Spv(A) \to Spec A$ sending a valuation to its kernel(support). Then this map is continuous, and the fiber of this map over $p$ is just isomorphic to the Riemann-Zariski space $RZ(k(p))$.

Moreover, the map $ker : Spv(A) \to Spec A$ is spectral, as the kernel of $D(f)$ is $U(\frac{f}{g})$.

Specialization Relations in $Spv(A)$

Def. (14.8.1.4) [Vertical Specializations]. Let $x, y \in Spv(A)$. We say that $x$ is a vertical specialization of $y$ if $x$ is a specialization of $y$ and $p_x = p_y$.

Valuations with Support Conditions

Def. (14.8.1.5) [$Spv(A, J)$]. We define a space $Spv(A, J) \subset Spv(A)$ by

$$ Spv(A, J) = \{ x \in Spv(A) | r(x) = x \} = \{ x \in Spv(A) | c_{x}(J) = \Gamma \}. $$

with the subset topology from $Spv(A)$.

Prop. (14.8.1.6).

- $Spv(A, J)$ is a spectral space.
- A basis of quasi-compact open subsets for the topology is given by the sets $U(\frac{f_1, \ldots, f_n}{g})$ where $J \subset \sqrt{(f_1, \ldots, f_n)}$.
- The retraction $r : Spv(A) \to Spv(A, J)$ is a spectral map.

Proof: Cf. [Mor19] P52. □
Continuous Valuation Spectrum

**Def. (14.8.1.7) [Continuous Valuations].** Let $A$ be a Huber ring, then we define $\text{Cont}(A)$ as the subspace of $\text{Spv}$ consisting of continuous valuations on $A$, then

$$\text{Cont}(A) = \{ x \in \text{Spv}(A, A^{00}) | x(A^{00}) < 1 \}$$

*Proof:* Cf. [Mor19]P64.

**Cor. (14.8.1.8) [Cont$(A)$ is Spectral].** For any Huber ring $A$, $\text{Cont}(A)$ is a spectral space, with a basis of quasi-compact open subsets given by $U(f_1, \ldots, f_n)$, where $A^{00} \subset \sqrt{(f_1, \ldots, f_n)}$, or equivalently $(f_1, \ldots, f_n)$ is open.

*Proof:* This is because $\text{Cont}(A) = \text{Spv}(A, A^{00}) - \bigcup_{g \in A^{00}} U(f)$, which is an open subset of $\text{Spv}(A, A^{00})$, thus the assertion follows from (14.8.1.6) and (3.8.4.7).

2 Adic Spectrums

**Def. (14.8.2.1) [Adic Spectrums].** Let $(A, A^+)$ be a Huber ring, the adic spectrum is defined to be

$$\text{Spa}(A, A^+) = \{ x \in \text{Cont}(A) | |A^+|_x \leq 1 \}$$

For a Huber ring $A$, denote $\text{Spa} A = \text{Spa}(A, A^0)$, where $A^0$ is the ring of power-bounded elements (10.3.5.8).

The shape of these open sets is dictated by the desired properties that both $\{ x|f(x) \neq 0 \}$ and $\{ x|f(x) \leq 1 \}$ be open. These desiderata combine features of classical algebraic geometry and rigid geometry, respectively.

**Prop. (14.8.2.2).** The adic spectrum construction defines a contravariant functor from the category of Huber pairs to the category of topological spaces. And for any ring of integers $A^+$, $\text{Spa} A = \text{Spa}(A, A^0) \hookrightarrow \text{Spa}(A, A^+)$ is an immersion of spaces, by (10.3.5.13).

**Def. (14.8.2.3) [Kernel map].** Taking kernels of valuations gives a map $\text{ker} : \text{Spa}(A, A^+) \to \text{Spec} A$. This map is continuous, as the inverse image of $D(f)$ is $\text{Spa}(A, A^+)(\frac{f}{g})$. We call a subset a Zariski open subset of $\text{Spa}(A, A^+)$ iff it is open in the initial topology along $\text{ker}$.

**Def. (14.8.2.4) [Rational Subsets].** A rational subset of $\text{Spa}(A, A^+)$ is defined to be

$$\text{Spa}(A, A^+)(\frac{f_1, \ldots, f_n}{g}) = \{ x \in \text{Spa}(A, A^+) | x(f_i) \leq x(g) \},$$

where $(f_i)$ is an open ideal.

**Prop. (14.8.2.5) [Adic Spectrums are Spectral].** The adic spectrum $\text{Spa}(A, A^+)$ is spectral, and a basis of quasi-compact open subsets are given by rational subsets. And the Spa functor is naturally a functor from the category of Huber rings to the category of spectral spaces.
Proof: Firstly Spa\((A, A^+)\) is closed in the constructible topology of \(\text{Cont}(A)\): for any \(a \in A\),

\[
\{x \in \text{Cont}(A) \mid |a|_x \leq 1\} = U(\frac{1}{1}, \frac{a}{1})
\]

is a quasi-compact open subset of \(\text{Cont}(A)\), so constructible, thus \(\text{Spa}(A, A^+) = \cap_{a \in A^+} \{x \in \text{Cont}(A) \mid |a|_x \leq 1\}\) is closed in the constructible topology.

So the assertions follow from (3.8.4.7) and (14.8.1.8). \(\Box\)

Remark (14.8.2.6). In spite of the proposition that adic spaces are spectral, it is very different from classical algebraic geometry. For example, the generalizations of a point \(y\) is totally ordered (localization of the valuation ring), but this nearly never happen for an affine variety.

Remark (14.8.2.7). The rational subsets forms a basis for the topology of \(\text{Spa}(A, A^+)\). But in general \(\text{Spa}(\frac{\mathbb{Z}}{\mathfrak{p}})\) is not quasi-compact, in particular, \(\ker: \text{Spa}(A, A^+) \to \text{Spec} A\) is not quasi-compact.

Def. (14.8.2.8) [Specialization Map]. The specialization map

\[\text{Sp}: \text{Spa}(A, A^+) \to \text{Spec}(A^+/A^{00})\]

that maps a point \(x\) to the inverse image of the maximal ideal of \(R_x\) along the valuation map \(A^+ \to R_x\) it corresponds. It clearly lies in \(\text{Spec}(A^+/A^{00})\) as any pseudo-uniformizer is mapped to a pseudo-uniformizer in \(R_x\) thus in the maximal ideal.

This map is continuous and spectral, unlike that the kernel map (14.8.2.23): the inverse image of a \(D(f)\) for \(f \in A^+\) is the set of points \(x \in \text{Spa}(A, A^+)\) that \(x(f)\) is a unit, i.e. \(|x(f)| = 1\). As \(|x(f)| \leq 1\) for all \(f \in A^+,\) this set is just \(\text{Spa}(A, A^+)\left(\frac{1}{f}\right)\), so specialization map \(\text{sp}\) is both continuous and spectral.

Completed Residue Fields

Def. (14.8.2.9) [Completed Residue Fields]. Let \(x \in \text{Spa}(A, A^+)\), then we denote by \(k(x)\) the fraction field of \(A/p_{x}\), with a valuation ring \(k^+(x)\). If \(x\) is not analytic, we set \(\kappa(x) = k(x), k^+(x) = k^+(x)\). If \(x\) is analytic, we set \(\kappa(x) = k(x)^\wedge, k^+(x) = k^+(x)^\wedge\). \((\kappa(x), k(x)^+)\) is called the completed residue field of \(x\).

Prop. (14.8.2.10) [Vertical Generalizations]. The morphism

\[\text{Spa}(\kappa(x), k(x)^+) \to \text{Spa}(A, A^+)\]

induces a homeomorphism onto the set of vertical generalizations of \(x\).

\(x\) is analytic iff \(\kappa(x)\) is microbial.

Proof: For the first assertion, if \(x\) is not analytic, then \(\text{Spa}(k(x), k(x)^+) \cong RZ(k(x), k(x)^+)\) is homeomorphic to the vertical generalizations of \(x\).

If \(x\) is analytic, then by (14.8.2.17), \(\text{Spa}(\kappa(x), k(x)^+) \to \text{Spa}(k(x), k(x)^+)\) is a homeomorphism. And now we need to check more that if \(R \in RZ(k(x), k(x)^+)\) corresponds to a vertical generalization \(y\), then \(|\cdot|_R\) is continuous iff \(|\cdot|_y\) is continuous. For this, see [Mor19] 107.

The second assertion follows from (10.3.6.7). \(\Box\)

Prop. (14.8.2.11) [Residue of Rational Subsets]. Let \(f: (A, A^+) \to (A(\mathbb{Z}), A(\mathbb{Z})^+)\) be a rational subset, and \(y \in \text{Spa}(A(\mathbb{Z}), A(\mathbb{Z})^+)\) with \(x = \text{Spa}(f)(y)\), then the canonical map \((k(x), k(x)^+) \to (k(y), k(y)^+)\) induces an isomorphism of Huber pairs \((\kappa(x), k(x)^+) \cong (\kappa(y), k(y)^+)\) after completion.

Def. (14.8.2.12) [Adic Points]. An adic point is Spa$(K, K^+)$ where $(K, K^+)$ is a Huber pair that $K$ is either a complete non-Archimedean field or a discrete field, and $K^+$ is an open and bounded valuation subring (hence integrally closed). An analytic adic point is one that $K$ is complete non-Archimedean.

Prop. (14.8.2.13). The adic point is not a point in general. In fact, if $K$ is non-Archimedean, Spa$(K, K^+)$ is totally ordered by inclusion\(^?\), with a unique closed point corresponding to $K^+$ and a unique generic point corresponding to $O_K$.

Prop. (14.8.2.14) [Valuation Ring Characterization of Spa]. For a Huber pair $(A, A^+)$, there is a natural bijection between Spa$(A, A^+)$ and the set of maps $\varphi : (A, A^+) \to (K, K^+)$ that Spa$(K, K^+)$ is an adic point where $K_x = \kappa(x)$ and $x$ corresponds to the image of the closed point of Spa$(K, K^+)$ under the map Spa$(\varphi)$. And $x$ is analytic iff the corresponding adic point Spa$(K, K^+)$ is analytic.

Proof: Let $\varphi : (A, A^+) \to (K, K^+)$ be a map of Huber pairs, then correspond the maps gives a continuous valuation on $A$ which is in Spa$(A, A^+)$ and $p_x = \ker(\varphi)$. Notice $x$ is the image of the closed point of Spa$(K, K^+)$. And we get a map $k(x) \to K$ such that $k(x)^+ = k(x) \cap K^+$, and that has dense image by assumption, so after completion (when non-Archimedean) induces an isomorphism $(\kappa(x), \kappa(x)^+) \cong (K, K^+)$. Thus this is a bijection of sets. 

Prop. (14.8.2.15) [Uniformity]. If $A$ is uniform, then the map

$$A \to \prod_{x \in \text{Spa}(A, A^+)} \kappa(x)$$

is a homeomorphism of $A$ onto its image, where $\kappa(x)$ is the completed residue field(14.8.2.9).

Proof: Berkovich, Étale cohomology for non-Archimedean analytic spaces. \(^?\)

Cor. (14.8.2.16). Let $\hat{O}_X$ be the sheafification of $O_X$, then if $A$ is uniform, $A \to H^0(X, \hat{O}_X)$ is injective.

Proof: In fact, $A \to H^0(X, \hat{O}_X) \to \prod_x \kappa(x)$ is injective. 

Properties of Adic Spectrums

Prop. (14.8.2.17) [Properties of Adic Spectrums].

- The completion map $(A, A^+) \to (\hat{A}, \hat{A}^+)$ induces a homeomorphism on the adic spectrums that preserves rational subsets.
- Spa$(A, A^+)$ vanishes iff its completion $\hat{A}$ vanishes.
- (Adic Nullstellensatz)$A^+ = \{f \in A | x(f) \leq 1, \forall x \in \text{Spa}(A, A^+)\}$. 
- If $A$ is complete, then $f \in A$ is a unit iff $|f|_x \neq 0$ for all $x \in \text{Spa}(A, A^+)$. 
- If $A$ is Tate, then $f$ is topologically nilpotent iff $|f|_x^n \to 0$ for any $x \in \text{Spa}(A, A^+)$. 

Proof: 1: Use the valuation ring characterization(14.8.2.14), a point of $x$ determined a continuous map $(A, A^+) \to (K, K^+)$. Now this extends to a map under completion, thus determines a point of Spa$(\hat{A}, \hat{A}^+)$, so the Spa map is surjective. And injectivity follows from the fact $A$ is dense in $\hat{A}$. 

□
For the homeomorphism, just notice that if \( f_i - f'_i, g - g' \in t^{N+1} \tilde{A} \), then
\[
\text{Spa}(f_1, \ldots, f_n) = \text{Spa}(f'_1, \ldots, f'_n),
\]
where \( f_n = t^N \). So now \( A \) is dense in \( \tilde{A} \), if we choose \( f_i, g \in A \), then this rational subset is clearly induced from \( A \).

2: Cf. [Mor19] P104.
3: Cf. [Mor19] P91.
4: Cf. [Mor19] P106.
5: Cf. [Mor19] P106.

\[\Box\]

Cor. (14.8.2.18) [Generalizations in Adic Spectrum]. The above proposition shows that the generalization relations of Spa are easily determined, for an element \( y \), all generalizations of \( y \) are in bijection with \( \text{Spec}(R_y/(t)) \) as a poset, thus totally ordered, and each \( y \) has a unique generic point as generalization, because it is microbial.

Moreover, \( \text{Spa}(A, A^0) \) is closed under generalization in \( \text{Spa}(A, A^+) \), and they have the same set of generic points.

Proof: The last assertion is because the generalizations of a point \( y \) is just valuation rings containing \( R_y \), and \( R_y \) contains \( A^0/p_y \), so does its generalizations. And for any generic point \( x \in \text{Spa}(A, A^+) \), \( A^0 \) is mapped to the valuation ring \( R_x \), because it is a rank 1 valuation, so if \( t^k f^N \subset R_x \), then \( f \in R_x \) because otherwise we have \( |t| < |f^{-n}| \) for \( n \) large.

Def. (14.8.2.19) [Specialization Map]. The specialization map
\[
\text{Sp}: \text{Spa}(A, A^+) \to \text{Spec}(A^+/A^{00})
\]
that maps a point \( x \) to the inverse image of the maximal ideal of \( R_x \) along the valuation map \( A^+ \to R_x \) it corresponds. It clearly lies in \( \text{Spec}(A^+/A^{00}) \) as any pseudo-uniformizer is mapped to a pseudo-uniformizer in \( R_x \) thus in the maximal ideal.

This map is continuous and spectral, unlike that the kernel map (14.8.2.23): the inverse image of a \( D(f) \) for \( f \in A^+ \) is the set of points \( x \in \text{Spa}(A, A^+) \) that \( x(f) \) is a unit, i.e. \( |x(f)| = 1 \). As \( |x(f)| \leq 1 \) for all \( f \in A^+ \), this set is just \( \text{Spa}(A, A^+) \{f\} \), so specialization map \( sp \) is both continuous and spectral.

Prop. (14.8.2.20) [Maximal Hausdorff Quotient]. Let \( X = \text{Spa}(A, A^+) \) be an affinoid Tate space, the if \( X \) is the quotient of \( X \) by the equivalence relation generated by specialization, then \( X \) is the Hausdorffification of \( X \), i.e. \( X \) is Hausdorff.

Proof: To show \( X \) is Hausdorff, if \( x, y \in X \) is not mapped to the same point in \( X \), then by (14.8.2.18), we may assume \( x, y \) is generic in \( X \), and \( \{x\} \cap \{y\} = \emptyset \). Now we must find two disjoint open subsets of \( x, y \) that is stable under specialization. Cf. [Bhatt Perfectoid Spaces P75].

Spectrality of Adic Spectrums

Def. (14.8.2.21) [Rational Subsets]. A rational subset of \( \text{Spa}(A, A^+) \) is defined to be
\[
\text{Spa}(A, A^+)(f_1, \ldots, f_n) = \{ x \in \text{Spa}(A, A^+) | x(f_i) \leq x(g) \},
\]
where \( (f_i) = (1) \).
Prop. (14.8.2.22). Rational subsets are stable under intersection (Easy).

Prop. (14.8.2.23). The rational subsets forms a subbasis for the topology of Spa($A, A^+$). But in generally Spa($\frac{f}{g}$) is not quasi-compact, in particular, Spv($A$) → Spa($A, A^+$) is not quasi-compact (proper).

Prop. (14.8.2.24)[Adic Spectrums are Spectral]. The adic spectrum Spa($A, A^+$) is spectral, and a basis of quasi-compact open subsets are given by rational subsets. And the Spa functor is naturally a functor from the category of Huber rings to the category of spectral spaces.

Proof: Firstly Spa($A, A^+$) is closed in the constructible topology of Cont($A$): for any $a \in A$,

$$\{x \in \text{Cont}(A) || a|_x \leq 1\} = U(\frac{1}{t}a^{1})$$

is a quasi-compact open subset of Cont($A$), so constructible, thus

$$\text{Spa}(A, A^+) = \cap_{a \in A^+} \{x \in \text{Cont}(A) || a|_x \leq 1\}$$

is closed in the constructible topology.

So the assertions follow from (3.8.4.7) and (14.8.1.8). □

Remark (14.8.2.25). In spite of the proposition that adic spaces are spectral, it is very different from classical algebraic geometry. For example, the generalizations of a point $y$ is totally ordered (localization of the valuation ring), but this nearly never happen for an affine variety.

Cor. (14.8.2.26)[Detecting Nilpotence Locally]. If ($A, A^+$) is an affinoid Tate ring and $f \in A$, then $f \in A^{00}$ iff $|f(x)|^n \to 0$ for all $x$.

Proof: If $f$ is topological nilpotent, then $f^N \in tA^+$ for some $n$, so $|f(x)|^n \leq |t(x)|^n \to 0$ because $x$ is continuous. Conversely, if $|f(x)|^n \to 0$ for all $x$, then $X = \cup_{n} X(\frac{f}{t^n})$. But $X$ is quasi-compact, so $|f(x)|^n \leq |t(x)|$ for all $x$, for some $n$. So by (14.8.2.17) $f^n \in tA^+$. Now $A^+$ is a filtered colimits of rings of definitions (10.3.5.14), so $f^n \in tA_0$ for some $tA_0$, which shows that $f \in A^{00}$. □

Constructions of Adic Spectrums

Prop. (14.8.2.27)[Direct Limits of Uniform Affinoids]. The direct limits exists in the category of uniform affinoid Tate rings. and $A^+ = \text{colim} \ A^+_i$.

Moreover,

$$|\text{Spa}(A, A^+)| \cong \lim_{\to i} |\text{Spa}(A_i, A_i^+)|$$

as a homeomorphism of spectral spaces, and each rational subset of Spa($A, A^+$) is pulled back from some rational subset of Spa($A_i, A_i^+$).

The same conclusion also hold in the category of complete uniform affinoid Tate rings (For the homeomorphism, (14.8.2.17) is used).

Proof: Suppose the colimit index has a minimal element $i_0$, let $t$ be a pseudo-uniformizer, then each $A_i^+$ is a ring of definition with pseudo-uniformizer $t$. Now we set $A = \text{colim} \ A_i$ with ring of definitions $A^+ = \text{colim} \ A_i^+$, then $A^+$ is integrally closed in $A$, thus ($A, A^+$) is truly a uniform affinoid Tate ring. Now we check it is the colimit: For any compatible map ($A_i, A_i^+$) → ($B, B^+$), there is a
map \( f : (A, A^+) \to (B, B^+) \) as abstract rings. We check it is continuous: we may assume \( B^+ \) is the ring of definition, then \( t^n A^+ \subset f^{-1}(t^n B^+) \), thus it is continuous.

For the adic spectrum, now a point \( x \in \text{Spa}(A, A^+) \) is determined by the map of uniform affinoid Tate rings \( (A, A^+) \to (k(p), R_x) \), and by the universal property, it is defined by a compatible set of maps \( (A_i, A_i^+) \to (k(p), R_x) \). Now it is easy to see the desired bijection of topological spaces, as the elements defining rational subsets are pullbacks from some \( A_i \).

\[ \square \]

Prop. (14.8.2.28) [Perfection of Adic Spectrum]. Let \( (A, A^+) \) be an affinoid Tate ring of charp, then

- The Frobenius map induces a homeomorphism on the adic spectrum of \( (A, A^+) \).
- If \( (A, A^+) \) is uniform, then there is a perfection functor, which is left adjoint to the forgetful functor from the category of perfect uniform affinoid Tate rings to the category of affinoid Tate rings. And it is just \( (A_{\text{perf}}, A_{\text{perf}}^+) \).
- The natural map \( (A, A^+) \to (A_{\text{perf}}, A_{\text{perf}}^+) \) induces a homeomorphism on the adic spectrum.

\[ \text{Proof:} \]

1: The Frobenius pulls a valuation a multiple of itself, thus equals itself.
2: Clearly \( A_{\text{perf}}^+ \) is integrally closed in \( A^+ \) and is in \( A_{\text{perf}}^0 \). It suffices to show \( (A_{\text{perf}}, A_{\text{perf}}^+) \) is uniform, but this is because \( A_{\text{perf}}^0 = (A_{\text{perf}})^0 \subset (t^{-n} A_0)_{\text{perf}} = t^{-n} (A_0)_{\text{perf}} \).
3: The Spa map is checked to be continuous and injective, for the converse, using the microbial valuation ring characterization, a point \( x \) of \( \text{Spa}(A, A^+) \) corresponds to a map \( A^+ \to \text{complete field } k^+(x) \), thus a map \( A_{\text{perf}}^+ \to k^+(x)_{\text{perf}} \), now \( k^+(x) \to k^+(x)_{\text{perf}} \) is faithfully flat that preserves pseudo-uniformizers, thus it is a point \( y \) that maps to \( y \).

\[ \square \]

3 Structure Presheaf and Adic Spaces

Lemma (14.8.3.1) [Functions on Rational Subsets]. If \( X = \text{Spa}(A, A^+) \) is a Huber ring, and \( U \) is a rational subset, then there is a unique complete affinoid Tate ring \( (\mathcal{O}_X(U), \mathcal{O}_X^+(U)) \) over \( (A, A^+) \) that the the Spa map

\[ \text{Spa}(\mathcal{O}_X(U), \mathcal{O}_X^+(U)) \to \text{Spa}(A, A^+) \]

is universal in all the complete affinoid Tate algebras that has image in \( U \).

And in this case, this Spa map is a homeomorphism identifying the rational subsets contained in \( U \) to rational subsets of \( \text{Spa}(\mathcal{O}_X(U), \mathcal{O}_X^+(U)) \). In particular, \( U \) is quasi-compact.

\[ \text{Proof:} \]

See Hub94 P1.3 for the proof in the Huber ring case.

Choose a ring of definition \( (A_0, t) \), and \( U = \text{Spa}(A, A^+) \frac{1}{g} f_i, g \in A_0 \), and \( f_n = t^n \), and let \( B = A[g^{-1}] \) and \( B_0 = A_0 \frac{1}{y} \). Then \( B = B_0[t^{-1}] \) (notice that \( A_0[t^{-1}] = A \)). So \( B \) is a Tate \( A \)-algebra with \( \text{ring of definition} (B_0, t) \). Now if \( B^+ \) is the integral closure of the subring \( B \) generated by \( A^+ \frac{1}{g} \), then \( (B, B^+) \) is an affinoid Tate ring. Set \( (\mathcal{O}_X(U), \mathcal{O}_X^+(U)) \) to be its completion.

By construction \( \text{Spa}(\mathcal{O}_X(U), \mathcal{O}_X^+(U)) \) maps into \( U \), because \( x(g) \neq 0 \) because \( g \) is a unit, and \( |x(f_i)| \leq |x(g)| \) as \( f_i/g \in B^+ \).

Now check universal property: if \( \text{Spa}(C, C^+) \) maps into \( U \), then \( g \) is a unit in \( C \) by (14.8.2.17), and then \( f_i/g \in C^+ \) by (14.8.2.17) again. Now \( C_0 \) is the filtered colimit of all rings of definition, so there is a ring of definition \( C_0 \) that contains \( A_0 \) and all \( f_i/g \) (10.3.5.17) is used). Then this gives a map of affinoid Tate rings that maps \( B_0 \) into \( C_0 \), and when passed to completion, induces a map
$\mathcal{O}_X(U) \to C$ of Tate algebras. Now also $B^+$ is mapped into $C^+$ because $C^+$ is integrally closed, so we are done.

For the last assertion, by (14.8.2.17), we only have to prove $\text{Spa}(B, B^+) \to U$ is a homeomorphism preserving rational subsets, for this, the injectivity is clear as $B$ is a localization of $A$. And the surjectivity follows immediately from the valuation ring characterization and universal property. Continuity is also clear.

For the openness, for any rational subset $X(\frac{f}{g})$ of $X = \text{Spa}(B, B^+)$, because $B = A[\varepsilon^{-1}]$, $g$ is a unit in $B$, we can assume that $f, g \in A_0$. Now we show $U \cap \text{Spa}(A, A^+)(\frac{f}{g})$ is rational, for this, it suffices to add a $t^N$ to $f$, and this is possible, as $X(\frac{f}{g})$ is quasi-compact by (14.8.2.24). (This is in fact similar to the proof that continuous bijection from compact to Hausdorff is homeomorphism). □

**Remark (14.8.3.2).** The proof goes through with complete replaced by Zariski or Henselian, because we only use item 5 of (14.8.2.17), which is true for all Zariski pairs.

And by looking at the construction, if a rational subset $U$ has a representation $X(\frac{f}{g})$, then $f_i \in \mathcal{O}_X(U)$, and $g$ is invertible in $\mathcal{O}_X(U)$.

**Stalks**

**Def. (14.8.3.3) [Stalks].** The stalks of an affinoid adic space is defined as in the case of schemes, i.e. the colimit of the function ring of rational subsets containing $x$, without topology, and similarly for the integral stalk. Notice that the function rings are defined by universal property w.r.t to complete Huber pairs, so the stalks only depend on the completion of $(A, A^+)$. 

**Lemma (14.8.3.4).** Let $U$ be an open subset of $X = \text{Spa}(A, A^+)$ and $f, g \in \mathcal{O}_X(U)$, then $V = \{x \in U \mid |f|_x \leq |g|_x \neq 0\}$ is an open subset of $X$.

**Proof:** Cf. Morel P116. □

**Prop. (14.8.3.5) [Valuations on the Stalks].** Let $X = \text{Spa}(A, A^+)$ be an affinoid adic ring, and $x \in X$, then:

- There is a valuation $x$ on $\mathcal{O}_{X,x}$ extending that on $A$, and $\mathcal{O}_{X,x}^+ = \{f \in \mathcal{O}_{X,x} \mid |f(x)| \leq 1\}$.

- $\mathcal{O}_{X,x}$ is local with maximal ideal $m_x = \ker x$, and $\mathcal{O}_{X,x}^+$ is local with maximal ideal $\{f \in \mathcal{O}_{X,x} \mid |f(x)| < 1\}$.

- If $k(x)$ is the residue field of $\mathcal{O}_{X,x}$ and $k(x)^+$ be the image of $\mathcal{O}_{X,x}^+$ in $k(x)$, then $k^+(x)$ is naturally a valuation ring, and $(k, k^+)$ is an affinoid field over $(A, A^+)$. In particular, there is an isomorphism between the residue fields of $\mathcal{O}_{X,x}^+$ and $k^+(x)$.

- If $\varphi : (A, A^+) \to (B, B^+)$ is a morphism of Huber pairs and $y \in \text{Spa}(B, B^+)$ is a point that $\text{Spa}(\varphi)(y) = x$, then the morphism of rings $\varphi_x : \mathcal{O}_{X,x} \to \mathcal{O}_{Y,y}$ induced by $\text{Spa}(\varphi)$ is such that $|\cdot|_x = \varphi(x) |\cdot|_y$. In particular, $\text{Spa}(\varphi)_x$ is a morphism of local rings. Also it sends $\mathcal{O}_{X,x}^+$ to $\mathcal{O}_{Y,y}^+$ and this is a morphism of local rings.

If moreover $A$ is Tate, then we have:

- The ring $\mathcal{O}_{X,x}^+$ is $t$-adically Henselian, and $\mathcal{O}_{X,x}^+ \to k^+(x)$ induces an isomorphism after $t$-adic completion.

- The pairs $(\mathcal{O}_{X,x}^+, m_x)$ and $(\mathcal{O}_{X,x}, m_x)$ are Henselian.
14.8. ADIC SPACES AND PERFECTOID SPACES (SCHOLZE) 1389


1: Consider the $t$-adic completion of the valuation ring $R_x$ corresponding to $x$, then $(\tilde{k}(p_x), \tilde{R}_x)$ is an affinoid Tate ring over $(A, A^+)$ that is mapped to $x$(and its generalizations), thus by universal property, there are unique maps from every rational subsets containing $x$ to $(\tilde{k}_x, \tilde{R}_x)$, thus inducing a map $(\mathcal{O}_{X,x}, \mathcal{O}_{X,x}^+) \to (\tilde{k}_x, \tilde{R}_x)$, which induces the desired valuation. And also we have $\mathcal{O}_{X,x}^+ \subseteq \{f \in \mathcal{O}_{X,x}\|f(x)\| \leq 1\}$, for the converse, if $|f(x)| \leq 1$, then $U(\frac{1}{t^n})$ is rational subsets in $U$ containing $x$, so by(14.8.3.2), $f \in \mathcal{O}_X(V)^+$, thus $f \in \mathcal{O}_{X,x}$. 

2: for $g$ not in $m_x$, $|g(x)| > |t(x)|^n$ for some $n$, so $g$ is invertible in $U(\frac{1}{g})$ by(14.8.3.2), hence invertible in $\mathcal{O}_{X,x}$. Similarly for $\mathcal{O}_{X,x}^+$, as $g$ is invertible in $U(\frac{1}{g})$.

3: This is clear from the construction of the valuation on $\mathcal{O}_{X,x}$ in item1.

4: 

5: As filtered colimits of Henselian pair is Henselian(4.3.10.3) and the function ring is complete, the stalk is Henselian. As for the completion, notice $m_x \subset \mathcal{O}_{X,x}$ and is $t$-divisible, thus $\mathcal{O}_{X,x}^+$ has the same $t$-adic completion as $k^+(x)$.

6: We first prove $(\mathcal{O}_{X,x}^+, t)$ is Henselian, for this, it suffices to prove $(\mathcal{O}_{X,x}^+(U), t)$ is Henselian, by(4.3.10.3). And $\mathcal{O}_{X,x}^+(U)$ is a filtered colimits of rings of definitions(10.3.5.14) and they are $t$-adically complete hence Henselian, so we are done by(4.3.10.3) again. Then so does $(\mathcal{O}_{X,x}, m_x)$ because the property of being Henselian only depends on $I(4.3.10.10)$. 

Cor. (14.8.3.6). By the construction of the valuation on the stalk, we have an inclusion of rings $k(p_x) \subset k(x) \subset \tilde{k}(x)$ that has the same completions, where the first is induced by the compatible map $A \to \mathcal{O}_X(X) \to \mathcal{O}_X(U)$. 

Def. (14.8.3.7)[Huber’s Presheaf]. Now by the universal property of function ring, we have a map between them induced by inclusion of rational subsets, so we can define the structure presheaf to be 

$$\mathcal{O}_X(W) = \lim_{U \subseteq W \text{ rational}} \mathcal{O}_X(U),$$

and similarly for the integral structure sheaf $\mathcal{O}_X^+$. Then there is a valuation of a point on $\mathcal{O}_X(W)$ by passing to the stalk, and

$$\mathcal{O}_X^+(W) = \{f \in \mathcal{O}_X(W)\|f(x)\| \leq 1, \forall x \in W\}.$$

because this is true for all rational subsets by adic nullstellensatz(14.8.2.17).

A Huber ring $(A, A^+)$ is called sheafy iff the structure sheaf $\mathcal{O}_X$ on $X = \text{Spa}(A, A^+)$ is a sheaf. In this case, $\mathcal{O}_X^+$ is also a sheaf by the above formula, so sheafyness is a property that only depends on $A$.

Criterion for Sheafyness

Def.(14.8.3.8) [Stably Uniform Huber Pair]. Let $(A, A^+)$ be a Huber pair that $A$ is analytic, then it is called stably uniform if $\mathcal{O}_X(U)$ is uniform for all rational subsets $U \subset X = \text{Spa}(A, A^+)$. 

Prop.(14.8.3.9). Let $A \to B$ be a continuous map of Huber rings which splits in the category of topological $A$-modules, then $A$ is stably uniform.

Proof: The splitting means the map is strict(10.3.1.4), so $A$ is also uniform. Also the splitting is preserved under completed tensor product with rational localization, so $A$ is stably uniform. $\Box$
Prop. (14.8.3.10) [Examples of Sheafy Huber Rings]. Let \((A, A^+)\) be a complete Huber pair, 
1. (Schemes) If \(A\) is discrete, then \(A\) is sheafy.
2. (Formal Schemes) If \(A\) has a Noetherian ring of definition, then \(A\) is sheafy.
3. (Rigid Spaces, Fargues-Fontaine Curves) If \(A\) is Tate and Strongly Noetherian (10.3.4.25), then \(A\) is sheafy.
4. (Perfectoid Spaces) \(A\) is analytic and \((A, A^+)\) is stably uniform (14.8.3.8), then \(A\) is sheafy and acyclic.

We use the arguments following (14.8.4.30).
If \(A\) is analytic and \((A, A^+)\) is stably uniform. Firstly the ideals \((f - gT), (g - fT)\) are closed in their rings, Cf.[Ked19]L1.5.26.
Then we have a diagram

\[
\begin{array}{c}
0 \\
\downarrow \\
B \langle T \rangle \oplus B \langle T^{-1} \rangle \xrightarrow{T^{-1}} B \langle T, T^{-1} \rangle \\
\downarrow \\
0 \\
0 \\
\downarrow \\
B \langle \frac{L}{g} \rangle \oplus B \langle \frac{q}{f} \rangle \\
\downarrow \\
0 \\
0 \\
\end{array}
\]

where the columns and the first two rows are exact, thus the third row are exact in the middle and right by spectral sequence. Also it is exact at the left by (14.8.2.16). \(\square\)

Remark (14.8.3.11). Notice that these contains nearly everything of interest, so Scholze comments that we can somehow pretend that non-sheafy Huber rings doesn’t appear in nature.

Remark (14.8.3.12). Stably uniform is hard to check in practice, so a recent paper of Hansen-Kedlaya [Sheafyness Criterion for Huber Rings] studied another class of sousperfectoid rings which can be splitly embedded into a perfectoid ring, and another class of diamaintine rings, which involves a condition on the cohomology of pro-étale site of \(A\), closely related to properties of diamonds.


4 Adic Spaces

Def. (14.8.4.1) [Huber category]. The category \(V^{pre}\) is a category that the objects are triples \((X, \mathcal{O}_X, v_x)\) that \(X\) is a topological space, \(\mathcal{O}_X\) is a \(\mathbb{m}_x\) \(\mathcal{O}_X\) has the structure of sheaf of complete topological rings, and \(v_x\) are continuous valuations on the stalk \(\mathcal{O}_{X,x}\) with support \(\mathbb{m}_x\).

And a morphism in \(V^{pre}\) is a pair \((f, f^\flat)\) where \(f: X \rightarrow Y\) is a map of topological spaces and \(f^\flat: \mathcal{O}_X \rightarrow f_* \mathcal{O}_Y\) is a morphism of presheaves of topological rings, and the induced morphism of \(f^\flat\) on the stalks are compatible with the valuations.

The Huber category \(V\) is the full subcategory of \(V^{pre}\) whose objects are triples \((X, \mathcal{O}_X, v_x)\) in \(V^{pre}\) that \(\mathcal{O}_X\) is a sheaf.
**Def. (14.8.4.2) [Open Immersions].** An open immersion in $V^{pre}$ is a homeomorphism onto an open subset that induces an isomorphism of presheaves.

**Def. (14.8.4.3) [Adic Spaces].** The category of affinoid adic spaces is the full subcategory of the Huber category whose objects are isomorphic to $\text{Spa}(A, A^+)$ for some Huber pair $(A, A^+)$, and the category of adic spaces is the full subcategory of Huber category whose objects are locally isomorphic to an affinoid adic space.

**Prop. (14.8.4.4) [Adic Spectrum Adjointness].** For any affinoid adic space $X = \text{Spa}(R, R^+)$ and $Y$ an arbitrary adic space, then there is a natural isomorphism

$$\text{Hom}(Y, X) \cong \text{Hom}((R, R^+), (O_Y(Y), O_Y^+(Y))).$$

**Proof:** It suffices to show for $Y = (S, S^+)$ affine, because an morphism from $Y \to X$ is glued from local morphisms, and $O_Y$ is a sheaf.

For this, Cf.Huber94 Prop2.1(2). □

**Def. (14.8.4.5) [Uniform Adic Spaces].** An adic space $X$ is called uniform if for all open affinoid $U = \text{Spa}(R, R^+)$ $\subset X$, the Huber ring $R$ is uniform.

**Cartier Divisors and Closed Immersions**

**Def. (14.8.4.6) [Cartier Divisors].** Let $X$ be a uniform analytic adic space, then a (effective) Cartier divisor on $X$ is an ideal sheaf $I \subset O_X$ that is locally free of rank 1. The support of a Cartier divisor is $\text{Supp}(O_X/I)$.

The support $Z$ of a Cartier divisor is a nowhere dense closed subset of $X$, and the map $I \mapsto I = iO_X$ induces a bijection between invertible ideals $I \subset R$ that $V(I)$ is nowhere dense in $X$ and Cartier divisors on $X$.

**Proof:** By (14.8.4.21), any Cartier divisor is of the form $I \otimes_R O_X$ for some invertible ideal $I \subset R$. We need to show that $\varphi : I \otimes_R O_X \to O_X$ is injective iff $V(I) \subset X$ is nowhere dense.

By restriction, we can assume $I = (f)$ is principle, and if $V(f)$ contains an open subset, then on an open rational subset, $f = 0$ by uniformity (14.8.2.15), so $\varphi$ is not injective. Conversely, if $V(f)$ is nowhere dense, we show $f$ is a nonzero-divisor: if $fg = 0$ and $g \neq 0$, then $U = U(f^{-1})$ is contained in $V(f)$ and is open, so $U = 0$, which implies $g = 0$ by uniformity (14.8.2.15), contradiction. □

**Prop. (14.8.4.7).** Let $X$ be a uniform analytic adic space and $I \subset O_X$ a Cartier divisor with support $Z$ and $j : U = X \setminus Z \to X$. There are injective maps of sheaves

$$O_X \hookrightarrow \lim_{n} I^{-n} \hookrightarrow j_* O_U.$$

**Proof:** This is local, it suffices to check this is for any affine subscheme of $X$, so we can assume $X = \text{Spa}(R, R^+)$ and $I = fO_X$ for some nonzero-divisor $f \in R$ whose vanishing locus $Z$ is nowhere dense, and check the global sections:

$$R \to R[\frac{1}{f}] \to \Gamma(U, O_U).$$

Then it suffices to show $R \to \Gamma(U, O_U)$ is injective. But if $g$ vanishes on $U$, then the vanishing locus of $g$ is a closed subset containing $U$, which implies that it is all of $X$ as $Z$ is nowhere dense, so $g = 0$ by uniformity (14.8.2.15). □
Def.(14.8.4.8) [Meromorphic Along the Cartier Divisor]. A function \( f \in H^0(U, \mathcal{O}_U) \) is meromorphic along the Cartier divisor \( \mathcal{I} \subset \mathcal{O}_X \) if it lifts to \( H^0(X, \varprojlim_n \mathcal{I}^{-n}) \).

Def.(14.8.4.9) [Closed Cartier Divisors]. On a uniform analytic adic space \( X \), a closed Cartier divisor is a Cartier divisor \( \mathcal{I} \subset \mathcal{O}_X \) with support \( Z \) that \( (Z, \mathcal{O}_X/\mathcal{I}, | \cdot |_x, x \in Z) \) is an adic space.

Prop.(14.8.4.10) [Closed Cartier Divisor and Closed Immersion]. On a uniform analytic adic space \( X \), a Cartier divisor \( \mathcal{I} \subset \mathcal{O}_X \) is closed iff the map \( \mathcal{I}(U) \hookrightarrow \mathcal{O}_X(U) \) has closed image for all open affinoid \( U \subset X \). In this case, for all open affinoid \( U = \text{Spa}(R, R^+) \subset X \), the intersection \( U \cap Z = \text{Spa}(S, S^+) \) is an affinoid adic space, where \( S = R/I \) and \( S^+ \) is the integral closure of the image of \( R^+ \) in \( S \).

Proof: The property of having closed image can be checked locally as affinoid subspace is quasi-compact. The fact \( \mathcal{O}_X/\mathcal{I} \) is a \( (\mathcal{O}_X/\mathcal{I})(U_i) \) is separated for an open covering \( \{U_i\} \) of \( X \), so at \( \mathcal{I}(U_i) \) is closed in \( \mathcal{O}_X(U_i) \).

Conversely, if \( \mathcal{I}(U) \hookrightarrow \mathcal{O}_X(U) \) has closed image for all open affinoid \( U \subset X \), we want to show \( (Z, \mathcal{O}_X/\mathcal{I}, | \cdot |_x, x \in Z) \) is an adic space: We can construct this locally, so if \( X = \text{Spa}(R, R^+) \), \( S = R/I \) separated and complete, thus a complete Huber ring, and consider the quotient Huber ring\((10.3.5.19) (S, S^+) \), then \( \text{Spa}(S, S^+) \hookrightarrow \text{Spa}(R, R^+) \) is a closed immersion of topological spaces with image \( V(I) \).

What’s left to show is that the map of presheaves \( \mathcal{O}_X/\mathcal{I} \to \mathcal{O}_Z \) is an isomorphism, and also \( \mathcal{O}_X/\mathcal{I}(U) = \mathcal{O}_X(U)/\mathcal{I}(U) \). To show this, we first show the presheaf \( \mathcal{O}_X/\mathcal{I} \) is a sheaf: this is by 3 × 3-lemma: \( \mathcal{I} \) is locally (f), and for a rational covering \( U_i \to X \),

\[
\mathcal{O}_X(X)/f \to \prod_i \mathcal{O}_X(U_i)/f \Rightarrow \prod_{ij} \mathcal{O}_X(U_{ij})/f
\]

is exact.

And to show \( \mathcal{O}_X/\mathcal{I} \to \mathcal{O}_Z \) is an isomorphism, it suffices to notice taking localization and taking quotient commutes, because they are both defined by universal properties.\((10.3.5.19)(10.3.5.32)\). □

Remark(14.8.4.11). Even if \( A \) is Tate and stably uniform, and \( f \in A \) is a nonzero-divisor that \( fA \subset A \) is closed, it may not be true that \( \mathcal{O} = f\mathcal{O}_X \hookrightarrow \mathcal{O}_X \) is a closed Cartier divisor on \( X = \text{Spa}(A, A^+) \). This is because there may be rational localization \( (A, A^+) \to (B, B^+) \) that \( fB \) is not closed in \( B \). Cf. \[Ked19\]P16.

Examples of Adic Spaces

Prop.(14.8.4.12) [Examples of Adic Spaces].
- (Adic Closed Unit Disk) The space \( \text{Spa}(\mathbb{Z}[T]) = \text{Spa}(\mathbb{Z}[T], \mathbb{Z}[T]) \) represents the functor \( X \mapsto \mathcal{O}_X^+(X) \).
- (Adic Affine Line) The functor \( X \mapsto \mathcal{O}_X(X) \) is also representable, by \( \text{Spa}(\mathbb{Z}[T], \mathbb{Z}) \). Notice for any non-Archimedean field \( K \),

\[
\text{Spa}(\mathbb{Z}[T], \mathbb{Z}) \times \text{Spa} K = \bigcup_{n \geq 1} \text{Spa} K(\varpi^n T) = \lim_{n,T \to \varpi T} \text{Spa} K(T).
\]

This is because for any Huber pair \((R, R^+)\) over \((K, \mathcal{O}_K)\), \( R = \bigcup_n \varpi^{-n} R^+ \) because \( \varpi \) is topologically nilpotent.
• (The Open Unit Disk) Let $D = \text{Spa} \mathbb{Z}[[T]]$, then for any non-Archimedean field $K$, $D_K = D \times \text{Spa} K$ represents the functor that maps a $K$-algebra $R$ to all its elements of norm $\leq 1$. Then this the open disk over $K$. And $D_K$ is also represented by

$$\bigcup_{n \geq 1} \text{Spa} K(T, \frac{T^n}{\omega}).$$

• (The Punctured Open Unit Disk) Let $D^* = \text{Spa} \mathbb{Z}((T))$, then

$$D^*_K = D^* \times \text{Spa} K = D_K(T) = D_K \setminus \{0\}$$

Prop. (14.8.4.13) [The Open Unit Disk over $\mathbb{Z}_p$]. Consider $X = \mathbb{Z}_p[[T]]$ with the $(p,T)$-adic topology, there is exactly one non-analytic point $x = x_{F_p}$. Let $X = \text{Spa}(\mathbb{Z}_p[[T]])$ and $Y = X \setminus \{x_{F_p}\}$, then for a point $x \in Y$, $T(x)$ and $p(x)$ cannot both be 0 by (10.3.6.2).

Then there exists a unique continuous map

$$\kappa : |Y| \to [0, \infty]$$

classified by the following property: For any rational number $m/n < r$, $|T(x)|^n > |p(x)|^m$, and for any rational number $m/n > r$, $|T(x)|^n < |p(x)|^m$. This map $\kappa$ is surjective.

Proof: Let $\tilde{x}$ be a maximal vertical generalization of $x$, then it has rank 1 and we can assume $\tilde{x}$ is real valued by (10.3.3.8). Now we define

$$\kappa(x) = \frac{\log |T(\tilde{x})|}{\log |p(\tilde{x})|}.$$ 

This is definable as $T(\tilde{x})$ and $p(\tilde{x})$ cannot both be 0.

The uniqueness of $\kappa(x)$ follows from the fact $|T(x)|^n > |p(x)|^m$ implies to $|T(\tilde{x})|^n \geq |p(\tilde{x})|^m$ because $\tilde{x}$ is a generalization of $x$.

To show $\kappa$ satisfies the condition, if $m/n < r$, then $|T(\tilde{x})|^n > |p(\tilde{x})|^m$, so $|T(x)|^n > |p(x)|^m$ because $x, \tilde{x}$ define the same topology. And it is continuous because

$$\kappa^{-1}((\infty, r)) = \bigcup_{m/n < r U} \left( \frac{T^n}{p^m} \right).$$

To show the surjectivity, if $\kappa = [x_0 : x_1]$, define the valuation as

$$v(\sum a_{ij} p^iT^j) = \sup_{a_{ij} \neq 0} e^{-x_0i-x_1j}$$

where $(a_{ij})^p = 1.$ □

Construction of Adic Spaces


Def. (14.8.4.15) [Adic Spaces attached to Schemes].

Def. (14.8.4.16) [Adic Spaces attached to Formal Schemes]. Cf. [Wed14].

Def. (14.8.4.17) [Adic Spaces attached to Rigid Analytic Spaces]. Cf. [Wed14].
Sheaves and Vector Bundles

**Def. (14.8.4.18).** Let \((A, A^+)\) be a Huber pair and \(X = \text{Spa}(A, A^+)\), let \(\widetilde{M} = M \otimes_A \mathcal{O}_X\) be the presheaf on \(X\).

**Prop. (14.8.4.19).** If \(A\) is sheafy, then for any finite projective \(A\)-module \(M\), the presheaf \(\widetilde{M}\) is a sheaf on \(X = \text{Spa}(A, A^+)\), and \(H^i(U, \mathcal{F}) = 0\) for any rational subset of \(X\) and \(i > 0\).

**Proof:** Because \(M\) is a direct sum of a finite free \(A\)-module, then we reduce to the case \(\mathcal{O}_X\) is sheafy. \(\square\)

**Remark (14.8.4.20).** This is a partial analogy with Tate’s acyclicity theorem in rigid analytic geometry(14.5.1.40)(14.5.3.10), but it only holds for f.p. modules, not even f.g. modules. One impediment is that the rational localization map are generally not flat. To get around this, Kedlaya defined a category of pseudo-coherent modules, with the property that even when flatness fails, tensoring is also exact in this category.

**Prop. (14.8.4.21) [Vector Bundles].** Let \((A, A^+)\) be a sheafy analytic Huber pair and \(X = \text{Spa}(A, A^+)\), then the functor \(M \rightarrow \widetilde{M}\) from the category of finite projective \(A\)-modules to the category \(\text{Vect}_X\) of locally finite free \(\mathcal{O}_X\)-modules is an equivalence of categories. In particular, \(\text{Vect}_X\) only depends on \(A\).

**Proof:** Cf.[Ked19].P40? \(\square\)

Pre-Adic Spaces

Main references are [S-W20]L3 and [Ked19].

**Def. (14.8.4.22)[Pre-Adic Spaces].**

**Remark (14.8.4.23).** Pre-adic spaces is an approach to work around the failure of sheafyness of general Huber pair, with techniques from algebraic stacks.

Analytic Points

**Prop. (14.8.4.24)[Analytic and Tate Rings].** Let \((A, A^+)\) be a complete Huber pair, then

- The Huber ring \(A\) is analytic iff all points of \(\text{Spa}(A, A^+)\) are analytic.
- A point \(x \in \text{Spa}(A, A^+)\) is analytic iff there is a rational nbhd \(U \subset \text{Spa}(A, A^+)\) that \(\mathcal{O}_X(U)\) is Tate.

**Proof:**

1: \(x\) is non-analytic iff \(A^{00} \subset \mathfrak{p}_x\) by(10.3.6.5), so all points are analytic iff \(A^{00}A = A\), which means \(A\) is analytic.

2: Let \(x\) be an analytic point, then there exists \(f \in I\) where \(I\) is an ideal of definition that \(|f|_x \neq 0\). Now \(\{g \in A| |g(x)| \leq |f(x)|\}\) is open(because \(|\cdot|_x\) is continuous), so contains some \(I^n\). Now let \(I^n = (g_1, \ldots, g_k)\), then \(U(\frac{g_1}{f}, \ldots, \frac{g_k}{f})\) is a rational subset. Then in \(\mathcal{O}_X(U)\), \(f\) is a unit, but also it is topologically nilpotent, because it is contained in \(I\).

Conversely, if \(x \in X\) has a rational nbhd \(U = U(\mathcal{I}_x^I)\) such that \(\mathcal{O}_X(U)\) is Tate, and \(x\) is not analytic, then \(\mathfrak{p}_x\) contains an ideal of definition \(I \subset A_0\). Now let \(f \in \mathcal{O}_X(U)\) be a topologically nilpotent unit, then there exists \(m \geq 1\) that \(f^m\) lies in the closure of \(\mathcal{I}A_0[t/s]t \in T\) in \(\mathcal{O}_X(U)\). Since \(x \in U\), the valuation \(|\cdot|_x\) extends to \(\mathcal{O}_X(U)\), and since \(|\cdot|_x\) is continuous, \(|f^m|_x = 0\), contradiction, as \(f\) is a unit in \(\mathcal{O}_X(U)\). \(\square\)
**Def. (14.8.4.25) [Analytic Points].** Let \( X \) be a pre-adic space, then a point \( x \in X \) is called an **analytic point** if there is some open affinoid nbhd \( U = \text{Spa}(A, A^+) \subset X \) of \( x \) that \( A \) is Tate. And \( X \) is called **analytic** if all of its points are analytic.

**Prop. (14.8.4.26).** Let \( f : X \to Y \) be a map of analytic pre-adic spaces, then \( |f| : |X| \to |Y| \) is generalizing. If \( f \) is quasi-compact and surjective, then \( |f| \) is a quotient map.

**Proof:** Cf.[Hub96]1.1.10. and [Étale Cohomology of Diamonds, L2.5]. □

**Def. (14.8.4.27).** A map \( f : Y \to X \) of pre-adic spaces is called **analytic** if it carries analytic points to analytic points.

**Proof of Acyclicity and Sheafyness by Cech Reduction**

**Def. (14.8.4.28) [Standard Rational Coverings].** Let \( X = \text{Spa}(A, A^+) \) and \( f_1, \ldots, f_n \in A \) which generates the unit ideal, then the sets \( X(\frac{f_1}{f_n}) \) covers \( X \), called the **standard rational covering** of \( X \). And if \( n = 2 \), it is called a **standard binary rational covering** of \( X \).

There are special types of standard binary rational coverings: if \( f_1 = f, f_2 = 1 \), then it is called a **simple Laurent covering**. If \( f_1 = f, f_2 = 1 - f \), then it is called a **simple balanced covering**.

**Lemma (14.8.4.29) [Reduction of Coverings].** Let \( A \) be an analytic Huber ring,

- (Huber) Every open covering of \( X \) can be refined by some standard rational covering.
- (Gabber-Ramero) Every open covering of a rational subspace of \( X \) can be refined by some compositions of simple Laurent coverings and simple balanced coverings.

**Proof:** 1: Cf.[Ked19]P28.

**Prop. (14.8.4.30) [Cech Reduction].** By a Cech cohomological argument the same as Tate’s acyclicity theorem in rigid geometry(14.5.1.40), it suffices to prove any presheaf is a sheaf or any sheaf is acyclic on simple Laurent coverings and simple balanced coverings.

That is, for every rational localization \((B, B^+)\) over \((A, A^+)\), every pair \( f, g \in B \) that \( g = f \) or \( 1 - f \), if the sequence

\[
0 \to B \to B\langle \frac{f}{g} \rangle \oplus B\langle \frac{g}{f} \rangle \to B\langle \frac{f}{g}, \frac{g}{f} \rangle \to 0,
\]

- is exact at exact at left and middle, then \( O_X \) is sheafy.
- is exact, then \( O_X \) is acyclic.

Also remember the following equations:

\[
B\langle \frac{f}{g} \rangle = B\langle T \rangle/(f - gT), \quad B\langle \frac{g}{f} \rangle = B\langle T \rangle/(g - fT), \quad B\langle \frac{f}{g}, \frac{g}{f} \rangle = B\langle T, T^{-1} \rangle/(f - gT)
\]

**Prop. (14.8.4.31) [Properties of (Finite)Étale Maps].**

- (Finite)Étale maps are invariant under compositions and pullbacks.
- If \( g \) and \( gf \) are (finite)étale, then so does \( f \).
- \( f \) is (finite)étale iff \( f^p \) is (finite)étale.

**Proof:** Cf.[S-W20]P65. □
5 Perfectoid Spaces

Affinoid Perfectoid Spaces and Tilting

Proposition (14.8.5.1) [Tilting Rational Subsets]. For a perfectoid affinoid $K$-algebra $(R, R^+)$ over a perfectoid field $K$,

- The map induces an isomorphism $X = \text{Spa}(R, R^+) \cong X^\flat = \text{Spa}(R^\flat, R^\flat_0)$ that identifies rational open subsets.
- For a rational subset $U$ with tilting $U^\flat$, the complete affinoid Tate algebra $(\mathcal{O}_X(U), \mathcal{O}_X^+(U))$ is perfectoid over $R$ with tilt $(\mathcal{O}_{X^\flat}(U^\flat), \mathcal{O}_{X^\flat}^+(U^\flat))$.

Proof: This follows from (14.8.5.5).

Lemma (14.8.5.2) [Huber’s Presheaf in Char $p$]. Assume $\text{char}K = p$ and $U = X(\frac{f_i - f_n}{g})$ is a rational subset that $f_i, g \in R^+$ and $f_n = \pi^N$, then:

- Consider the subring $R^+[(\frac{f_i}{g})^{1/p^N}]$, its $\pi$-adic completion $(R^+[(\frac{f_i}{g})^{1/p^N}])^a$ is a perfectoid $K_{0a}$-algebra.
- The map $R^+[X_i^{1/p^N}] \rightarrow R^+[(\frac{f_i}{g})^{1/p^N}]$ has kernel containing and almost equal to $I = (g^{1/p^N} X_i^{1/p^N} - f_i^{1/p^N})$.
- $\mathcal{O}_X(U)$ is a perfectoid $K$-algebra and $\mathcal{O}_X(U)^{0a} \cong (R^+[(\frac{f_i}{g})^{1/p^N}])^a$.

Proof:

1: The ring $R^+[(\frac{f_i}{g})^{1/p^N}]$ is perfect and $\pi$-torsion-free, and $R^+$ is semi-perfect, thus its completion is clearly a perfectoid $K_{0a}$-algebra by (10.3.9.1).

2: Clearly $I \subset \ker$ and notice $R^+[(\frac{f_i}{g})^{1/p^N}][\pi^{-1}] = R[g^{-1}]$ as $f_n = \pi^N$, so $I[\pi^{-1}] = \ker[\pi^{-1}]$. Now consider the mapping

$$P_0 = R^+[X_i^{1/p^N}]/I \rightarrow R^+[(\frac{f_i}{g})^{1/p^N}]$$

Now this map is an isomorphism after inverting $\pi$, so the kernel is $\pi^\infty$-torsion. But we have $I = I^{[p]}$ because $R^+$ is semi-perfect, so $P_0$ is perfect, so the kernel must be almost zero.

3: Consider the inclusion $R^+[(\frac{f_i}{g})] \hookrightarrow R^+[(\frac{f_i}{g})^{1/p^N}]$, we show the cokernel is killed by $\pi^{nN}$: as $f_n = \pi^N$,

$$\pi^{nN} \prod_{i=1}^n \left( \frac{f_i}{g} \right)^{1/p^N} = \prod_{i=1}^n \left( \frac{f_i^{1/p^N} g^{-1/p^N}}{g} \right)^{f_n/g} \in R^+\left[ \frac{f_i}{g} \right].$$

So these two ring has the same $\pi$-adic completion, the first one is just $\mathcal{O}_X(U)$ by the construction (14.8.3.1), so $\mathcal{O}_X(U)$ is perfectoid $K$-algebra, and the isomorphism is by tilting equivalence $\text{Perf}_K \cong \text{Perf}_{K_{0a}}$ (10.3.9.5).

Lemma (14.8.5.3) [Huber’s Presheaf in Char 0]. Let $U = X(\frac{f_i - f_n}{g})$ is a rational subset that $f_i, g$ are perfect elements in $R^+$, $f_i = a^i, g = b^i$, and $f_n = \pi^N$, so $f_i, g$ have compatible $p^n$-th roots, then let $U^\flat = X^\flat(\frac{f_i - f_n}{g})$ be the tilting of $U$, $U$ is the inverse image of $U^\flat$ along the map $X \rightarrow X^\flat$. Then the conclusion of (14.8.5.2) is also true, and moreover, $(\mathcal{O}_X(U), \mathcal{O}_X^+(U))$ tilts to $(\mathcal{O}_{X^\flat}(U^\flat), \mathcal{O}_{X^\flat}^+(U^\flat))$. 
Proof: 1, 2 of (14.8.5.2): Notation as before, there is a map $P_0 = R^+[X_i^{1\over p^\infty}] / I \to R^+[\langle t \rangle^{1\over p^\infty}]$, and an inclusion $R^+[\langle t \rangle^{1\over p^\infty}] \to \mathcal{O}_X^+(U)$. Now write $(S, S^+)$ for the untilt of the perfectoid $(R^0, R^0^+)$-algebra $(\mathcal{O}_X, \mathcal{O}_X^+(U))$, then by the tilting process (10.3.9.13), Spa$(S, S^+)$ maps into $U$, so by the universal property, there is a map

$$\mu : (\mathcal{O}_X(U), \mathcal{O}_X^+(U)) \to (S, S^+).$$

Consider the composition

$$P_0 \xrightarrow{a_0} R^+[\langle t \rangle^{1\over p^\infty}] \xrightarrow{d_0} S^+,$$

we prove their completion gives the same $K^{\text{oa}}$-algebras (notice $S^+$ is already complete): $a_0$ is surjective, thus so does its completion, the map $d_0 \circ a_0$ is almost isomorphism modulo $\pi$ by (14.8.5.2) item 2 and tilting equivalence, so does its completion. Now (4.8.3.2) tells us the completion of $d_0 \circ a_0$ is almost isomorphism, so does $a$ and $d$ as $a$ is surjective.

By the way, we know that $R^+[\langle t \rangle^{1\over p^\infty}] / \langle t \rangle [\pi^{-1}]$ is the untilt of $\mathcal{O}_X^+(U)$. 3 of (14.8.5.2) is proved as before.

For the tilting, by the above, we already know $R^+[\langle t \rangle^{1\over p^\infty}]$ tilts to the perfectoid $K^{\text{oa}}$-algebra $\mathcal{O}_X^+(U)$, and by item 3 $\mathcal{O}_X(U)$ tilts to the perfectoid $K^0$-algebra $\mathcal{O}_X(U)$. Now the question is the untilt of $\mathcal{O}_X^+(U)$, notice as in the proof of item 1, there is a natural map

$$(R^+[\langle t \rangle^{1\over p^\infty}] / \langle t \rangle [\pi^{-1}], R^+[\langle t \rangle^{1\over p^\infty}]) \to (\mathcal{O}_X(U), \mathcal{O}_X^+(U)),$$

whose tilting gives by university of Huber’s presheaf a map

$$\xi : (\mathcal{O}_X(U), \mathcal{O}_X^+(U)) \to (\mathcal{O}_X(U), \mathcal{O}_X^+(U))^\flat.$$

These two maps $\mu, \xi$ are inverse to each other, showing that the tilting of $(\mathcal{O}_X(U), \mathcal{O}_X^+(U))$ is $(\mathcal{O}_X(U), \mathcal{O}_X^+(U))^\flat$. [\square]

Lemma (14.8.5.4) [Approximation Lemma]. Assume $R = K\langle T_0^{1\over p^\infty}, \ldots, T_k^{1\over p^\infty} \rangle$, $f \in R^0$ is homogeneous of degree $d \in \mathbb{N}[p^{-1}]$, then for any $c > 0$, $\varepsilon > 0$, there exists some $g_{c, \varepsilon} \in R^{p^0}$ homogeneous of degree $d$ that

$$|f - g^\flat|(x) = |\pi|^1 - \varepsilon \max\{|f(x)|, |\pi|^c\}.$$

In particular, if $\varepsilon < 1$, then

$$\max\{|f(x)|, |\pi|^c\} = \max\{|g_{c, \varepsilon}(x)|, |\pi|^c\}.$$

Proof: Cf.[Sholze Perfectoid Spaces, Lemma6.5]?.

Prop. (14.8.5.5). For an arbitrary perfectoid $K$-algebra $R$,

- The same conclusion of (14.8.5.4) holds.

- For $f, g \in R$, there exist $a, b \in R^0$ that $X(\frac{f^\sharp c}{g^\flat}) = X(\frac{a^\sharp p^c}{b^\flat})$. In particular, any rational subsets $U$ of $X$ comes from $X^\flat$, thus (14.8.5.3) applies for $U$.

- For any $x \in X$, the non-Archimedean field $K(x)$ is perfectoid.
• $X \to X^\circ$ is a homeomorphism preserving rational subsets.

\textbf{Proof:} 1: Using the tilting equivalence, we can write $f = g_0^\circ + \pi g_1^\circ + \ldots + \pi^c g_c^\circ + f_{c+1} \pi^{c+1}$, let $f_0 = g_0^\circ + \pi g_1^\circ + \ldots + \pi^c g_c^\circ$. Then notice that the solution $g_{c,\varepsilon}$ for $f_0$ is suitable for $f$ as well. So now if we consider the mapping

$$
\mu : K\langle T_0^\circ, \ldots, T_n^\circ \rangle \to R : T_i \to g_i^\circ,
$$

together with its tilting

$$
\mu^b : K^\circ\langle T_0^\circ, \ldots, T_n^\circ \rangle \to R^b.
$$

Then for the approximation $g^\circ_{c,\varepsilon}$ for $f' = \sum \pi^i T_i$, $\mu^b(g)$ is what we are searching for.

2: Using 1, we find $a, b \in R^b$ that $|(g - b')| < \max\{|g(x)|, |\pi|\}$ and $\max\{|f(x)|, |\pi|\} = \max\{|a^\circ(x)|, |\pi|\}$ for all $x \in \text{Spa}(R, R^+)$.

3: By (14.8.3.5), $k^+(x)$ equals the completion of the colimit $\colim O_x^+(U)$ over rational subsets $U$ containing $x$. As these are all perfectoid $K^{0_b}$-algebras (10.3.9.14), and completion of the filtered limits of perfectoid $K^{0_b}$-algebras is perfectoid (10.3.9.10), we know that $k^+(x)$ is perfectoid over $K^{0_b}$, thus inverting $\pi$ shows $k(x)$ is also perfectoid over $K$.

4: This is injective because $X$ is $T_0$ and a rational subset is the untilt of a rational subset of $X^\circ$ by item 2. For surjectivity, a point of $X^\circ$ determines a continuous map $(R^b, R^{b+}) \to (k(x), k^+(x))$, thus by untilting (10.3.9.13) corresponds to a map $(R, R^+) \to (L, L^+)$, then $(L, L^+)$ is a perfectoid field, by (10.3.9.15), so it corresponds to a point $y \in X$. Then it is clear that $y$ maps to $x$, because

$$
\begin{array}{ccc}
R^b & \xrightarrow{i} & R \\
\downarrow & & \downarrow \\
k(x) & \xrightarrow{i} & L
\end{array}
$$

is commutative. \hfill \Box

\textbf{Def. (14.8.5.6) [Perfectoid Space].} \textit{Now for any perfectoid affinoid $K$-algebra $R$, we associated to it an affinoid adic space $\text{Spa}(R, R^+)$, called an \textbf{affinoid perfectoid space}.}

Tate’s acyclicity (14.8.6.19) shows that the adic spectrum of a perfectoid affinoid $K$-algebra is sheafy, so we can defined the category of \textbf{perfectoid spaces} is defined to be the full subcategory of adic spaces that is locally isomorphic to an affinoid perfectoid space.

\textbf{Remark (14.8.5.7).} Notice that it is not true that if $(A, A^+)$ is a Huber pair over a perfectoid field $K$ and $\text{Spa}(A, A^+)$ is a perfectoid space, then $A$ is a perfectoid ring. Thus there is ambiguity to the term affinoid perfectoid spaces. But we always use this to mean the affinoid adic space associated to a perfectoid Huber pair.

\textbf{Proof:} Cf.[Ked19]P62. \hfill \Box

\textbf{Prop. (14.8.5.8).} The absolute product of two perfectoid spaces of char $p$ is also a perfectoid space.

\textbf{Proof:} Cf.[Sch17]P71. \hfill \Box

\textbf{Prop. (14.8.5.9) [Fiber Products of Perfectoid Spaces].} The category of perfectoid spaces over $K$ admits fiber products.
**Proof:** Perfectoid spaces are constructed by glueing, thus it suffices to show that the category of perfectoid $K^\flat$-algebras has fiber pushouts, by tilting equivalence. For this, if $X = (A, A^+), Y = (B, B^+), Z = (C, C^+)$, define $X \otimes_Y Z = (D, D^+)$, where $D$ is the completion of $A \otimes_B C$, and $D^+$ is the completion of the integral closure of $A^+ \otimes_B C^+$ in $D$. Then $D$ is a perfect $K^\flat$-algebra, and it is truly the filtered colimits, by (10.3.5.23).

Notice that we don’t even need a base field $K$, Cf. [Ked19]P57.

□

**Prop. (14.8.5.10)** [Tilting Equivalence for Perfectoid Spaces]. Fix a perfectoid field $K$, then for any perfectoid space $X/K$, there is a unique perfectoid space $X^\flat/K$ that satisfies: $X(R, R^+) \cong X^\flat(R^\flat, R^\flat^+)$ functorially, called the **tilt** of $X$. Moreover, this $X^\flat$ satisfies naturally $|X| \cong |X^\flat|$.

**Proof:** Firstly, the universal property truly determines the tilt $X^\flat$ uniquely: if there are two tilts $X_1, X_2$, as they are locally affinoid perfectoid like Spa$(R^\flat, R^\flat^+)$ by (14.8.5.1), the immersion map $\text{Spa}(R^\flat, R^\flat^+) \to X_1$ determines via the functorial isomorphism a morphism $\text{Spa}(R^\flat, R^\flat^+) \to X_2$. Now $X_1$ has a sheaf structure, so these morphisms glue to give a morphism $X_1 \to X_2$. The same argument shows conversely there is a morphism $X_2 \to X_1$, and they are clearly converse to each other, so $X_1 \cong X_2$.

The construction of $X$ is just the glueing of the tilting of the affinoid perfectoid spaces, as the tilting defined in (14.8.5.1) is a functor. The universal property is verified by just checking on the affinoid perfectoid spaces, as we can glue using the sheaf property. For the affinoid case, we should use (14.8.4.4). The last assertion is by (14.8.5.1).

□

6 Properties of Perfectoid Spaces

**Totally Disconnected Spaces**

**Def. (14.8.6.1)** [Totally Disconnected Spaces]. A perfectoid space $X$ is called **totally disconnected** if it is qcqs and any open covering $\{U_i \to X\}$ splits, i.e. $\bigsqcup U_i \to X$ splits, or equivalently, there is a refinement covering $\{V_i \to X\}$ that $X \cong \bigsqcup V_i$.

A perfectoid space $X$ is called **strictly totally disconnected** if it is qcqs and every étale cover splits.

**Prop. (14.8.6.2).** Let $X$ be a qcqs perfectoid spaces, then $X$ is totally disconnected iff all its connected components are of the form $\text{Spa}(K, K^+)$ where $(K, K^+)$ are perfectoid affinoid fields. And it is strictly totally disconnected if moreover $K$ are all alg.closed.

**Proof:** Cf. [Sch17].P29, P35.

□

**Prop. (14.8.6.3).** if $X$ is a totally disconnected perfectoid space, then $X$ is affinoid.

**Proof:** Cf. [Sch17].P30.

□

**Injections**

**Def. (14.8.6.4)** [Injections]. A map $f : X \to Y$ of perfectoid spaces is called an injection if for any perfectoid space $Z, f_* : \text{Hom}(Z, X) \to \text{Hom}(Z, Y)$ is an injection.
Prop. (14.8.6.5)[Residue Field Map is Injection]. Let $X$ be a perfectoid space and $x \in X$, giving rise to a map of residue fields

$$i_x : \text{Spa}(\kappa(x), \kappa(x)^+) \to X,$$

then $i_x$ is an injection of perfectoid spaces.

Proof: To show this, firstly we can replace $X$ with an affinoid nbhd of $X$. Then notice that $\text{Spa}(\kappa(x), \kappa(x)^+)$ is the filtered limit over all rational nbhds $U$ of $x$ in $X$, and for each $U$, $U \to X$ is an injection by definition (14.8.3.1), so $i_x$ is also an injection. □

Prop. (14.8.6.6)[Characterizations of Injections]. Let $f : Y \to X$ be a map of perfectoid spaces, then the following conditions are equivalent:

- $f$ is an injection.
- For any perfectoid adic field $(K, K^+)$, the map of sets $f_* : Y(K, K^+) \to X(K, K^+)$ is an injection.
- The map $\vert f \vert : \vert Y \vert \to \vert X \vert$ is injective, and for all rank 1 point $y \in Y$ with image $f(y) = x \in X$, the map of completed residue fields $\kappa(x) \to \kappa(y)$ is an isomorphism.
- The map $\vert f \vert : \vert Y \vert \to \vert X \vert$ is injective, and $f$ is final in the category of maps $Z \to X$ that $\vert Z \vert \to \vert X \vert$ factors through the map $\vert Y \vert \to \vert X \vert$.

In particular, by item 4, an injection of perfectoid spaces is determined by its topological map.

Proof: $4 \to 1 \to 2$ is trivial. For the rest, Cf.[Sch17]P21. □

Prop. (14.8.6.7)[Injection and Base Change].

- Let $f : Y \to X$ be an injection of perfectoid spaces, and $X' \to X$ any map of perfectoid spaces, then the pullback $f' : Y' = Y \times_X X' \to X'$ is also an injection, and the induced map $\vert Y' \vert \to \vert Y \vert \times_{\vert X \vert} \vert X' \vert$ is a homeomorphism.

A map of perfectoids spaces is an injection iff it is universally injective.


Immersions

Def. (14.8.6.8)[Immersions]. A map of perfectoid spaces $f : Y \to X$ is called an immersion if $f$ is an injection and $\vert f \vert : \vert Y \vert \to \vert X \vert$ is a locally closed immersion. If $\vert f \vert$ is moreover closed or open, then it is called closed/open immersion.

Def. (14.8.6.9)[Zariski Closed Immersion]. Let $f : Z \to X$ be a map of perfectoid spaces where $X = \text{Spa}(R, R^+)$ is affinoid perfectoid, then

- the map $f$ is called Zariski closed immersion if $f$ is a closed immersion and $\vert Z \vert = V(I) \subset \vert X \vert$, where $I \subset R$ is an ideal.
- the map $f$ is called strongly Zariski closed immersion if $Z = \text{Spa}(S, S^+)$ is affinoid perfectoid, $R \to S$ is surjective, and $S^+$ is the closure of $R^+$ in $S$.

Prop. (14.8.6.10).
• If \( f \) is strongly Zariski closed, then \( f \) is Zariski closed, in particular a closed immersion.
• If \( f \) is Zariski closed, then \( Z \) is affinoid.
• If \( X \) is of characteristic \( p \), and \( f \) is Zariski closed, then \( f \) is strongly Zariski closed.

Proof: Cf.\([Sch12]\) Section 2.5.

Prop. (14.8.6.11). For any map of perfectoid spaces \( Y \to X \), the diagonal map \( \Delta_f : Y \to Y \times_X Y \) is an immersion.

Proof: Clearly \( \Delta_f \) is an injection, thus it suffices to show that \( |\Delta_f| \) identifies \( Y \) with a locally closed subset of \( |Y \times_X Y| \). This can be checked locally on the target, so we can assume \( X = \text{Spa}(R, R^+) \) and \( Y = \text{Spa}(S, S^+) \), then the diagonal map is strongly Zariski closed, as \( S \hat{\otimes}_R S \to S \) is surjective and maps the integral closure of \( S^+ \hat{\otimes}_R S^+ \to S^+ \) onto \( S^+ \). Thus by (14.10.1.11), \( \Delta_f \) is a closed immersion in this case.

Def. (14.8.6.12) [Separated Map]. A map \( f : Y \to X \) of perfectoid spaces is called separated if \( \Delta_f \) is a closed immersion.

Prop. (14.8.6.13) [Valuation Criterion]. Let \( f : Y \to X \) be a map of perfectoid spaces. The following are equivalent:
• \( f \) is separated.
• \( |\Delta_f| : |Y| \to |Y \times_X Y| \) is a closed immersion.
• \( |f| \) is quasi-separated, and for any perfectoid adic field \((K, K^+)\) and any diagram

\[
\begin{array}{ccc}
\text{Spa}(K, \mathcal{O}_K) & \xrightarrow{f} & Y \\
\downarrow & & \downarrow f \\
\text{Spa}(K, K^+) & \to & X \\
\end{array}
\]

Almost Acyclicity

Def. (14.8.6.14) [\( p \)-Finite Tate Ring]. Denote \( L = \mathbb{F}_p[[t]]_{\text{perf}}[t^{-1}] \), an \( \mathbb{F}_p[t] \) algebra \( A^+ \) is called algebraically admissible if it is f.p., reduced, \( t \)-torsion-free, and integrally closed in \( A^+[t^{-1}] \). A perfectoid affinoid \( L \)-algebra \((R, R^+)\) is called \( p \)-finite if it is the completion of the perfection (14.8.2.28) of a uniform Tate ring of the form \((A^+[t^{-1}], A^+)\), where \( A^+ \) is algebraically admissible.

Lemma (14.8.6.15) [Tate’s Acyclicity for Classical Affinoid Algebra]. If \( A^+ \) is an algebraically admissible \( \mathbb{F}_p[t] \)-algebra, then \((A^+[t^{-1}], A^+)\) is a uniform affinoid Tate algebra (because it is finite), and:
• For any rational subset \( U \subset X \), the structure presheaf \((\mathcal{O}_X(U), \mathcal{O}_X^+(U))\) is also uniform, and it is a perfection of an algebraically admissible \( \mathbb{F}_p[t] \)-algebra, so \( \mathcal{O}_X^+(U) = \mathcal{O}_X(U)^0 \).
• For any covering \( \mathcal{U} : U_i \to X \) of rational subsets, the \( \check{\text{Cech}} \) cohomology groups \( H^i(\mathcal{U}, \mathcal{O}_X^+) \) are all killed by \( t^N \) for \( N \) large.
• \((A, A^+)\) is sheafy, with \( H^i(X, \mathcal{O}_X^+) \) being \( t^\infty \)-torsion for all \( i \).

Proof: ?
Lemma (14.8.6.16) [Tate’s Acyclicity for $p$-Finite Perfectoid Algebras]. Let $(R, R^+)$ be a $p$-finite perfectoid $L$-algebra that comes from the completion of perfection of $(A, A^+)$, then:

- The map $X = \text{Spa}(R, R^+) \rightarrow Y = \text{Spa}(R, R^+)$ is a homeomorphism.
- For rational subset $V \subset Y$ with preimage $U \subset X$, $(\mathcal{O}_X(U), \mathcal{O}_X^+(U))$ is the completion of the perfection of $(\mathcal{O}_Y(V), \mathcal{O}_Y^+(V))$.
- For any covering $U_i : U_i \rightarrow X$ of rational subsets, the Čech cohomology groups $H^i(\mathbb{U}, \mathcal{O}_X^+)$ are all almost zero.
- $(R, R^+)$ is sheafy, with $H^i(X, \mathcal{O}_X^+)$ almost zero for all $i > 0$.

Proof: 1: This is because the adic spectrum is insensitive for perfection (14.8.2.28) and completion (14.8.2.17).

2: This is by the universal property, as these two are both the universal elements for the complete and affinoid adic spaces mapping to $X$ that factors through $U$.

3: The complex calculating $H^i(\mathbb{U}, \mathcal{O}_X^+)$ is just the complex calculating $H^i(\mathbb{U}, \mathcal{O}_Y^+)$ under completion of perfection ([14.8.2.27] used). So (14.8.6.15) and (14.8.6.17) (applied to every element) shows that the perfection makes the complex almost acyclic, and this is preserved under completion as $(-)^a$ is exact.

4: The complex calculating $H^i(\mathbb{U}, \mathcal{O}_X^+)$ is just the complex calculating $H^i(\mathbb{U}, \mathcal{O}_Y^+)$ inverting $t$, thus they are all 0 as localization is exact. For the second, it is because of item 3 and the fact $\mathcal{O}_X^+$ is almost isomorphic to $\mathcal{O}_X^p$ (10.3.9.14). $\square$

Lemma (14.8.6.17). Let $A$ be a ring with an element $t$ that admits compatible $p^n$-th roots, then for an $A$-module $M$ that $t^nM = 0$, consider the Frobenius pushforward $M \rightarrow F_*M$, then the colimit $\text{colim}_{F_*} F^n_* M$ is naturally a module over $A_{\text{perf}}$, and it is annihilated by $t^N$ for all $n$.

Proof: The $A_{\text{perf}}$ structure is natural, and notice $F^n_* M$ is annihilated by $t^N$, thus naturally the colimit is annihilated by $t^N$ for all $n$. $\square$

Prop. (14.8.6.18) [Noetherian Approximation in Charp]. If $K$ is a perfectoid field of charp with pseudo-uniformizer $t$, then $K$ is an extension of $L = F_p[[t]]_{\text{perf}}[t^{-1}]$, and If $A$ is an $R^0$-perfectoid algebra that is integrally closed in $A[t^{-1}]$, then:

- $A$ is a completion of a filtered colimit $\text{colim}_i B_i$ that $B_i$ are $p$-finite, that induces an homeomorphism

$$\text{Spa}(A[t^{-1}], A) \cong \lim_i \text{Spa}(B_i[t^{-1}], B_i)$$

that each rational subset of $\text{Spa}(A[t^{-1}], A)$ comes from a rational subset of some $\text{Spa}(B_i[t^{-1}], B_i)$.

- If $U_i \subset \text{Spa}(B_i[t^{-1}], B_i)$ is a compatible system of rational subsets that corresponds to $U \subset \text{Spa}(A, A^+) = X$, then

$$(\mathcal{O}_X(U), \mathcal{O}_X^+(U)) \cong \lim_j (\mathcal{O}_j(U_j), \mathcal{O}_j^+(U_j)).$$

Proof: 1: $A = \text{colim}_i A_i$, where $A_i$ are all the f.p. $F_p[[t]]$-algebras in $A$. Then each $A_i$ is reduced (as $A$ is complete and integrally closed in $A[t^{-1}]$) and $t$-torsion-free, and we can assume they are integrally closed in $A_i[t^{-1}]$ because $A$ does, by passing to their integral closure.
Then applying the $(-)_{\text{perf}}$ functor gives $\text{colim}_i (A_i)_{\text{perf}} = A$, as $A$ is perfect, and applying the completion gives

$$\hat{\text{colim}_i (A_i)} = A,$$

as $A$ is already complete, so we are done.

2: This is immediate from 1 and (14.8.2.27).

3: This is because by universal property for Huber presheaves, there are pushouts diagrams

$$
\begin{array}{ccc}
(B_i[t^{-1}], B_i) & \longrightarrow & (B_j[t^{-1}], B_j) \\
\downarrow & & \downarrow \\
(O_{X_i}(U_i), O_{X_i}^+(U_i)) & \longrightarrow & (O_{X_j}(U_j), O_{X_j}^+(U_j))
\end{array}
$$

So the conclusion follows as colimits commutes with colimits.

Prop. (14.8.6.19) [Almost Acyclicity for Perfectoids]. Fix a perfectoid field $K$ and a perfectoid affinoid $K$-algebra $(R, R^+)$ with adic spectrum $X = \text{Spa}(R, R^+)$, then

- $(R, R^+)$ is sheafy, i.e. $O_X$ and $O_X^+$ are sheaves.
- $O_X^+(X) = R^+$, and $H^i(X, O_X^+)$ is almost zero for $i > 0$.
- $O_X(X) = R$, and $H^i(X, O_X) = 0$ all $i > 0$.

Proof: As in the proof of (14.8.6.16), it suffices to prove $O_X^+$ is almost exact w.r.t any covering $\mathcal{U}$.

For this, notice each term is $\pi$-adically complete and flat by (14.8.5.1), so it suffices to prove it is almost exact modulo $\pi(4.8.3.2)$. Then by the tilting equivalence, it suffices to prove for $X^n$. So we may assume at first that $K$ is of char $p$. Then we may replace $K$ by $L = \mathbb{F}_p[[t]]_{\text{perf}}[t^{-1}]$.

But then Noetherian approximation (14.8.6.18) shows that the rational subrings are completion of filtered colimits of $p$-finite $K$-algebras ((14.8.2.27) used), and then we reduced to the $p$-finite case, as in the proof of (14.8.6.16).

7 Étale Site of Perfectoid Spaces

Def. (14.8.7.1) [Finite Étale Map of Adic Spaces]. A map of Huber pairs $(A, A^+) \to (B, B^+)$ is called finite étale if $A \to B$ is finite étale, and $B^+$ is the integral closure of $A^+$ in $B$.

A map $f : X \to Y$ of adic spaces is called finite étale if there is a cover of $Y$ by affinoids $V \subset Y$ that $U = f^{-1}(V)$ are all affinoids, and the map $(O_Y(V), O_Y^+(V)) \to (O_X(U), O_X^+(U))$ is finite étale. Write $Y_{\text{f\acute{e}t}}$ for the category of all such maps.

Def. (14.8.7.2) [Étale Maps]. A map $X = \text{Spa}(A, A^+) \to Y = \text{Spa}(B, B^+)$ of adic spaces is called étale iff for any $x \in X$, there exists an open $x \in U$ and open $f(U) \subset V$ together with an adic space $W$ that $f : U \to V$ factors through an open immersion $U \to W$ and a finite étale map $W \to V$.

Cf.[?P65].

Def. (14.8.7.3) [Strongly Finite Étale]. For convenience, in case of perfectoid affinoid $K$-algebras, we call a map of Huber pairs $(A, A^+) \to (B, B^+)$ strongly finite étale if it is finite étale and $B^{+a}$ is almost finite étale over $A^{+a}$.

A map $f : X \to Y$ of adic spaces is called strongly finite étale if there is a cover of $Y$ by affinoids $V \subset Y$ that $U = f^{-1}(V)$ are all affinoids, and the map $(O_Y(V), O_Y^+(V)) \to (O_X(U), O_X^+(U))$ is strongly finite étale. Write $Y_{s\text{f\acute{e}t}}$ for the category of all such maps.
Finally we will prove that if \((A, A^+)\) is perfectoid, then any finite étale map \((A, A^+) \to (B, B^+)\) is strongly finite étale.

**Prop. (14.8.7.4) [Strongly Finite Étale Maps Form a Stack].** If \(f : X \to Y\) is a strongly finite étale map that \(Y = \text{Spa}(A, A^+)\) is an affinoid perfectoid, then \(X\) is also affinoid perfectoid, and the structure map \((\mathcal{O}_X(X), \mathcal{O}^+_X(X)) \to (\mathcal{O}_Y(Y), \mathcal{O}^+_Y(Y))\) is strongly finite étale.

**Proof:** By (14.8.7.9), it suffices to prove in charp. Then we can replace \(K\) by \(L = \mathbb{F}_p[[t]]_{\text{perf}}[t^{-1}]\). Then by Noetherian approximation (14.8.6.18), we can assume that \(Y\) is a limit of \(p\)-finite affinoids \(\text{Spa}(B_i, B_i^+)\). As both rational subsets and finite étale algebras pass through filtered colimits, and adic spectrum is quasi-compact (14.8.2.24), we can assume that a finite étale cover of \(Y\) arises through base change of some \(\text{Spa}(B_i, B_i^+)\). So it suffices to prove the proposition in case of \(Y\) \(p\)-finite. Then \(Y\) is a completion of perfection of some algebraically admissible ring over \(\mathbb{F}_p[t]\). Then by the above argument again, we can assume that \(Y\) is algebraically admissible.

Now a classical theorem (Cf. [Étale cohomology of rigid analytic varieties and adic spaces, Huber 1.6.6(2)]) shows that the finite étale cover of \(X\) is global finite étale. Notice the strongness is not needed because we are working in char \(p\), where almost purity theorem is already proven.

**Cor. (14.8.7.5).** For an affinoid perfectoid space \(Y = \text{Spa}(R, R^+)\), the functor \(X \mapsto \mathcal{O}^+_X(X)\) defined an equivalence of categories \(Y_{sf\text{-ét}} \cong R^a_{af\text{-ét}}\), and the functor \(X \mapsto \mathcal{O}_X(X)\) gives a fully faithful functor \(Y_{sf\text{-ét}} \to R_{f\text{-ét}}\).

**Def. (14.8.7.6) [Étale Site of Perfectoid Spaces].** Let \(X\) be a perfectoid space, then the étale site of \(X\) is the category \(X_{\text{ét}}\) of perfectoid spaces that is étale over \(X\), and coverings are given by topological coverings. We also consider the following subcategories:

- \(X^\text{off}\), the category of affinoid perfectoid spaces étale over \(X\).
- \(X_{\text{ét},qcqs}\), the full subcategory of qcqs perfectoid spaces étale over \(X\).
- \(X_{\text{ét},qc,sep}\), the full subcategory of qc separated perfectoid spaces étale over \(X\).

**Prop. (14.8.7.7) [Gabber-Ramero].** If \(A\) is a finite \(K^0\)-algebra that is \(\pi\)-adically Henselian, then
\[
A[\pi^{-1}]_{f\text{-ét}} \cong \hat{A}[\pi^{-1}]_{f\text{-ét}}.
\]

**Proof:** Cf. [Almost Ring Theory P5.4.53].

**Cor. (14.8.7.8) [Finite Étale Covers and Direct Limits of Complete Uniform Rings].** Let \((A_i, A_i^+)\) be a filtered system of complete uniform affinoid \(K\)-algebras, and \((A, A^+)\) be their colimit in the category of complete uniform affinoid Tate rings, then
\[
2 - \text{colim}_i A_{i, f\text{-ét}} \cong A_{f\text{-ét}}
\]
as categories.

**Proof:** By (14.8.2.27), \(A^+\) is the \(\pi\)-adic completion of the algebraic colimit \(B^+\) of \(A_i^+\), and \(A = A^+[\pi^{-1}]\). Each \(A_i\) is complete and \(\pi\)-torsion-free, thus the colimit is Henselian and \(\pi\)-torsion-free (4.3.10.3) (4.3.10.6). Then the proposition (14.8.7.7) shows that \(B^+[\pi^{-1}]_{f\text{-ét}} \cong A_{f\text{-ét}}\). Now it remains to show that
\[
2 - \text{colim}_i A_{i, f\text{-ét}} \cong B^+_{f\text{-ét}}[\frac{1}{\pi}]_{f\text{-ét}},
\]
which is because étale sites commutes with taking filtered colimits.
Final Proof of Almost Purity Theorem

Prop. (14.8.7.9). We have an equivalence of categories $X_{sf\text{ét}} \cong X^b_{sf\text{ét}}$. For this, use (14.8.7.5), (14.8.5.10) and the proven part of (10.3.10.1) and notice that

$$A^+_{af\text{ét}} = A^{0a}_{af\text{ét}} \cong A^{00a}_{af\text{ét}} = A^{b+a}_{af\text{ét}},$$

and the integral closure clearly corresponds. (It get around the problem that $R^a_{f\text{ét}} \to R_{f\text{ét}}$ hasn’t been proven essentially surjective).

Prop. (14.8.7.10) [Proof of Almost Purity Theorem]. Fix a perfectoid affinoid $K$-algebra $(R, R^+)$, if $S \in R_{f\text{ét}}$, then the integral closure of $S^+$ in $R^+$ lies in $R^{a+}_{af\text{ét}}$, and this gives an inverse to the morphism $d$ in (10.3.10.1), thus finishing the proof of almost purity theorem.

Proof: Continuing the proof of (10.3.10.1), it suffices to show that $d: R^a_{af\text{ét}} \to R_{f\text{ét}}$ is essentially surjective, because $S^+ \to S \subset R^+$ is the only possible inverse, by the almost purity theorem in char$p$ and tracing the tilting equivalence (10.3.9.6). Given (14.8.7.5), it suffices to prove that for $X = \text{Spa}(R, R^+)$, the prestacks $X_{sf\text{ét}} \cong X_{f\text{ét}}$, where $X_{sf\text{ét}}(U) = \mathcal{O}^+_X(U)_{sf\text{ét}}$, and $X_{f\text{ét}}(U) = \mathcal{O}_X(U)_{f\text{ét}}$.

We use (5.1.3.22), firstly $X_{af\text{ét}}$ is a stack, by (14.8.7.4), and for each $U$, $X_{sf\text{ét}}(U) \to X_{f\text{ét}}(U)$ is fully faithful by almost purity theorem (10.3.10.1). $X_{f\text{ét}}$ is separated by (14.8.4.21), because the structure section of an element $S \in X_{f\text{ét}}$ is determined its value on the stalk.

Its left to prove that their stalks are equal, for this, use the formula

$$\text{colim}_{x \in U}(\mathcal{O}_X(U), \mathcal{O}^+_X(U)) = (\widehat{k(x)}, \widehat{k^+(x)})$$

in the category of complete uniform affinoid $K$-algebras (they are all perfectoids (14.8.5.1) thus uniform), by definition. So we get by (14.8.7.8):

$$\text{colim}_{x \in U} \mathcal{O}_X(U)_{f\text{ét}} \cong \widehat{k(x)}_{f\text{ét}},$$

and by (14.8.7.8) together with the proven part of almost purity theorem (10.3.10.1):

$$\text{colim}_{x \in U} \mathcal{O}^+_X(U)_{af\text{ét}} \cong \text{colim}_{x \in U'} \mathcal{O}^+_X(U^b)_{af\text{ét}} \cong \kappa^+(x^b)_{af\text{ét}} \cong \kappa^+(x)_{af\text{ét}}.$$

Now we have already proved the almost purity over fields (10.3.10.1) which says $\kappa(x^b)_{af\text{ét}} \cong \kappa^+(x)_{af\text{ét}}$, so their stalks are the same.

Cor. (14.8.7.11) [Invariance of Étale Site under Tilting]. There is a natural isomorphism of categories $X_{\text{ét}} \cong X^b_{\text{ét}}$, by almost purity theorem (10.3.10.1) and the localness of étale maps.

Prop. (14.8.7.12) [Almost Acyclicity]. For any perfectoid space $X$, the functor $U \mapsto \mathcal{O}_X(U)$ is a sheaf on $X_{\text{ét}}$, and $H^i(X_{\text{ét}}, \mathcal{O}^+_X)$ is almost zero if $X$ is affinoid perfectoid.
14.9 Fargues-Fontaine Curve

Basic references are [FF curves Lurie], [FF Curve Johannes], [The Fargues-Fontaine Curve and Diamonds Mathew Morrow], [Laurent Fargues and Jean-Marc Fontaine. Courbes et fibrés vectoriels en théorie de Hodge p-adique]

1 Fontaine’s Rings

Fontaine’s Ring $A_{\text{inf}}$

Def.(14.9.1.1)[Fontaine’s Ring $A_{\text{inf}}$]. Let $C^0$ be a perfectoid field of char$p$, Fontaine’s ring $A_{\text{inf}}$ is defined to be the Witt vectors $W(O_{C^0}) = A_{\text{inf}}(O_C)$

the set of all the char0 untilts of $C$ is denoted by $Y$, and $Y_{[a,b]}$ denotes those untilts that $a \leq |p|^K \leq b$.

Prop.(14.9.1.2). By(10.3.9.7), if $K$ is perfectoid field of char0 with tilt $C^0$, there is a diagram

$$
\begin{array}{ccc}
A_{\text{inf}} & \xrightarrow{\theta} & O_K \\
\downarrow & & \downarrow \\
O_C & \xrightarrow{\varphi} & O_K/\pi
\end{array}
$$

And the kernel $\ker \theta$ is generated by $\xi = \pi u - [t]$, where $[t]$ is the Techmuller lift, because it generate after modulo $p$, and use Nakayama.

Lemma(14.9.1.3). If $R$ is a commutative ring, $x, y \in R$, if $x$ is not a zero-divisor in $R$ and $R$ is $x$-adically complete Hausdorff, and $y$ is not a zero-divisor in $R/\pi x$ and $R/\pi x$ is $y$-adically complete, then the same is true with $x, y$ interchanged.

Proof: ?

Prop.(14.9.1.4)[Untilts and Distinguished Elements]. (14.9.1.2) shows that for any untilt $K$ of $C^0$, the kernel is generated by a distinguished element. Conversely, for any distinguished element $\xi$, $A_{\text{inf}}(\xi)$ can be identified with the valuation ring $O_K$ of a perfectoid field $K$, and $O_{C^0} = A_{\text{inf}}/\pi \to A_{\text{inf}}(\xi)/\pi \cong O_K/\pi$

exhibits $K$ as an untilt of $C^0$.

Proof: May assume $\xi = [t] - u\pi$ and $t \neq 0$. Consider the mapping $\theta : A_{\text{inf}} \to A_{\text{inf}}(\xi) = O_K$, and denote $\theta([x])$ by $x^t$.

Firstly, we can apply lemma(14.9.1.3) to $\xi$ and $p$ to conclude that $A_{\text{inf}}$ is $\xi$-complete and $\xi$-torsion-free, and $O_K$ is $p$-adically complete and $p$-torsion-free.

Now for any $y \in O_K$ is $p$-adically complete, there is a $x \in O_C$ that $(y) = (x^t)$: multiplying $p$-power, we can assume $y$ is not divisible by $p$, and there is a $x$ that $y \equiv x^t \mod p$, thus $x$ is not divisible by $t$. Now $t = xx'$ for some $x' \in m_C$, thus $y = x^t + t^2w = x^2(1 + x'w)$, and $1 + x'w$ is invertible in $O_K$.

Next we prove $O_K$ is an integral domain: It suffices to show any $y \neq 0 \in O_K$ is not a zero-divisor. We can assume $y = x^t$, by what just proved, and then $x$ divides $t^n$ for some $n$, so it suffices to consider $y = t^n = p^n$, and $p^n$ is not a zero-divisor by what just proved.
Now we can endow $\mathcal{O}_K$ with the valuation $|y| = |x|_{C^0}$ for $y = x^u$, and extend it to the quotient field $K$. Then this is a Non-Archimedean valuation and the residue field has char $p$ because $|p| < 1$, and $K$ has char 0, because $p \neq 0$ in $K$. And it is $p$-adically complete.

Finally, $\mathcal{O}_K/p\mathcal{O}_K \cong A_{\inf}/(\xi,p) = \mathcal{O}_{C^0}/\pi$, so the Frobenius is surjective, thus $K = K(\mathcal{O}_K)$ is a perfectoid field.

**Cor. (14.9.1.5).** The correspondence $\xi \mapsto \text{Quot}(A_{\inf}/(\xi))$ induces a bijection

\[
\{\text{Distinguished elements}\}/\text{units} \cong \{\text{Untilts of } C^0\}/\text{isomorphisms}.
\]

**Prop. (14.9.1.6)[*A_{\inf} as Holomorphic Function in $p*$].** Any element in $A_{\inf}$ can be written uniquely as a unique Teichmuller representation $[c_0] + [c_1]p + [c_2]p^2 + \ldots$. Now we can regard these elements as holomorphic functions on $B(0,1)$, and any untilts $K$ of $\mathcal{O}_{C^0}$ can be regarded as points, where $A_{\inf}$ take value $c_0^2 + c_1^2p + \ldots \in \mathcal{O}_K$ at the point $K$.

This map can in fact be extended to $A_{\inf}[\frac{1}{[t]}, \frac{1}{p}]$ that

\[
A_{\inf} \leftrightarrow A_{\inf}[\frac{1}{[t]}] \leftrightarrow A_{\inf}[\frac{1}{[t]}, \frac{1}{p}] \rightarrow K.
\]

called the valuation map.

**Ring $B$**

**Def. (14.9.1.7)[*Fontaine’s Ring $B*$].** If compared to the complex case, the elements of $A_{\inf}$ are just elements $\sum a_n z^n$ that $|a_n| \leq 1$, this are not all the holomorphic functions on $B(0,1)$, which is $\sum a_n z^n$ that $\lim \sup |a_n| \leq 1$. This leads to an enlargement of $A_{\inf}$:

For $0 < a \leq b < 1$ in the value group of $C^0$, $|\pi_a| = a, |\pi_b| = b$, define

\[
B_{[a,b]} = A_{\inf} \bigg[ \frac{\pi_a}{p}, \frac{p}{\pi_b} \bigg] [p^{-1}]^{-1},
\]

this is definable at any untilts $K$ that $a \leq |p|_K \leq b$.

Then $B_{[a,b]}$ is an algebra over $A_{\inf}[\frac{1}{[t]}, \frac{1}{p}]$, and define $B = \lim B_{[a,b]}$.

**Prop. (14.9.1.8)[*Gauss Norm*].** Any element $f$ in $A_{\inf}[\frac{1}{[t]}, \frac{1}{p}]$ is of the form $\sum a_n z^n$ where $\{|c_n|\}$ is bounded. So we can define the valuation $|f|_\rho = \sup\{|c_n|\}$, where $|a|_\rho^n$. Notice that for an until $y = (K, \iota)$, if $\rho = |p|_K$, then $|f(y)| \leq |f|_\rho$.

Then this is a non-Archimedean valuation on $A_{\inf}[\frac{1}{[t]}, \frac{1}{p}]$.

**Proof:** Firstly $|f + g|_\rho \leq \max\{|f|_\rho, |g|_\rho\}$ for every $\rho$ that is generic for $f + g$ and in the value group of $C^0$: In this case,

\[
|f + g|_\rho = |(f + g)(y)| \leq \max\{|f(y)|, |g(y)|\} \leq \max\{|f|_\rho, |g|_\rho\}
\]

for some point $y$ by(14.9.1.8), then by continuity and(14.9.1.9), this is true for any $\rho$.

The same method shows that $|f|_\rho |g|_\rho = |fg|_\rho$.

**Lemma(14.9.1.9)[*Generic Norms*].** $\rho$ is called generic for $f$ iff the valuation is realized exactly once. Notice if $\rho$ is generic for $f$ and in the value group of $C^0$, then $|f|_\rho = |f(y)|$ for some $y$(Choose $K = A_{\inf}/([c] - p)$ where $|c|_{C^0} = \rho$).

For any $f$, the numbers $\rho$ that $\rho$ is not generic for $f$ is discrete in $\rho$.  

Lemma (14.9.1.10). If \( y \) is a point that \( |p|_{K} = \rho \), then \( |f(y)| \leq |f|_{\rho} \), and equality holds if either \( \rho \) is generic or \( f \) is invertible.

Prop. (14.9.1.11) [Valuation Map]. For \( 0 < a < b < 1 \) in the value group of \( C^0 \), \( |\pi_a| = a, |\pi_b| = b, \)
\[
A_{\inf}[\frac{[\pi_a]}{p}, \frac{p}{[\pi_b]}] = \{ f \in A_{\inf}[\frac{1}{p}, \frac{1}{p}] | |f|_a \leq 1, |f|_b \leq 1 \} = V_0,
\]
Thus the ring \( B_{[a,b]} \) is identified with the completion of \( A_{\inf}[\frac{1}{p}, \frac{1}{p}] \) w.r.t the valuation \( | \cdot |_a + | \cdot |_b \). In particular, for any point \( y \) that \( a \leq |p|_{K} \leq b \), the valuation map (14.9.1.6) can be extended to a map
\[
B_{[a,b]} \rightarrow K.
\]

Proof: Notice \( V_0 \) is a subring by (14.9.1.8), so clearly \( A_{\inf}[\frac{[\pi_a]}{p}, \frac{p}{[\pi_b]}] \subset V_0 \).

For the reverse containment, notice that \( \{|c_n|\} \) is bounded, so there is an \( m \) that \( \pi^m c_n \in C^0 \) for any \( n \). Now
\[
f = \sum_{n<m} [c_n]p^n + \left( \sum_{n \geq 0} [c_{n+m}\pi^m]p^n \right) \left( \frac{p}{\pi} \right)^m,
\]
so it suffices to prove the case \( f \) has finite presentation. Now \( c_n \pi^m_a, c_n \pi^m_b \in \mathcal{O}^0_C \), thus \( [c_n]p^n = [c_n \pi^n_a] \left( \frac{p}{\pi} \right)^{-n} = [c_n \pi^n_b] \left( \frac{p}{\pi} \right)^{n} \in A_{\inf}[\frac{[\pi_a]}{p}, \frac{p}{[\pi_b]}] \), where \( n \geq 0 \) or \( n \leq 0 \). Thus the inverse containment is true. \( \square \)

Prop. (14.9.1.12) [Topology of \( B \)]. For \( 0 < a < c \leq b < 1 \), \( |f|_{c} \leq \max \{|f|_a, |f|_b\} \) (trivial), thus the Fontaine’s ring \( B \) can be realized as the completion of all the norms, and endowed with the topology of \( p \)-adic Fréchet space.

Prop. (14.9.1.13) [Teichmuller Expansion]. An infinite sum \( f = \sum [a_n]p^n \) converges in \( B \) iff it converges in any norm \( | \cdot |_\rho \) for \( 0 < \rho < 1 \), which is equivalent to
\[
\limsup_{n \to \infty} |c_n|^{1/n}_{C^0} \leq 1, \quad \lim_{n \to \infty} |c_{-n}|^{1/n}_{C^0} = 0.
\]
This is analogous to the complex case (10.5.3.5). However, for now, we don’t know if every element of \( B \) is of this form, and whether the representation is unique?.

Prop. (14.9.1.14) [Frobenius Action]. Notice the Frobenius action of \( C^0 \) extends to a Frobenius action on the Witt vector \( A_{\inf} \), and it satisfies
\[
|\varphi(f)|_{\rho^p} = (|f|_{\rho})^{p},
\]
Thus induces an isomorphism \( B_{[a,b]} \cong B_{[a\rho,b\rho]} \). Passing to the limit, we get an automorphism of \( B \), denoted also by \( \varphi \).
Fargues-Fontaine Curve

Def. (14.9.1.15) [Fargues-Fontaine Curve]. The sum $\oplus_n B^{p^n}$ is a graded ring. In fact, it is non-negatively graded $(14.9.2.29)$, and we define the **Fargues-Fontaine curve** as the scheme

$$\text{Proj}(\oplus_{n \geq 0} B^{p^n}).$$

Def. (14.9.1.16) [Formal Logarithm]. For $x \in 1 + \mathfrak{m}_{C^p}$, $[x] - 1 = [x - 1] + \sum_{n > 0}[c_n]p^n$, thus $|[x] - 1|_p \geq |x - 1| > 0$, thus the formal logarithm

$$\log([x]) = \sum_{k > 0} \frac{(-1)^{k+1}}{k}([x] - 1)^k$$

converges for every Gauss norm $|.|_p$, thus converges to some element in $B$. And clearly $\varphi(\log([x])) = p\log([x])$, thus $\log([x]) \in B^{p^n}$. And $\log([xy]) = \log([x]) \log([y])$.

Prop. (14.9.1.17) [Artin-Hasse Exponential]. There is another way of constructing elements in $B^{p^n}$, which is

$$T : a \in \mathfrak{m}_{C^p} \mapsto \sum_n \frac{[a^{p^n}]}{p^n}.$$

We want to relate this one to the formal logarithm:

There is a bijection of sets $\mathfrak{m}_{C^p} \cong 1 + \mathfrak{m}_{C^p}$ that $\log([E(a)]) = T(a)$, which is defined by the **Artin-Hasse exponential**

$$E(x) = \prod_{(d,p)=1} \left( \frac{1}{1 - x^d} \right)^{\frac{\mu(d)}{d}}.$$

Proof: Firstly, it has coefficients in $\mathbb{Z}(p)$, because $(1 - x^d)^\frac{1}{d} = \sum(-1)^k C_k \frac{x^{kd}}{d}$ has coefficient in $\mathbb{Z}(p)$. And $[1 - x] = \lim_k(1 - [x^{p^{-k}}])^{p^k}$, so

$$\log\left( \prod_{(d,p)=1} \left( \frac{1}{1 - x^d} \right)^{\frac{\mu(d)}{d}} \right) = \sum_{(d,p)=1} \frac{\mu(d)}{d} \log(1 - \frac{1}{1 - d}) = \sum_{(d,p)=1} \frac{\mu(d)}{d} \sum_{a \in p^{-n} \mathbb{Z}} \left[ \frac{x^{da}}{a} \right]$$

Notice the right hand side stabilizes for any term $[x^\beta]$, and if $\beta \neq \frac{1}{p^r}$, it will vanish, thus for $x \in \mathfrak{m}_{C^p}$, it converges, and the sum equals $\sum_n \frac{[x^{p^n}]}{p^n}$. \hfill \Box

Cor. (14.9.1.18). The set of elements of the form $\sum_n \frac{[a^{p^n}]}{p^n}$ is closed under addition.

the Field $B_{df}$

Prop. (14.9.1.19)[Untilts with Roots of Unity]. Let $Q^{cyc}_p = Q_p(\mu_{p^n})$, and $\varepsilon = (1, \mu_p, \mu_{p^2}, \ldots)$ be a compatible $p^n$-th roots of unity that is an element of $(Q^{cyc}_p)^\varepsilon$. Then $\varepsilon - 1$ is a pseudo-uniformizer of $(Q^{cyc}_p)^\varepsilon$. For any untilts $K$ of $\mathbb{C}^p$ and an embedding of $Q^{cyc}_p$ in $K$, the tilting maps $\varepsilon - 1$ to a pseudo-uniformizer of $\mathbb{C}^p$. This induces a bijection:

$$\{\text{Untilts } (K,i) \text{ of } \mathbb{C}^p \text{ with an embedding } Q^{cyc}_p \hookrightarrow K \} \cong \{x \in \mathbb{C}^p | 0 < |x - 1| < 1\}.$$
Proof: In fact, the left hand side is equivalent to $K$ has a compatible $p^n$-th roots of unity, and we want to prove that for any $x$ in the right hand side, there is a unique untilts $K$ that $(x^p)^\xi$ is a compatible primitive roots of unity, and this is equivalent to $(x^\frac{1}{p})^\xi$ satisfies $1 + x + \ldots + x^{p-1} = 0$, and further equivalent to $\theta : A_{inf} \to \mathcal{O}_K$ annihilates $1 + [x^\frac{1}{p}] + \ldots + [x^{\frac{p-1}{p}}]$.

It suffices to show $\xi = 1 + [x^\frac{1}{p}] + \ldots + [x^{\frac{p-1}{p}}]$ is distinguished\(^{(14.9.1.5)}\). Let $\xi = \sum [c_n]p^n$, consider reducing to the residue field: $W(\mathcal{O}_{CS}) \to W(\mathcal{O}_{CS}/\mathfrak{m}_{CS})$, then $\pi = 1$, and $\xi = p$, thus $|c_0| < 1, |c_1 - 1| < 1$, so it is distinguished\(^{(4.5.4.20)}\).

\textbf{Cor. (14.9.1.20)} Considering different $p^n$-th roots of unities, there is a correspondence:

\[\{\text{Char 0 Untilts } (K, \iota) \text{ of } C^0 \text{ with a compatible } p^n \text{-th roots of unity}\} \cong \{x \in C^0 | 0 < |x-1| < 1\}/\mathbb{Z}_p^*,\]

where $\mathbb{Z}_p^*$ acts by exponentiation\(^{(10.3.8.8)}\).

Furthermore, there is a correspondence:

\[\{\text{Char 0 Untilts } (K, \iota) \text{ of } C^0 \text{ with a compatible } p^n \text{-th roots of unity}\}/\varphi_{CS} \cong \{x \in C^0 | 0 < |x-1| < 1\}/\mathbb{Q}_p^*,\]

where the inverse is given by $x \mapsto$ the vanishing locus of $\log([x]) \in B$.

\textbf{Proof:} The only thing needed to be proven is the inverse is given by $N(\log([x]))$. Notice for any untilts $K$, $[(x^{p^n})^\xi - 1] < |p|^{1/(p-1)}$ for $n$ large, then $\log((x^{p^n})^\xi) = 0 \iff (x^{p^n})^\xi = 1$ by Newton polygon. Now $x^\xi \neq 1$ because $x \neq 1$ and $\xi$ is injective. Hence composing $\varphi^n$ for some unique $n$, we can assume $x^\xi = 1, x^{\frac{1}{p}} \neq 1$, thus it corresponds an untilt as in\(^{(14.9.1.19)}\). \hfill $\Box$

\textbf{Def. (14.9.1.21)}\([B^+_dR]\). For an untilts $K$ of $C^0$ that corresponds to a distinguished element $\xi\(^{(14.9.1.5)}\)$, $p$ is not a zero-divisor in $A_{inf}/(\xi^n)$, as in the proof pf\(^{(14.9.1.4)}\), so we can define

\[B^+_dR = \lim_{n \to \infty} A_{inf}/(\xi^n)[p^{-1}]\]

\textbf{Prop. (14.9.1.22)} $B^+_dR$ is a complete discrete valuation ring with $\xi$ a uniformizer, and the residue field is isomorphic to $K$. Hence we can define $B_{dR}$ as the quotient field of $B^+_dR$.

\textbf{Proof:} Firstly $\xi$ is not a zero divisor in $B^+_dR$, because if $\xi x = 0, x = (x_n)$, then for any $n > 0$, and some $k$ that $p^k x_n \in A_{inf}/(\xi^n)$, so $p^k x_n$ is annihilated by $\xi$ in $A_{inf}/(\xi^n)$, thus $p^k x_n = \xi^{-1} y_n$ for some $y_n$, because $\xi$ is a non-zero-divisor in $A_{inf}/(\xi^n)$\(^{(14.9.1.4)}\). So $p^{n-1} x_{n-1} = 0 \in A_{inf}/(\xi^n)$, thus $x_{n-1} = 0$, because $p$ is non-zero-divisor in $A_{inf}/(\xi^n)$\(^{(14.9.1.4)}\).

Next there is a map $B^+_dR/(\xi^m) \to A_{inf}/(\xi^m)[p^{-1}]$. I claim this is an isomorphism: it is clearly a surjection, and if $x = (x_n)$ is mapped to 0, then for each $n \geq m$, we choose $p^n x_n = 0 \in A_{inf}/(\xi^n)$, then $p^n x_n = \xi^{-1} y_n$ for a unique $y_n \in A_{inf}/(\xi^n)$, so $x = \xi^m \cdot (\frac{y_n}{p^{n+1}}) \in \xi^m B_{dR}$. (Notice the uniqueness of $y_n$ shows $\frac{y_n}{p^{n+1}}$ is an element in $B^+_dR$).

Then it follows $B^+_dR \cong \lim_{\to \infty} B^+_dR/(\xi^m)$, which shows that $B^+_dR$ is $\xi$-adically complete, and $m = 1$ shows the residue field is equal to $K$. \hfill $\Box$

\textbf{Remark (14.9.1.23)} remark if $\xi = [t] - pu$, then $A_{inf}/(\xi^n)[p^{-1}] = A_{inf}/(\xi^n) [[t]^{-1}]$, so if $K$ is of char $p$, then $B^+_dR$ is just $W(C^0)$.

When $K$ is of char0, then $B_{dR}$ contains a field isomorphic to $K$ by??, thus $B^+_dR$ is (non-canonically) isomorphic to $K[[t]]$, and should be thought as the completed local ring at the point $y = (K, \iota)$.
Prop. (14.9.1.24) [The Stalk Map]. Notice $A_{\text{inf}} = \lim_{n \to \infty} A_{\text{inf}}/(\xi^n)$ by (14.9.1.4), thus there is a natural map $A_{\text{inf}} \to B_{dR}^+$, whose composition with $B_{dR}^+ \to B_{dR}^+/\xi \cong K$ maps $p, [t]$ to $p, t^e$, which shows they are invertible in $B_{dR}^+$, so there is a map

$$e : A_{\text{inf}}[\frac{1}{p}, \frac{1}{[t]}] \to B_{dR}^+.$$ 

In case $a \leq |p|_K \leq b$, this can be further extended to a map $e : B_{[a, b]} \to B_{dR}^+(\text{The stalk map}).$

**Proof:** It suffices to prove for $a = |p|_K = b$ because the topology is stronger. In this case, choose $t = p^b \in C^p$, then $|t|_{C^p} = |p|_K$, thus $\mathfrak{e}_n$ determined a map

$$A_{\text{inf}}[\frac{t}{p}, \frac{p}{[t]}] \to B_{dR}^+/(\xi^n) \cong (A_{\text{inf}}/(\xi^n))[p^{-1}],$$

It suffices to prove the image is contained in $p^{-k}(A_{\text{inf}}/(\xi^n))$ for some $k = k(n)$, because then $\mathfrak{e}_n$ is $p$-adically continuous, and extends to map of $B_{[a]} = (A_{\text{inf}}[\frac{t}{p}, \frac{p}{[t]}])_{p} \to (A_{\text{inf}}/(\xi^n))[p^{-1}]$, which is compatible w.r.t $n$, thus gives a map $B_{[a]} \to B_{dR}^+.$

For this, consider $f = \mathfrak{e}_n(\frac{t}{p}), g = \mathfrak{e}_n(\frac{p}{[t]})$, then their reduction under $B_{dR}^+/(\xi^n) \to B_{dR}^+/\xi \cong K$ is in $O_K \cong A_{\text{inf}}/(\xi)$, thus

$$f = f_1 + \frac{\xi}{p^e}f_2, \quad g = g_1 + \frac{\xi}{p^e}g_2$$

for $f_1, f_2, g_1, g_2 \in A_{\text{inf}}/(\xi^n)$ for some $c$. Then any

$$f^m = (f_1 + \frac{\xi}{p^e}f_2)^m = \sum_{i=0}^{n-1} C_m^i f_1^{m-i}(\frac{\xi}{p^e}f_2)^i \in p^{-nc}(A_{\text{inf}}/(\xi^n)).$$

Thus $\mathfrak{e}_n(A_{\text{inf}}[\frac{t}{p}, \frac{p}{[t]}]) \in p^{-nc}(A_{\text{inf}}/(\xi^n)).$ \hfill $\square$

**Cor. (14.9.1.25).** The stalk map $e : B_{[a, b]} \to B_{dR}^+$ composed with the map $B_{dR}^+/\xi \cong K$ are in fact equivalent to the valuation map (14.9.1.11).

## 2 Divisors

**Valuation Function**

Def. (14.9.2.1) [Exponential Valuation]. For any positive real number $s$, define a valuation on $A_{\text{inf}}[\frac{1}{p}, \frac{1}{[t]}]$ by the formula $v_s(f) = -\log |f|_{\text{exp}(-s)}$, then it is a valuation by (14.9.1.8).

If $f$ has a Teichmuller expansion $\sum_{n \to \infty} c_n p^n$, then

$$|f|_p = \sup \{|c_n|_{C^p} p^n\}, \quad v_s(f) = \inf \{v(c_n) + ns\}.$$ 

Prop. (14.9.2.2). For any $f \neq 0 \in A_{\text{inf}}[\frac{1}{p}, \frac{1}{[t]}], s \mapsto v_s(f)$ is a concave function in $s$ which is piecewise linear with integral slopes.

**Proof:** Consider the Newton Polygon. \hfill $\square$
Lemma (14.9.2.3). If \( s > 0 \) and \( f_n \) is a Cauchy sequence in \( \mathcal{A}_{\text{inf}}[\frac{1}{p}, \frac{1}{p}] \) for the norm \( |\cdot|_{\exp(-s)} \) and doesn’t converge to 0, then the sequences
\[
|v_s(f_n), \, \partial_{-}v_s(f_n), \, \partial_{+}v_s(f_n) |
\]
stabilize.

Proof: Easy. Cf.[If Curve Lurie P44].

Prop. (14.9.2.4). If \( 0 < a \leq b < 1 \), and \( f_n \) is a Cauchy sequence in \( \mathcal{A}_{\text{inf}}[\frac{1}{p}, \frac{1}{p}] \) and doesn’t converge to 0 for either the norm \( |\cdot|_{a} \) or \( |\cdot|_{b} \), then the sequence of functions \( s \mapsto v_s(f) \) stabilizes on \( [-\log(b), -\log(a)] \).

Proof: Suppose \( f_n \) doesn’t converge to 0 for the form \( |\cdot|_{b} \), then by (14.9.2.3), the sequences \( v_s(f_n), \partial_{+}v_s(f_n) \) converges, thus \( v_s(f_n) \) is bounded uniformly, thus \( v_s(f) \) is bounded.

Then choose \( N \) large that \( |f-f_m|_{\rho} \) very small for any \( m > N \) and \( a \leq \rho \leq b \), then \( v_s(f) = v_s(f_m) \) for any \( a \leq s \leq b \), thus it stabilizes.

Cor. (14.9.2.5). Let \( f \) be a non-zero element in \( B \), then the construction \( s \mapsto v_s(f) \) is a concave function in \( s \) with piecewise linear function with integral slopes. This is analogous to the Hadamard three circle theorem (10.5.6.11).

Proof: This is true for \( f \in B_{[a,b]} \), because any \( f \) is a limit of a sequence \( f_n \) in both the norm \( |\cdot|_{a} \) and \( |\cdot|_{b} \), so by the proposition, there for \( n \) large, \( v_s(f) = v_s(f_n) \) on \( [-\log(b), -\log(a)] \), thus the conclusion is true by (14.9.2.2). And for \( f \in B \), for any interval \( [a, b] \) we can do the same, thus the conclusion is true on each interval, thus it is true.

Metric Structures on \( Y \)

Def. (14.9.2.6) [Metric on \( \overline{Y} \)]. Let \( \overline{Y} = Y \cup \{0\} \) be the isomorphism classes of untilts of \( C^0 \), where 0 corresponds to \( C^0 \) itself.

(14.9.1.5) show \( \overline{Y} \) corresponds to distinguished elements in \( \mathcal{A}_{\text{inf}} \) up to units. So for any \( x, y \in \overline{Y} \), we let \( d(x, y) = |\xi_x(y)|_{K_y} \leq 1 \). Then this is a metric, it is an non-Archimedean.

Proof: Firstly, if \( d(x, y) = 0 \), then \( \xi_x \) divides \( \xi_y \), which is equivalent to \( (\xi_x) = (\xi_y) \), by (4.5.4.21).

Secondly, for any \( x, y \), since \( C^0 \) is alg. closed, we can assume \( \xi_x(y) = c^x \) for some \( c \in C^0 \). Notice \( \xi(y) = t^2 + pu(y) \) is in \( m_K \), thus \( c \in m_{C^0} \). So \( \xi_x - [c] \) is also a distinguished element and vanishes at \( y \), so we may assume that \( \xi_y = \xi_x - [c] \) by (4.5.4.21) again. Then
\[
d(y, x) = |\xi_y(x)|_{K_x} = |c^x|_{K_x} = |c|_{C^0} = |c^x|_{K_y} = d(x, y).
\]

Finally it is non-Archimedean because any valuation field \( K \) is non-Archimedean.

Prop. (14.9.2.7) [\( \overline{Y} \) is Complete]. \( \overline{Y} \) is complete w.r.t this metric.

Proof: Given a Cauchy sequence of points \( y_n \) in \( \overline{Y} \), as in the proof of (14.9.2.6), we can assume that \( \xi_{y_n} = \xi_{y_{n-1}} + [c_n] \) for some \( c_n \in m_{C^0} \), and \( |c_n|_{C^0} = d(y_{n-1}, y_n) \). Now \( \mathcal{A}_{\text{inf}} \) is \([t]\)-adically complete for a uniformizer \( t \in C^0 \), thus \( \sum |c_n| \) is definable in \( \mathcal{A}_{\text{inf}} \), and \( \xi = \xi_0 + \sum |c_n| \) is also distinguished, and corresponds to a point \( y \) which \( y_n \) clearly converges to.
14.9. FARQUES-FONTAINE CURVE

Divisors

Lemma (14.9.2.8) $B_{[a,b]}$ is an integral domain.

Proof: By (14.9.2.5), the valuation function $v_s(f)$ and $v_s(g)$ are bounded, thus it is clear that $v_s(fg)$ is also finite, so $fg \neq 0$. □

Prop. (14.9.2.9) [Divisors] Assume $C^\flat$ is alg. closed, then for any $f \in B_{[a,b]}$ and $y = (K, \ell) \in Y_{[a,b]}$, we define the **order of vanishing** $\text{ord}_K(f) \in \mathbb{Z} \cup \{\infty\}$ as the valuation of $e_K(f) \in B_{dR}^+(K)$, then

- if $f \neq 0 \in B_{[a,b]}$, then $\text{ord}_K(f) < \infty$ for each $K \in Y_{[a,b]}$, and there are only f.m. $K$ that $\text{ord}_K(f) \neq 0$. In particular, $B_{[a,b]}$ is an integral domain.

- if $x, y \neq 0 \in B_{[a,b]}$, then $x$ divides $y$ iff $\text{ord}_K(x) \geq \text{ord}_K(y)$ for each $K \in Y_{[a,b]}$. Thus for each $f \in B_{[a,b]}$, we can define the **divisor** of $K$ as the formal sum $\sum_{K \in Y_{[a,b]}} \text{ord}_K(f) K$, and this is also definable for $f \in B$, but it may be an infinite but locally finite sum.

Proof: Firstly, by (14.9.2.13) and (14.9.2.14), if $\text{div}(f) \cap Y_{[a,b]} \neq 0$, then there is a distinguished element $\xi$ at $f = \xi f_1$. And we can iterate this, and eventually end up with $f = \xi_1 \ldots \xi_n f_n$ that $\text{div}(f_n) \cap Y_{[a,b]} = 0$, by (14.9.2.15), so by (14.9.2.16), $f_n$ is invertible in $f$, so $\text{div}(f)$ is finite. And if $\text{div}(g) \geq \text{div}(f)$, then $g$ also divides $\xi_1 \ldots \xi_n$, so $g$ divides $f$. □

Remark (14.9.2.10). Notice by (14.9.1.25), for a $f \in B_{[a,b]}$, $\text{ord}_K(f) > 0$ iff $f(y) = 0 \in K$.

Cor. (14.9.2.11) [$B$ is Integral Domain]. $B$ is an integral domain, and if $C^\flat$ is alg. closed, then $x$ is divisible by $y$ if and only if $\text{div}(x) \geq \text{div}(y)$.

Cor. (14.9.2.12). $B$ is integrally closed.

Proof: $B$ is an integral domain by (14.9.2.11), it is integrally closed because if $f/g$ is integral over $B$, then there image in $B_{dR}^+(y)$ is integral over $B_{dR}^+(y)$ for all $y \in Y$, thus in $B_{dR}^+(y)$ because it is a valuation ring, and then $f$ is divisible by $g$ by (14.9.2.11). □

Prop. (14.9.2.13) [Examples of Divisors].

- For a distinguished element $\xi$, if $\xi = u_p$, then $\xi$ is invertible in $B$, thus $\text{div}(\xi) = 0$. Otherwise $\xi$ defines a char0 untilts $K$ of $C^\flat$, and $\xi$ is a uniformizer of $B_{dR}^+(K)$, and it doesn’t divides other distinguished elements (4.5.4.21), thus $\text{div}(\xi) = K$.

- $\text{div}(\log([x])) = \sum_{n \in \mathbb{Z}} \varphi(n)(K)$.

Proof: 2: $\log([x])$ vanishes at a single $\varphi$-orbits of $Y$, and one of them is given by the distinguished element $\xi = 1 + [x^{1/p}] + \ldots + [x^{(p-1)/p}] = \frac{[x]^{p-1}}{[x]^{p-1}}$. Notice $[x^{1/p}] - 1$ is mapped to an invertible element in $K$, thus it is invertible in $B_{dR}^+(K)$, so $[x] - 1$ is associated to $\xi$, and notice

$$\log([x]) = \sum_{k>0} \frac{(-1)^{k+1}}{k} ([x] - 1)^k \equiv [x] - 1 \ mod \ ([x] - 1)^2,$$

so $\text{ord}_K(\log([x])) = 1$, and because $\varphi(\log([x])) = p \log([x])$, $\text{ord}_{\varphi^a(K)}(\log([x])) = 1$ for any $n$, so we are done. □

Lemma (14.9.2.14). Let $C^\flat$ be alg. closed. If $\xi$ is a distinguished element of $A_{\text{inf}}$ vanishes at a point $y \in Y_{[a,b]}$ and $g \in B_{[a,b]}$ also vanishes at $y$, then $g$ is divisible by $\xi$ in $B_{[a,b]}$. 

Proof: If \( g \in A_{\inf}([\frac{1}{p}, \frac{1}{|p|}]) \), then this is easy by (14.9.2.10) and \( A_{\inf}/(\xi) = O_K(14.9.1.4) \).

Now generally \( g \) is a limit of \( g_n \in A_{\inf}([\frac{1}{p}, \frac{1}{|p|}]) \), so \( g(y) \) is the limit of \( g_n(y) \in K \). Now \( g(y) = 0 \), so \( \lim_n g_n(y) = 0 \). Now \( K \) is alg.closed by (10.3.8.15), so we can let \( g_n(y) = c_n \), so \( c_i \) converges to 0 in \( C^\circ \). So \( \{c_n\} \) converges to 0 in norm \( |\cdot|_a \) and \( |\cdot|_b \), so we can replace \( g_n \) by \( g_n - [c_n] \) and assume \( g_n(y) = 0 \).

Now the first part shows \( g_n = \xi h_i \), and now \( h_i \) is a Cauchy sequence for both \( |\cdot|_a \) and \( |\cdot|_b \), so converges to some \( h \), and then \( g = \xi h \). \( \square \)

Lemma (14.9.2.15). Given this lemma (14.9.2.14), we have a strategy of proving (14.9.2.9), that is, decomposing \( f, g \) into distinguished elements, but we need to show this decomposition is finite. And this is true:

If \( f \neq 0 \in B_{[a,b]} \), denote \( \beta = -\log(b) \), \( \alpha = -\log(a) \) and let \( N = \partial_- v_\beta(f) - \partial_+ v_\alpha(f) \geq 0 \), then \( f \) cannot be divisible by a product of \( \xi_1, \ldots, \xi_{N+1} \) of \( N + 1 \) distinguished elements.

Proof: By (4.5.4.20), if \( \xi \) is distinguished, then \( v_\xi(\xi) = \max\{s, v(v_0)\} \). Now \( v(v_0) = v(t^2) = v(|p|_K) \) in \( O_K = A_{\inf}/(|t| - u_p) \), so if \( K \) corresponding to \( \xi \) belongs to \( Y_{[a,b]} \), then \( v(v_0) \in [\beta, \alpha] \), so \( \partial_- v_\beta(\xi) = 1, \partial_+ v_\alpha(\xi) = 0 \).

So if \( f = \xi_1, \ldots, \xi_{N+1} u \), then \( N(f) \geq \sum N(\xi_i) \geq N + 1 \). \( \square \)

Lemma (14.9.2.16) [Valuation Functon And Invertibility]. Let \( C^\circ \) be alg.closed and \( f \neq 0 \in B_{[a,b]} \), then the following are equivalent:

- \( f \) is invertible.
- \( \partial_- v_\beta(f) = \partial_+ v_\alpha(f) \).
- \( \text{div}(f) \cap Y_{[a,b]} = \varnothing \).

Proof: \( 2 \rightarrow 3 \) by (14.9.2.15).

1 \( \rightarrow \) 2: Because \( N(f) + N(f^{-1}) = 0 \), and \( N(f) \geq 0, N(f^{-1}) \geq 0 \), so \( N(f) = 0 \).

2 \( \rightarrow \) 1: Assume first that \( f = \sum_{n > n_0} c_n p^n \in A_{\inf}([\frac{1}{p}, \frac{1}{|p|}]) \), then the hypotheses just says that \( s \rightarrow v_\alpha(f) \) is linear in a small nbhd of \([\beta, \alpha] \); that is, there is a \( n_0 \) that \( v(c_n) + ns > v(c_{n_0}) + n_0 s \) for all \( n \neq n_0 \) and \( s \in [\beta, \alpha] \).

Now we can normalize \( f \) that \( n_0 = 0 \) and \( c_0 = 1 \), so \( |f - 1|_{\rho} < 1 \) for all \( \rho \in [\beta, \alpha] \), so \( f - 1 \) is topologically nilpotent in \( B_{[a,b]} \), and thus \( f \) is invertible.

Generally, \( f \) is a limit of a sequence \( f_n \in A_{\inf}([\frac{1}{p}, \frac{1}{|p|}]) \), and by (14.9.2.4) we can assume the hypothesis holds for all \( f_n \). Then \( f_n \) is invertible, and it is easily shown that \( f_n^{-1} \) is a Cauchy sequence in \( B_{[a,b]} \), so converges to some \( f^{-1} \).

3 \( \rightarrow \) 2: Firstly, if \( \partial_- v_\beta(f) > \partial_+ v_\alpha(f) \), then we must have \( \partial_- v_\rho(f) > \partial_+ v_\rho(f) \) for some \( s \), so wlog, we can assume \( a = b = s \), and we need to show \( f \) vanishes at some point in \( Y_{exp(s)} \). Now combining with (14.9.2.14) and (14.9.2.15), this is equivalent to another statement that any element \( y \in B_{[\rho, \rho]} \) has a decomposition \( y = c_1 \ldots c_n \) where \( c_i \) corresponds to points in \( Y_{\rho} \), and \( g \) is invertible in \( B_{\rho} \). The proof is finished at (14.9.2.26). \( \square \)

Primitive Elements and the Proof of 3 \( \rightarrow \) 2 of The Lemma on Valuation Function and Invertibility

Def. (14.9.2.17). Let \( C^\circ \) be alg.closed, an element in \( B_{[\rho, \rho]} \) is called good iff it has a decomposition as in the proof of 3 \( \rightarrow \) 2 of (14.9.2.16).
Prop. (14.9.2.18) [Approximating Zero]. If \( f \) is a good element having \( n \)-zeros on \( Y_\rho \), and \( g \in B_\rho \) that \( |f - g|_\rho < |f|_\rho \), then for any zero \( y \) of \( g \) on \( Y_\rho \), there exists a zero \( y' \) of \( f \) on \( Y_\rho \) that \( d(y'; y) < \rho(\frac{|f-g|_\rho}{|f|_\rho})^{1/n} \).

Proof: \( |f - g|_\rho \geq |(f - g)(y)|_K = |f(y)|_K \). Now \( f = g\xi_1 \ldots \xi_n \), and \( \xi \) corresponds to \( y_i \), then

\[
|f(y)|_K = |g(y)|_K|\xi_1(y)|_K \ldots |\xi_n(y)|_K = |f|_\rho \prod_i |\xi_i|_\rho d(y_i, y) = |f|_\rho \prod_i \frac{d(y_i, y)}{\rho}.
\]

(Notice \( |g\rho| = |g(y)|_K \) because \( g \) is invertible(14.9.1.10)) and \( d(y_i, y) \leq \rho \). So at least one \( \xi \) satisfies the desired inequality. \( \square \)

Cor. (14.9.2.19). If \( f \in B_\rho \) is given by a Cauchy sequence of good elements, and \( \partial_- v_\rho(f) > \partial_+ v_\rho(f) \), then \( f \) has a root on \( Y_\rho \).

Proof: By (14.9.2.3), passing to a subsequence, we may assume

\[
v_s(f) = v_s(f_n), \quad \partial_- v_s(f) = \partial_- v_s(f_n), \quad \partial_+ v_s(f) = \partial_+ v_s(f_n), \quad |f_{n+1} - f_n|_\rho < |f|_\rho.
\]

Let \( n = \partial_- v_s(f) - \partial_+ v_s(f) > 0 \), then each \( f_i \) has exactly \( n \) roots on \( Y_\rho \), and applying (14.9.2.18), we can find successively roots \( y_n \) of \( f_n \) that \( d(y_{n+1}, y_n) \leq \rho(\frac{|f_{n+1} - f_n|_\rho}{|f|_\rho})^{1/n} \), so the sequence \( \{y_n\} \) is Cauchy and converges to some point \( y \in Y \), so

\[
|f(y)|_K \leq |f|_\rho \frac{d(y_i, y)}{\rho} \to 0.
\]

so \( f(y) = 0 \). \( \square \)

Def. (14.9.2.20) [Primitive Elements]. An element \( f = \sum_{n \geq 0}[c_n]p^n \in A_{inf} \) is called primitive of degree \( d \) if \( c_0 \neq 0 \), \( |c_d| = 1 \) for some smallest element \( d \).

Clearly an element is distinguished of degree 1 iff it is distinguished and corresponds to an untilts of \( X^0 \) of char0.

Prop. (14.9.2.21).

- Any element \( f \in A_{inf} \) of finite Teichmuller expansion can be written uniquely as \( f = p^m[c]g \), where \( c \in C^b \) and \( g \) is primitive.
- For an element \( f \in A_{inf}[\frac{1}{p}, \frac{1}{m}] \), \( f \) can be written as \( p^m[c]g \) iff \( v_s(f) \) consists of f.m. line segments iff sup\(\{c_n\}\) is achieved by some \( n \).
- If \( f = gh \) in \( A_{inf} \) is primitive, then \( g, h \) are also primitive, and \( \deg(f) = \deg(g) + \deg(h) \).

Prop. (14.9.2.22). Let \( f = \sum[c_n]p^n \in A_{inf} \) be primitive of degree \( d > 0 \), and let \( \lambda \in (0, 1) \) be the number that \( s = -\log(\lambda) \) is the minimal number that \( v_s(f) \) is non-differentiable at, i.e. \( s \) is \(-1\) times the slope of the line segment on the left of \( v(c_d) \). Then \( f \) has a zero on \( Y_\lambda \).

Proof: By (14.9.2.23) there is a \( y \in Y_\lambda \) that \( |f(\lambda)| \leq \lambda^{d-1} \), and then (14.9.2.24) shows we can find successively \( y_n \) that

\[
d(y_n, y_{n+1}) \leq \lambda^{1+\frac{d}{n}}, \quad |f(\lambda)| \leq \lambda^{d+m}.
\]

So \( y_n \) is a Cauchy sequence thus converges to some \( y \), and then \( f(y) = 0 \). \( \square \)
Lemma (14.9.2.23) [Lemma for Approaching a Zero]. If $C^\circ$ is alg. closed and $f \in A_{\text{inf}}$ is primitive of degree $d > 0$, and let $\lambda$ as in (14.9.2.22), then there is a point $y \in Y_\lambda$ that $|f(y)|_{K_y} \leq \lambda^{d+1}$.

Proof: Let $f = \sum [c_n]p^n$, we may assume $c_d = 1$, and let $F = x^d + c_{d-1}x^{d-1} + \ldots + c_0$, then the largest valuation of the roots of $F$ on $C^\circ$ is $\lambda$, by Newton polygon. Let $r$ be such a root, then $c_i$ is divisible by $r^{d-i}$, and let $\xi = p - [r]$ be a distinguished element of $A_{\text{inf}}$ and corresponds to an until $K$, then $|p|_K = \lambda$, and

$$p^{-d}f(y) = \sum_{n \geq 0} c_n p^{n-d} = \sum_{i=0}^d (\frac{c_i}{r^{d-i}})^\# \mod p = (r^{-d}F(r)) \mod p = 0$$

thus $f(y)$ is divisible by $p^{d+1}$, which is equivalent to $|f(y)|_K \leq \lambda^{d+1}$.

Lemma (14.9.2.24) [Lemma for Approaching a Zero]. Situation as in (14.9.2.23), if $y \in Y_\lambda$ and $|f(y)| = \lambda^d \cdot \alpha$, then there is a $y'$ that $d(y,y') \leq \lambda \cdot \alpha^{1/d}$ that $|f(y')| \leq \lambda^{d+1}\alpha$.

Proof: Since $A_{\text{inf}}$ is $\xi$-complete and every element of $A_{\text{inf}}/\xi \cong \mathcal{O}_K$ belongs to the image of $\xi : \mathcal{O}_C \to \mathcal{O}_K$, thus by induction, we can write $f = \sum_{n \geq 0} [c_n] \xi^n$. Because $f$ is primitive of degree $d$, we may assume $c_d = 1$, and $|c_0|_{C^\circ} = |f(y)|_K = \lambda^d \alpha$.

Let $F(x) = c_0 + c_1 x + \ldots + c_{d-1} x^{d-1} + x^d$, because $C^\circ$ is alg. closed, let $r$ be a root of minimal absolute value, then $|r|_{C^\circ}^{n} |c_m|_{C^\circ} \leq \lambda^n \alpha^n$, in particular $|r|_{C^\circ} \leq \lambda^{1/n}$. So let $\xi' = \xi - [r]$, then $\xi$ is also distinguished, and $d(y',y) = |r|_{C^\circ} \leq \lambda \alpha^{1/n}$ (14.9.2.6), and $d(0,y') = \lambda$, and $\xi(y') = r^\#$.

Now

$$\frac{\langle f(y') \rangle_{c_0}^\#}{\xi_0^\#} = \sum_{n \geq 0} \frac{c_0^\#}{c_0^\#} \xi(y')^n = \sum_{n \geq 0} \left(\frac{c_n r^n}{c_0}\right)^\# \equiv \sum_{i=0}^n \left(\frac{c_n r^n}{c_0}\right)^\# \mod p = \left(\frac{F(r)}{c_0}\right)^\# = 0,$$

So $|f(y')|_{K'} \leq |c_0|_{K'} |p|_{K'} = |c_0|_{C^\circ} \lambda = \lambda^{d+1}\alpha$.

Cor. (14.9.2.25) [Primitive Elements Decompose as Distinguished Elements]. If $f \in A_{\text{inf}}$ is a primitive element of degree $d > 0$, then $f$ admits a factorization as products of distinguished elements $\xi$ corresponding to points in $Y$.

Proof: Use induction on $d$. If $d = 1$, then $f$ is distinguished by (14.9.2.20), and if $d > 1$, then by (14.9.2.22), $f = \xi g$, so $g$ is primitive of degree $d - 1$ by (14.9.2.21), so induction is finished.

Prop. (14.9.2.26) [Finite Teichmüller Expansion is Good]. Any element of finite Teichmüller expansion is good.

In particular, because any element of $B_\rho$ can be approximated by elements in $A_{\text{inf}}[\frac{1}{p}, \frac{1}{|\bar{g}|}]$, and such element can be approximated by elements of finite Teichmüller expansion, by (14.9.2.19), we finishes the proof of 3 $\to$ 2 of (14.9.2.16).

Proof: If $f$ has finite Teichmüller expansion, then $f = p^m [c_0] g$, where $g$ is primitive of degree $d$. If $d = 0$, then $g$ is invertible in $A_{\text{inf}}$, thus $f$ is invertible in $B_\rho$. Otherwise, we can use (14.9.2.25) to factorize $g$ into distinguished elements, and the elements that corresponds to points outside $Y_\rho$ is invertible in $B_\rho$ because $v_s(\xi) = \max \{s, v(v_0)\}$ and $2 \to 1$ of (14.9.2.16), so $f$ is good.
14.9. FARGUES-FONTAINE CURVE 1417

Bounded Meromorphic Functions

Prop. (14.9.2.27). If \( f \in B \), then \( f \in A_{\inf} \iff |f|_\rho \leq 1 \) for any \( 0 < \rho < 1 \).

Easily we can get characterization of \( f \) being in \( A_{\inf}[\frac{1}{p^k}], A_{\inf}[\frac{1}{p^l}] \) or \( A_{\inf}[\frac{1}{p^k}, \frac{1}{p^l}] \).

Proof: One direction is trivial, for the other, by (14.9.2.28), we can find successively \( f_n \) that \( f = \sum_{i<n} |c_i| p^i + f_n \), and \( |f_n|_\rho \leq \rho^n \) for all \( 0 < \rho < 1 \). So \( f_n \) converges to 0 in any norm \( \rho \), thus it converges to 0 in \( B \), and \( f = \sum_{n\geq 0} |c_n| p^n \in A_{\inf} \).

\( \square \)

Lemma (14.9.2.28). If \( f \in B \) satisfies \( |f|_\rho \leq \rho^n \) for all \( 0 < \rho < 1 \), then there is a \( c \in O_{C^0} \) that \( f = [c] p^n + g \) that \( |g|_\rho \leq \rho^{n+1} \) for all \( 0 < \rho < 1 \).

Proof: Replace \( f \) by \( \frac{f}{p^n} \), we may assume \( m = 0 \). Choose a sequence \( f_i \) in \( A_{\inf}[\frac{1}{p^k}, \frac{1}{p^l}] \) converging to \( f \) in \( B \), where \( f_i = \sum_{n>\infty} |c_{n,i}| p^n \).

Firstly we want to truncate \( f_i \) with the positive part \( f_i^+ \). Notice for each \( \rho \) and any \( 0 < \varepsilon < 1 \), because \( \lim |f_i - f|_\rho = 0 \), thus for \( i \) large, \( |f_i|_\rho = |f|_\rho \leq 1 \), thus \( |c_{-n,i}| c^{n+1} \rho^{-n} \leq \varepsilon^n < \varepsilon < \varepsilon \), so \( |f_i - f|^+ < \rho \) for \( i \) large, so \( f_i^+ = f \) also in \( B \).

Secondly, \( |c_{0,i} - c_{0,j}| c^n \leq |f_i - f_j|_\rho \) for each \( \rho \), thus \( c_{0,i} \) is Cauchy in \( C^0 \) thus converges to some \( c \in C^0 \), and when \( i \) is large, \( |c_{i,1} - c|_\rho = |f_i|_\rho \leq 1 \), so \( c \in O_{C^0} \). Now let \( g_i = \sum_{n>0} |c_{n,i}| p^n \), then \( g_i \) is also Cauchy in \( B \) for any norm \( |\cdot| \) and converges to some \( g \), and \( f = g + [c] \).

It’s left to check \( |g|_\rho \leq \rho \): each \( v_s(g_i) \) has positive slopes, then so does \( v_s(g) \) because by (14.9.2.3), \( v_s(g_i) \) stabilizes to \( v_s(g) \) uniformly on compact intervals. So if \( v_s(g) < s - \varepsilon \) for some \( s \), then \( v_s(g) \leq v_s(g) - (s - \varepsilon) < 0 \), but this cannot happen because \( v_s(g) \leq \max \{v_s(f), -\log |c|_{C^0} \} \geq 0 \).

Eigenspaces of Frobenius

Prop. (14.9.2.29).

- The vector space \( B^{p^n} \) vanish for \( n < 0 \).
- The canonical map \( Q_\rho \to B^{p}\id \) is an isomorphism.

Proof: 1: Consider \( v_{ps}(\varphi(f)) = pv_s(f)(14.9.1.14) \), \( v_s(p^n f) = ns + v_s(f) \), so if \( \varphi(f) = p^n f \), then \( pv_{s/p}(f) = v_s(\varphi(f)) = v_s(p^n f) = ns + v_s(f) \).

Let \( h(s) = \partial_+ v_s(f) \), then \( h(s/p) = n + h(s) \), but \( h \) must by non-increasing(14.9.2.2), so \( n \geq 0 \).

2: Firstly we prove \( B^{p}\id \) is a field: by (14.9.2.11), it suffices to show that \( \text{div}(f) = 0 \) for \( f \neq 0 \in B^{p}\id \). If \( \text{div}(f) \neq 0 \), because \( f \) is fixed by \( \varphi \), so \( \text{div}(f) \geq \sum_{\nu \in \mathbb{Z}} \varphi^{\nu}(y) \) for some \( y \), and \( \sum_{\nu \in \mathbb{Z}} \varphi^{\nu}(y) = \text{div}(\log(|\varepsilon|)) \) for some \( \varepsilon \in 1 + m_{C^0} \) because \( K \) is alg.closed and by (14.9.1.20). So by (14.9.2.11) again \( f = g \log(|\varepsilon|) \), and \( g \in B^{p^{-1}} \) by (14.9.1.16), then \( g = 0 \) by item1.

3: From (14.9.2.30) and (14.9.2.27), \( f \in A_{\inf}[\frac{1}{p^k}] \), thus \( f = \sum_{n>\infty} |c_n| p^n \), so \( \varphi(f) = f \) shows \( c_n = c_n \), which is equivalent to \( c_n \in E_p \). So \( f \in W(E_p)[\frac{1}{p}] = Q_\rho \).

\( \square \)

Lemma (14.9.2.30). If \( f \neq 0 \in B^{p}\id \), then there is an integer \( n \) that \( |f|_\rho = \rho^n \).

Proof: Notice \( |f|_\rho = |\varphi(f)|_\rho = |f|_\rho \), so \( v_{ps}(f) = pv_s(f) \), differentiation shows that \( \partial_- v_{ps}(f) = \partial_- v_s(f) \). This is for all \( s < 0 \), and \( \partial_- v_s(f) \) is non-decreasing, thus it is constant, and \( v_{ps}(f) = pv_s(f) \) shows \( v_s(f) = ns \) for some integer \( n \).

\( \square \)

Cor. (14.9.2.31). For \( n \geq 0 \), any element \( f \in B^{p^n} \) factors uniquely up to action of \( \Omega^\rho \) as \( \lambda \log(|\varepsilon_1|) \cdots \log(|\varepsilon_n|) \) where \( \lambda \in B^{p\id} \), \( 0 < |\varepsilon_i - 1| < 1 \).
Proof: The existence is by (14.9.2.26)
For the uniqueness: it suffices to prove \( \log([\varepsilon]) \) is a prime element in \( \oplus_{n \geq 0} B^{\varphi=p^n} \). For this, notice for any \( f \in B^{\varphi=p^n} \), \( \text{div} (f) \) is fixed by \( \varphi \), and \( \text{div} (\log([\varepsilon])) \) is a single orbit of \( \varphi \), thus by (14.9.2.11), if \( \log([\varepsilon]) \) divides \( fg \), then \( \log([\varepsilon]) \) divides \( f \) or \( g \).

Applications

Cor. (14.9.2.32). If \( C^\varphi \) is alg.closed, then every untilts \( K \) of \( C^\varphi \) belongs to the vanishing locus of \( \log([x]) \) for some \( x \in C^\varphi \) that \( 0 < |x - 1| < 1 \), and the map
\[
\psi : 1 + m_{C^\varphi} \to K : y \mapsto \log(y^\varphi)
\]

is surjective with kernel generated by \( x \) (as a \( \mathbb{Q}_p \)-subspace of \( 1 + m_{C^\varphi} \)).

Proof: By (10.3.8.15), any untilts of \( C^\varphi \) is alg.closed, thus it has a compatible \( p^n \)-th roots of unity. So it belongs to some locus of \( \log([x]) \) by (14.9.1.20). Now if \( |z| < |p|^{1/(p-1)} \), then \( z = \log(\exp(z)) \), and \( \exp = y^\varphi \) for some \( y \) because \( K \) is alg.closed. So \( \psi \) contains sufficiently small elements, but it is a map of \( \mathbb{Q}_p \)-vector spaces, thus it is surjective. For the kernel, if \( \log(y^\varphi) = 0 \), then \( \log([y]) \) vanish on \( K \), thus by (14.9.1.20), \( y, x \) is in the same \( \mathbb{Q}_p \)-vector space.

Cor. (14.9.2.33). If \( C^\varphi \) is alg.closed, then the map
\[
1 + m_{C^\varphi} \xrightarrow{\log([x])} B^{\varphi=p}
\]
is an isomorphism.

Proof: Firstly any untilts of \( C^\varphi \) is alg.closed by (10.3.8.15). It is injective because of the correspondence (14.9.1.20), and for the surjectivity, for each \( f \in B^{\varphi=\text{id}} \), if \( f = 0 \), then \( f = \log([1]) \), and if \( f \neq 0 \), then notice \( \text{div}(f) \neq \emptyset \), because in this case \( f \) is invertible in \( B \) by (14.9.2.11), thus \( f^{-1} \in B^{\varphi=p^{-1}} \), so \( f^{-1} = 0 \) by (14.9.2.29), contradiction.

Now if \( \text{ord}_K(f) \geq 1 \), then \( \text{ord}_{\varphi^n(K)}(f) \geq 1 \) for any \( n \in \mathbb{Z} \) since \( \varphi(f) = pf \). Consider \( \text{div} (\log([x])) = \sum_{n \in \mathbb{Z}} \varphi^n(K)(14.9.2.13) \), then \( f \) is divisible by \( \log([x]) \) by (14.9.2.11), \( f = \log([x])g \), then \( g \in B^{\varphi=\text{id}} \), so \( g \in \mathbb{Q}_p \) by (14.9.2.29), thus \( f = \log([x^g]) \).

Cor. (14.9.2.34) [Filtration on \( B_{dR} \)]. By (14.9.2.13) and (14.9.2.32), we see that for any untilt \( K \) of \( C^\varphi \), there is a unique up to \( \mathbb{Q}_p \)-constant \( \varepsilon \) that \( t = \log([\varepsilon]) \) is the uniformizer of \( B_{dR}(y) \). In fact, this \( \varepsilon \) can be to be \( \varepsilon = (1, \xi_p, \ldots, x_p, \ldots) \), where \( \xi_p \) is a compatible roots of unity in the alg.closed field \( K \).

Now we prefer to use the filtration \( Fil^n = t^{-n}B_{dR}^+ \) on \( B_{dR} \) because it is \( G_{\mathbb{Q}_p} \) invariant, as \( \varepsilon \) does.

Prop. (14.9.2.35). Let \( C^\varphi \) be alg.closed, then any point \( x \) of the Fargues-Fontaine curve \( X_{FF} \) that is not the generic point corresponds to the prime \( x_K = (\log([\varepsilon]))(14.9.2.31) \) where \( K \in \text{div}(\log([\varepsilon]))(14.9.2.32) \). And the residue field of \( x_K \) can be identified to \( K \).

Proof: By (14.9.2.31), we can cover \( X_{FF} \) by affine schemes of the form \( \text{Spec}(R_f = B[f^{-1}]^{\varphi=\text{id}}) \) for \( f \in B^{\varphi=p} \), now for any prime \( p \subset R_f \), let \( \frac{g}{f^\lambda} \in p \), then \( g = \lambda \log([\varepsilon_1]) \ldots \log([\varepsilon_n]) \), thus some \( \frac{\log([\varepsilon])}{f} \in p \). Let \( K \) be a point that \( \log([\varepsilon]) \) vanish(14.9.1.20), then we claim \( (\log([\varepsilon])/f) \) is maximal.

In fact, we may assume \( f \) doesn’t vanish on \( K \), otherwise \( \log([\varepsilon])/f \) is a unit, then there is a map \( \rho : B[f^{-1}]^{\varphi=1} \subset B[f^{-1}] \to K \), and this map is surjective with kernel \( \log([\varepsilon])/f \): it is surjective even on \( f^{-1}B^{\varphi=p} \) by (14.9.2.32), and if \( \log([\varepsilon_1])/f \) is mapped to 0, then \( \log([\varepsilon_1]) \) differs from \( \log([\varepsilon]) \) by some \( Q^*_p \) by (14.9.1.20).
Cor. (14.9.2.36). If \( C \) is alg.closed, there is a bijection of sets:
\[
Y \rightarrow \varphi_C^{Z} \cong \{ \text{Closed points of } X_{FF} \}.
\]
by (14.9.1.20).

Cor. (14.9.2.37). \( X_{FF} \) is a Dedekind scheme (5.4.2.13).

**Proof:** Let \( \text{Spec}(\mathbb{R}) = B[F^{−1}[\varphi]=id] \), two elements \( f = \log([\varepsilon]), g = \log([\mu]) \) can cover it. The proof of (14.9.2.35) shows that every prime ideals of \( R_f \) is maximal principal, in particular f.g, thus by (4.1.1.47), it is Noetherian. And it has Krull dimension 1 and it is regular because all of its maximal ideals are principal, hence normal (4.3.5.32). So \( X_{FF} \) is a Dedekind scheme. \( \square \)

### 3 Line Bundles and Filtrations

Def. (14.9.3.1). By (14.9.2.31), the graded algebra \( \oplus_{n \geq 0} B^{\varphi=p^n} \) is generated over \( \mathbb{Q} \) by \( B^{\varphi=p} \), so we can define the Serre twisting sheaf \( \mathcal{O}(1) \) on \( X_{FF} \), which is a line bundle, and on an open affine scheme \( U = X - \{ x \} \), where \( x \) corresponds to \( \log([\varepsilon]) \), \( O(1)(U) = (B[\frac{1}{\log([\varepsilon])}])^{\varphi=p} \). Similarly we can define \( O(1)(m) \), and \( O(1)(m) = O(1)^m \).

Lemma (14.9.3.2). There is an isomorphism \( \text{Div}(X) \rightarrow \text{Pic}(X) \) that maps each \( x \) to the inverse of its ideal sheaf (5.5.3.15) (4.3.5.20). And there is also a degree map \( \text{Div}(X) \rightarrow \mathbb{Z} \). Then:
\[
\text{Div}(X) \xrightarrow{\text{deg}} \mathbb{Z} \xrightarrow{\rho} \text{Pic}(X)
\]
commutes.

**Proof:** It suffices to show that any \( O(x) \) is isomorphic to \( O(1) \). As \( \log([\varepsilon]) \) is a global section of \( O(1) \) that vanishes of order 1 at \( x \), it induces an isomorphism \( O(1) \cong O(x) \) by (5.5.3.15). \( \square \)

Lemma (14.9.3.3) [Cohomology of Line Bundles]. For any integer \( m \), \( B^{\varphi=p^m} \rightarrow H^0(X, O(m)) \) is an isomorphism and \( H^i(X, O(m)) = 0 \) for \( i > 0, m > 0 \).

**Proof:** This is trivial using Cech cohomology, as \( \oplus_{n \geq 0} B^{\varphi=p^n} \) is PID, so \( X \) is separated. \( \square \)

Prop. (14.9.3.4). The construction induces an isomorphism \( \rho : \mathbb{Z} \cong \text{Pic}(X) : m \mapsto O(m) \).

**Proof:** By lemma (14.9.3.2), \( \rho \) is surjective because \( \text{Div}(X) \rightarrow \text{Pic}(X) \) does, and it is injection because if \( O(m) \cong O(n) \), then tensoring \( O(−m) \), we can assume \( O \cong O(−k) \), but they have different global sections by lemma (14.9.3.3) and (14.9.2.29)-(14.9.2.31).

**Harder-Narasimhan Filtration of Vector Bundles**

Prop. (14.9.3.5) [Harder Narasimhan Formalism for Bundles]. For a vector bundle \( L \) on \( X \), we can define \( \text{deg}(L) = n \) if \( L \cong O(n) \) (14.9.3.2), and for a vector bundle \( E \), define \( \text{deg}(E) = \text{deg}(\wedge(E)) \). And define the generic rank on the category of coherent sheaves on \( X \). Then this is a Harder-Narasimhan formalism on \( C = Bund_X \) with \( A = Vect_K(X) \).
Proposition (14.9.4.1) [Base Change]. Let $C^o$ be alg.closed. For any finite extension $E$ of $Q_p$ of degree $n$, $\text{Spec } E \to \text{Spec } Q_p$ is finite étale, and finite locally free of degree $n$, so does $X_E = X \otimes_{Q_p} E \to X (5.6.2.24)$.

In particular, $X_E$ is also a Dedekind scheme?. For any closed point $x$ of $X$ corresponding to an untilt $K$ of $C^o$, which is alg.closed, the fiber of $X_E$ over $x$ is identical to the spectrum of $E \otimes_{Q_p} K \cong K^n$ as $K$ is alg.closed.

In this situation and use(14.9.2.36), we see that the closed points of $X_E$ are in bijection with isomorphism classes of $(K, \iota, u)$ module $\varphi$-actions, where $(K, \iota)$ is an untilt of $C^b$, and $u : E \to K$ is an embedding of $E$ into $K$ over $Q_p$, isomorphism classes of these triples are denoted by $Y_E$.

Proposition (14.9.4.2). By(14.9.4.1) and flat base change(5.7.5.1), we know $H^0(X_E, \mathcal{O}_{X_E}) = E$, in particular $X_E$ is connected.

Lemma (14.9.4.3). If $E$ is unramified of degree $n$ over $Q_p$, then $E \cong W(F_{p^n})[\frac{1}{p}]$. In particular,

$$\text{Hom}_{Q_p}(E, K) \cong \text{Hom}_{Z_p}(W(F_{p^n}), \mathcal{O}_K) \cong \text{Hom}_{F_p}(F_{p^n}, \mathcal{O}_K) \cong \mathcal{O}_{C^b}/[t]) \cong \text{Hom}_{F_p}(F_{p^n}, C)$$

where the last isomorphism is by Henselian lemma.

Therefore, $Y_E \cong Y \otimes \text{Hom}_{F_p}(F_{p^n}, C)$, and

Closed points of $Y_E \cong Y_E/\varphi^Z \cong (Y \otimes \text{Hom}_{F_p}(F_{p^n}, C))/\varphi^Z \cong Y/\varphi^{nZ}$.

Proposition (14.9.4.4). If $E$ is unramified of degree $n$ over $Q_p$ and $U \neq X$ is an affine open defined by a homogenous element $t$, then

$$U_E = \text{Spec}((B[t^{-1}] \otimes_{Q_p} E)^{\varphi=\text{id}}) = \text{Spec}(B[t^{-1}]^{\varphi^n=1}).$$

where $\varphi$ acts trivially on $E$.

Proof: Each $u \in \text{Hom}_{F_p}(F_{p^n}, C^b)$ induces a map $W(F_p) \to W(\mathcal{O}_{C^b}) = A_{\text{inf}} \to B$, which extends to a map $\overline{u} : E \to B[t^{-1}]$. and induces a map $q_n : B[t^{-1}] \otimes_{Q_p} E \to B[t^{-1}]$. Now

$$B[t^{-1}] \otimes_{Q_p} E \to \prod_{\text{Hom}_{F_p}(F_{p^n}, C)} B[t^{-1}]$$

is an isomorphism, which is just because $x^{p^n} - x$ splits in $B[t^{-1}]$.

And under this isomorphism, the action of $\varphi$ is

$$\varphi((f_0, \ldots, f_{n-1}) = (\varphi(f_{n-1}), \varphi(f_0), \ldots, \varphi(f_{n-2})),$$

so proposition is clear.
Cor. (14.9.4.5). Fix now a finite extension $E/Q_p$ with uniformizer $\pi$ that has ramification degree $e$ and inertia degree $d$, and $E_0$ is the maximal unramified subextension, then there are maps $E_0 \to B$ by (14.9.4.4), fix forever one of them $p_u$, this induces a map

$$B[\frac{1}{t}] \otimes Q_p E \to B[\frac{1}{t}] \otimes E_0 E$$

and this induces an isomorphism

$$(B[\frac{1}{t}] \otimes Q_p E)^{\varphi=\text{id}} = (B[\frac{1}{t}] \otimes Q_p E_0)^{\varphi=\text{id}} \otimes E_0 E = (B[\frac{1}{t}] \otimes E_0 E)^{\varphi^d=\text{id}}$$

Def. (14.9.4.6) $[Y_E^0]$. Define $Y_E^0 \subset Y_E$ is triples $(K, \iota, u)$, where $(K, \iota)$ is an untilt of $C^b$, and $u: E \to K$ is an embedding that $u|_{E_0}$ is identical to $e_K \circ p_u: E_0 \to B \to K$. Notice $Y_E^0$ is not stable under the Frobenius, but it is stable under $\varphi^d$, and induces an isomorphism

$$Y_E^0/\varphi^d \simeq Y_E^0/\varphi^d.$$  

Prop. (14.9.4.7). Notice for an element $y$ of $Y_E^0$, the map $u: E \to K_y = B_{dR}^+(y)/\xi$ extends uniquely to a map $E \to B_{dR}^+(y)$ that is compatible with $e_K \circ p_u: E_0 \to B \to K$, because $E$ is separable over $E_0$. i.e.

$$E_0 \xrightarrow{e_K \circ p_u} B_{dR}^+(y) \xrightarrow{\cdot u} K$$

Then this defines a map $B \otimes E_0 E \to B_{dR}^+(y)$, also called the stalk map.

Prop. (14.9.4.8). For any finite extension $E/Q_p$, the degree map $\deg : \text{Pic}(X_E) \cong \mathbb{Z}$ is an isomorphism.

Proof: It suffices to show that $O_{X_E}(x) \cong O_{X_E}(x')$ for each pair of closed points $x, x'$ of $X_E$.

We attempt to construct a line bundle $O_{X_E}(1)$ on $X_E$ that $O_{X_E}(1)(U_E) = (B[\frac{1}{t}] \otimes E_0 E)^{\varphi^d=\pi}$, because $O_{X_E}(U_E) = (B[\frac{1}{t}] \otimes E_0 E)^{\varphi^d=1}$.

We show simultaneously that $O_{X_E}(1)$ is a line bundle and it is isomorphic to $O_{X_E}(x)$ for any closed point $x \in X_E$. For any $x \in X_E$ corresponding to a $\varphi^d$-orbit of $Y_E^0$, let $f$ be the element constructed by lemma (14.9.4.9) below, we show that for any affine open $U = D(t)$, multiplying by $f : O_{X_E}(x)(U_E) \to O_{X_E}(1)(U_E)(\ast)$ is an isomorphism:

Notice $B \otimes E_0$ is free over $B$, let $N(f) \in B$ be its norm, the norm is local, so for each $y \in Y$, $N(f)_y = \prod f_{\overline{y}}$, where $\overline{y} \in Y_E$ are over $y$, so it vanishes with order 1 in a $\varphi^d$-orbit of $Y(1)$ because $f$ only vanishes at $\overline{y}$ in the orbit corresponding to $x$, and then $N(f)\varphi(N(f))\ldots\varphi^{d-1}(N(f))$ vanishes at a single $\varphi$-orbit of $Y$ with order 1, thus equals $u \log([\varepsilon])$ for some $\varepsilon \in m_{C^0}$, by (14.9.2.13)/(14.9.2.9). In particular, $y$ divides $\log([\varepsilon])$.

Now if $x \notin U_E$, then $\log([\varepsilon])$ divides $t$, so $f$ divides $t$, thus $f$ is invertible in $B[\frac{1}{t}] \otimes E_0 E$, thus $(\ast)$ is an isomorphism.

Otherwise if $x \in U_E$, then choose some $x'$ not in $U_E$, then the same argument shows that $f'$ is invertible in $B[\frac{1}{t}] \otimes E_0 E$, so $f/f' \in (B[\frac{1}{t}] \otimes E_0 E)^{\varphi=id}$ that vanishes with a single zero at $x$, so multiplying by $f'/f$ defines an isomorphism $O_{X_E}(U_E) \cong O_{X_E}(x)(U_E)$, so it suffices to show the composition

$$O_{X_E}(U_E) \xrightarrow{f/f'} O_{X_E}(x)(U_E) \xrightarrow{f} O_{X_E}(1)(U_E)$$

is an isomorphism, but this reduces to the first case. \qed
Lemma (14.9.4.9) [Uniformizer Existence]. If \( x \) be a closed point of \( X_E \) corresponding to an orbit of \( \varphi \) in \( Y_E \) such that \( S \) of \( \varphi^d \) in \( Y_E^0 \), then there is an element \( f \in (B \otimes_{E_0} E)^{\varphi^d=\pi} \) that \( \text{ord}_\varphi(f) = 1 \) if \( \overline{y} \in S \), and 0 otherwise.

Proof: The map defined \((14.9.4.18)\) composed with the Teichmüller section \((14.9.4.16)\) in fact has image in \((B \otimes_{E_0} E)^{\varphi^d=\pi}\) because \( [\pi] = \pi t + b^\pi = \varphi^n \) on \( \mathcal{O}_S \), and it is an isomorphism of \( \mathcal{O}_E \) modules. Now there are commutative diagrams:

\[
G_{LT}(\mathcal{O}_S) \xrightarrow{\sigma} G_{LT}(A_{inf} \otimes_{\mathcal{O}_{K_0}} \mathcal{O}_E) \xrightarrow{\log_G} B \otimes_{E_0} E \\
\downarrow \quad \quad \quad \downarrow \\
G_{LT}(\mathcal{O}_K) \xrightarrow{\log_G} K
\]

The map \( G_{LT}(\mathcal{O}_S) \to G_{LT}(\mathcal{O}_K) \) has kernel \( \mathcal{O}_{E_0} u \) for some \( u \), thus we can let \( f = \log_G(\sigma(u)) \), then the image of \( f \in K \) is 0, which means \( f \) has a zero at the point \( y \in Y_E^0 \). And \((14.9.4.13)\) shows the the zeros of \( f \) is just the \( \varphi^d \)-orbit containing \( y \).

\[\square\]

Lubin-Tate Formal Groups and the Proof of the Lemma of Uniformizer

Prop. (14.9.4.10). The ring \( B \otimes_{E_0} E \) is an integral domain.

Proof: Cf.[Lurie P95]. In fact this is the ramified Witt vector, which is by the same reason as before an integral domain, Cf.[FF Curve Johannes]. \[\square\]

Cor. (14.9.4.11). If \( f \neq 0 \in B \otimes_{E_0} E \), then \( N_{E/E_0}(f) \neq 0 \in B \), in particular, the vanishing locus of \( f \) is finite.

Cor. (14.9.4.12). If \( f, g \in B \otimes_{E_0} E \), then \( f \) is divisible by \( g \) iff for each \( \overline{y} \in Y_E^0 \), \( \text{ord}_\varphi(f) \geq \text{ord}_\varphi(g) \).

Proof: If \( \text{ord}_\varphi(f) \geq \text{ord}_\varphi(g) \), suppose \( N_{E/E_0}(g) = gh \), then multiplying by \( h \), we can assume \( g \in B \). Now \( f \) is written uniquely as \( f_0 + f_1 \pi + \ldots + f_{e-1} \pi^{e-1} \) where \( f_k \in B \), thus it suffices to show \( f_k \) is divisible by \( g \), which is equivalent to \( \text{ord}_y(f_k) \geq \text{ord}_y(g) \) for each \( y \in Y \), by (14.9.2.11). Now if \( \text{ord}_y(g) = n \), the hypothesis shows \( f \) vanishes in

\[
\prod_{\overline{y} \to y} B_{dR}^+(y)/\xi^n = (B_{dR}^+(y)/\xi^n) \otimes_{E_0} E = B_{dR}^+(y)/\xi^n + \pi B_{dR}^+(y)/\xi^n + \ldots + \pi^{e-1} B_{dR}^+(y)/\xi^n
\]

thus \( \text{ord}_y(f) \geq n = \text{ord}_y(g) \). \[\square\]

Cor. (14.9.4.13). If \( f \in (B \otimes_{E_0} E)^{\varphi^d=\pi} \), then the vanishing locus of \( f \) is a single \( \varphi^d \)-orbit, and all zeros are simple.

Proof: Set \( N_{E/E_0}(f) = f' \) and \( N_{E/E_0}(\pi) = \pi' \), then \( f \) belongs to \( B^{\varphi^d=\pi'} \), and its divisor is just the image of divisor of \( f \) in \( Y_E^0 \). So it suffices to show that \( f' \) vanishes on a single \( \varphi^d \)-orbit.

Now for \( 0 < \rho < 1 \),

\[
p^{d^s} | f' \rangle_{\rho^{d^s}} = | \pi' f' \rangle_{\rho^d} = | f' \varphi^d \rangle_{\rho^d} = | f' \rangle_{\rho^d}^{d^s},
\]

thus

\[
p^{d^s} + v_p^{d^s}(f') = p^{d^s} v_s(f')
\]
for each $s > 0$, differentiating, we get
\[ 1 + \partial_- v_s(f') = \frac{\partial_- v_s}{1 + \varphi} \]

Now the divisor of $f'$ is $\varphi^{dZ}$-invariant, and it has exactly one zero on any annulus $(\rho^n, \rho)[14.9.2.15]$, thus its divisor is a single $\varphi^d$-orbit.

**Def. (14.9.4.14) [Universal Lubin-Tate Formal Group].** Recall that if $E$ is a finite extension of $Q_p$ with uniformizer $\pi$, for a $O_E$-algebra $A$ complete w.r.t $\pi$, $G_{LT}(A)$ is the Lubin-Tate formal group, with elements the topological nilpotent elements of $A$.

Now we define the **universal cover of Lubin-Tate formal group** $\tilde{G}T$ as the functor
\[ A \mapsto \text{lim}\{\cdots \xrightarrow{\pi} G_{LT}(A) \xrightarrow{\pi} G_{LT}(A)\}. \]

**Prop. (14.9.4.15).**
- Notice for $K$ an alg.closed extension of $E$, $G_{LT}(O_K)$ is in bijection with $m_K$, and the kernel of $[\pi^n]$ on $G_{LT}(O_K)$ has order $O_E/\pi^n$, thus the kernel of $\tilde{G}_{LT}(O_K) \to G_{LT}(O_K)$ is a 1-dimensional $O_E$-module.
- If $\pi$ vanishes on $A$ and $A$ is perfect, then $[\pi] = \pi t + t^q = t^q$ on $A$, so it is just the Frobenius, and $\tilde{G}_{LT}(A) \to G_{LT}(A)$ is a bijection.
- $\tilde{G}_{LT}(A) \to \tilde{G}_{LT}(A/I)$ is an isomorphism for $\pi \in I$ and $A$ is $I$-adic.
- $\tilde{G}_{LT}(A) \to \tilde{G}_{LT}(A/I)$ is an isomorphism for any ideal $I$ that $I + (\pi) \neq (1)$, because both of them is isomorphic to $\tilde{G}_{LT}(A/(I + (\pi)))$.

**Proof:** For 3, it suffices to prove that $\tilde{G}_{LT}(A/I^{n+1}) \to \tilde{G}_{LT}(A/I^n)$ for $n \geq 1$. Notice $F(u,v) \equiv u + v \mod I^{2n}$, so we have an exact sequence
\[ 0 \to I^n/I^{n+1} \to G_{LT}(A/I^{n+1}) \to G_{LT}(A/I^n) \to 0. \]

In particular the kernel is annihilated by $\pi$, so there is a commutative diagram
\[ \cdots \xrightarrow{\pi} G_{LT}(A/I^{n+1}) \xrightarrow{\pi} G_{LT}(A/I^{n+1}) \]
\[ \quad \downarrow \quad \downarrow \quad \downarrow \]
\[ \cdots \xrightarrow{\pi} G_{LT}(A/I^{n+1}) \xrightarrow{\pi} G_{LT}(A/I^{n+1}) \]

which show that $\tilde{G}_{LT}(A/I^{n+1}) \cong \tilde{G}_{LT}(A/I^n)$. \qed

**Cor. (14.9.4.16) [Teichmuller Section].** Consider the $O_E$-algebra $A_{inf} \otimes_{O_{E_0}} O_E$. Because there are isomorphism $O_{E_0}/p \cong O_E/\pi$, we have an isomorphism
\[ C^p \cong A_{inf}/p \cong (A_{inf} \otimes_{O_{E_0}} O_E)/\pi \]

Now(14.9.4.15) shows the diagram
\[ \tilde{G}_{LT}(A_{inf} \otimes_{O_{E_0}} O_E) \xrightarrow{\cong} \tilde{G}_{LT}(O_{C^p}) \]
\[ \downarrow \quad \downarrow \]
\[ G_{LT}(A_{inf} \otimes_{O_{E_0}} O_E) \longrightarrow G_{LT}(O_{C^p}) \]

So the lower horizontal map is surjective, and it even has a canonical section $\sigma$, called the **Teichmuller section**.
Cor. (14.9.4.17). Given a point of $Y^0_E$ which corresponds to an untilt of $C^\flat$ together with a $E_0$-map $E \rightarrow K$, then this gives a commutative diagram

$$
\tilde{G}_{LT}(A_{inf} \otimes O_{E_0} O_E) \xrightarrow{\cong} \tilde{G}_{LT}(O_K) \\
\downarrow \quad \downarrow \\
G_{LT}(A_{inf} \otimes O_{E_0} O_E) \longrightarrow G_{LT}(O_K)
$$

where the right vertical arrow is surjective with kernel free of rank 1 over $O_E$. So this together with (14.9.4.16) shows there is a surjection $G_{LT}(O_{C^\flat}) \rightarrow G_{LT}(O_K)$ with kernel a rank-1 $O_E$-module.

Prop. (14.9.4.18). There is a canonical $O_E$-module map

$$G_{LT}(A_{inf} \otimes O_{E_0} O_E) \xrightarrow{\log_G} B \otimes_{E_0} E.$$

and it is equivariant w.r.t $\varphi$.

Proof: $G_{LT}(A_{inf} \otimes O_{E_0} O_E)$ are in bijection with the maximal ideal of $A_{inf} \otimes O_{E_0} O_E$, and $\log_G(x)$ is of the form $x + \frac{a_2}{n}x^2 + \ldots + \frac{a_n}{n}x^n + \ldots$, with $c_n \in O_E$.

Now for $x \in G_{LT}(A_{inf} \otimes O_{E_0} O_E)$, we show that $\log_G(x)$ converges in $B \otimes_{E_0} E = B + \pi B + \ldots + \pi^{n-1}B$: Let $c_n x^n = \sum a_{n,i} \pi^i$, then we need to show $a_{n,i}/n$ converges to 0 for each of the norm $|\cdot|_\rho$. And this is because if $x = x_0 + \pi y_0$, then for $n \geq em$, $|x|_\rho \leq \max\{|x_0|_{\rho}^m, \rho^n\}$, which decays exponential in $n$, and $|\frac{1}{n}|_\rho$ decays linearly in $n$. \[\square\]

Prop. (14.9.4.19). The map $\log_G(\sigma(\cdot)) : G_{LT}(O_{C^\flat}) \rightarrow (B \otimes_{E_0} E)^{\varphi^n=\pi}$ as in (14.9.4.9) is an isomorphism.

Proof: For surjectivity, as any $f \in (B \otimes_{E_0} E)^{\varphi^n=\pi}$ vanishes at a single $\varphi^D$-orbit, then by (14.9.4.9) we can find a $\log_G(u)$ that vanishes at the same locus, so $f = \log(u)\lambda$ where $\lambda$ is a unit in $B \otimes_{E_0} E (14.9.4.12)$, so

$$\lambda \in (B \otimes_{E_0} E)^{\varphi^n=\id} = (B \otimes_{Q_\rho} E)^{\varphi=\id} (14.9.4.5) = B^{\varphi=\id} \otimes_{Q_\rho} E = E.$$

For injectivity, we proved in (14.9.4.9) that each $\log_G(\sigma(u))$ only vanishes at a single $\varphi^D$-orbit in $Y^0_E$, so it cannot by 0, which vanishes at all points. \[\square\]

Cor. (14.9.4.20). There are canonical bijections

$$\{\text{Closed Points of } X_E\} \cong \{\varphi^{D} \text{orbits of } Y^0_E\} \cong ((B \otimes_{E_0} E)^{\varphi^n=\pi} - \{0\})/E^* \cong (G_{LT}(O_{C^\flat}) - \{0\})/E^*$$

by (14.9.4.9)(14.9.4.19),(14.9.4.12).

**Vector Bundles and Base Change**

Prop. (14.9.4.21) [Vector Bundles on the Cover]. Let $\pi : X_E \rightarrow X$ be the covering map, for any vector bundle $\mathcal{E}$ on $X_E$, $\pi_*(\mathcal{E})$ is a vector bundle on $X$, and this induces an isomorphism

$$\{X_E\text{-Bundles}\} \cong \{X \text{-Bundles with an } E\text{-action}\}.$$

Now define $\deg(\mathcal{E}) = \deg(\pi_\ast \mathcal{E})$, and $\text{slope}(\mathcal{E}) = \frac{\deg(\mathcal{E})}{\text{rank}(\mathcal{E})} = \frac{1}{n}\text{slope}(\pi_* \mathcal{E})$.

Then $\mathcal{E}$ is semistable of slope $\lambda$ iff $\pi_* \mathcal{E}$ is semistable of slope $\lambda/n$. 
**Proof:** One direction is clear, for the other, if \( \mathcal{F} = \pi_* \mathcal{E} \) is not semistable, choose its HN-filtration, then \( \lambda_1 > \lambda/n \). Now the action of \( E \) on \( \mathcal{F} \) preserves the HN-filtration, thus \( \mathcal{F}_1 \) is an \( E \)-vector bundle, thus by the correspondence above, \( \mathcal{F}_1 = \pi_* \mathcal{E}' \) for some subbundle \( \mathcal{E}' \subset \mathcal{E} \), and clearly this contradicts the semistability of \( \mathcal{E} \).

**Corollary (14.9.4.22).** For any integral number \( d, n \) with \( n > 0 \), there exists a semistable vector bundle on \( X \) with rank \( n \) and degree \( d \).

**Proof:** Let \( E \) be an extension of \( \mathbb{Q}_p \) of degree \( n \), then \( \pi_*(\mathcal{O}_{X_E}(d)) \) is semistable of rank \( n \) and degree \( d \), by (14.9.4.1)(5.6.2.23), because \( \mathcal{O}_{X_E}(d) \) is a line bundle (14.9.4.8) so clearly semistable, and it is of degree \( d \) because ?.

**Isocrystals and Classification of Semistable Vector Bundle over \( X \).**

**Remark (14.9.4.23).** Recall the Dieudonné-Manin Classification (14.2.3.7)(14.2.3.10): Any isocrystal over \( k \) is a finite sum of modules pure of slopes \( \lambda_i \). And if \( k \) is alg.closed, then any isocrystal over \( k \) has a unique decomposition as sums of \( E_{\lambda_i} \).

**Proposition (14.9.4.24).** Let \( k = \mathbb{F}_p \subset C^0 \), then there is an inclusion \( W(k) \to A_{\inf} \), which extends to a map \( K \to B \). Now given an isocrystal \( V \) over \( k \), denote \( \mathcal{E}_V \) the coherent sheaf on \( X \) defined by the graded module \( \oplus_{m \geq 0} \text{Hom}_K(V, B)^{\varphi=p^m} \). In other words, on an affine open subscheme \( U = D(t) \), \( \mathcal{E}_V(U) = \{ \varphi \text{-equivariant} \ \text{K-linear maps} \ V \to B[\mathbb{A}_t] \} \).

And when \( V = E_{m/n} \) is the simple isocrystal, then \( \mathcal{E}_V \) is denoted by \( \mathcal{O}(\frac{m}{n}) \).

**Proposition (14.9.4.25).** In fact we have \( \mathcal{O}(\frac{m}{n})(U) \cong (B[t^{-1}])^{\varphi=p^m} = (\rho_*(\mathcal{O}(m))(U) \), where \( \rho: X_E \to X \), and \( E \) is an unramified extension of \( \mathbb{Q}_p \).

**Proposition (14.9.4.26)[Classification of Semistable Vector Bundles over \( X \)].** For every vector bundle on \( X \), the HN-filtration splits non-canonically, and the construction \( V \to \mathcal{E}_V \) induces an equivalence of categories between

\[ \{ \text{Isoclinic Isocrystals of slope} \ \mu \}^{\text{op}} \to \{ \text{Semistable vector bundles on} \ X \ \text{of slope} \ \mu \} \]

**Proof:** Cf.[FF Curve Johannes].

**Corollary (14.9.4.27).** Any two semistable vector bundles of slope \( \lambda \) over \( X \) is isomorphic, and a semistable vector bundle of slope 0 is trivial.

**Proposition (14.9.4.28).** If \( \mathcal{E}, \mathcal{E}' \) be semistable vector bundles on \( X \) of slopes \( \mu, \mu' \), then \( \mathcal{E} \otimes \mathcal{E}' \) is semistable of slope \( \mu + \mu' \).

**Proof:** We can assume \( \mathcal{E} = \rho_* \mathcal{O}_{X_E}(d) \) for an unramified extension \( E/\mathbb{Q}_p \) by (14.9.4.27), and then \( \mathcal{E} \otimes \mathcal{E}' = \rho_*(\mathcal{O}_X(d) \otimes \rho^* \mathcal{E}') \). Since \( \rho_* \rho^* \) preserves semistability (by (14.9.4.21) and ?). So it suffices to prove \( \mathcal{O}(d) \otimes - \) preserves semistability, but this is clear, as \( \mathcal{O}(d) \) shifts degree.

**Diamonds Definitions**

**Definition (14.9.4.29)[Diamond].** Let Perf denote the site of perfectoid spaces of characteristic \( p \) equipped with the pro-étale topology. A **diamond** \( X \) is a sheaf (of sets) on Perf of the form \( X = \text{Hom}_{\text{perf}}(\mathcal{Z}, R) / R \), where \( \mathcal{Z} \in \text{Perf} \) and \( R \in \mathbb{Z} \times \mathbb{Z} \) is a reasonable representable equivalence relation.
Prop. (14.9.4.30) [Scholze]. Let $R = (R, R^+)$ be a Huber pair, then
\[
\text{Spd}(R) = \mathcal{Z} \mapsto \{\text{untilts of Spa}(R) \text{ over } \mathcal{Z}\}
\]
is a diamond.

And this construction can be glued to give diamond $X^\circ$ of any adic space $X$, which is a sheaf.

Def. (14.9.4.31) [Adic Fargues-Fontaine Curve]. Let $\mathcal{V}$ be the adic Spa$(A_{\text{inf}})$ removing the vanishing locus of $p$ and $[t]$, then by what we proved, the Frobenius act totally discontinuous on $\mathcal{V}$, thus the quotient $X^{FF}$ is an adic space, the FF-curve.

Prop. (14.9.4.32). There is an isomorphism of diamonds:
\[
\mathcal{V}^\circ \cong \text{Spd}(C^\flat) \times \text{Spd}(\mathcal{Q}_p), \quad X^{FF,\circ} \cong \text{Spd}(C^\flat)/\varphi^\mathcal{Z} \times \text{Spd}(\mathcal{Q}_p)
\]
More generally, over any Huber pair $R$, there is a relative FF-curve which is defined by
\[
\text{Spd}(R) \times \text{Spd}(\mathcal{Q}_p)/\varphi^\mathcal{Z}
\]

Proof: $C^\flat$ is a perfectoid of char$\rho$, so for a perfect Huber pair, $S$ point of $C^\flat$ is just a morphism $u : (C^\flat, \mathcal{O}_{C^\flat}) \rightarrow (S, S^+)$. And a $\mathcal{Q}_p$ point is just a char$0$ untilts $T$ of $S$.

So for each pairs $(T, u)$, we need to find a morphism $A_{\text{inf}}[\frac{1}{p}, [\frac{1}{p}]] \rightarrow T$. For this, consider
\[
A_{\text{inf}} = W(\mathcal{O}_{C^\flat}) \rightarrow W(S^+) \cong W(T^\flat) \stackrel{2T}{\rightarrow} T
\]
This is a bijection, as we proved in the beginning (14.9.1.2).

Prop. (14.9.4.33). There is a morphism of ringed spaces $X^{FF} \rightarrow X^{FF}$ that regard $X^{FF}$ as the rigid analytification of $X$, so they have the same category of vector bundles and cohomology, prove by Kedlaya-Liu.

5 Applications

Prop. (14.9.5.1). The FF curve $X$ is geometrically simply connected, i.e. the projection defines an isomorphism of étale groups $\pi_1(X) \rightarrow \pi_1(\text{Spec } \mathcal{Q}_p) = Gal(\mathcal{Q}_p)$.

Equivalently, the pullback defines an equivalence of étale sites.

Proof: Let $\tilde{X} \rightarrow X$ be an finite étale morphism, we want to prove that $\tilde{X} = X \otimes_{\text{Spec } \mathcal{Q}_p} \text{Spec}(E)$ for some étale $\mathcal{Q}_p$-algebra. Let $A = \rho_\ast \mathcal{O}_{\tilde{X}}$, and $E = H^0(X, A) = H^0(\tilde{X}, \mathcal{O}_{\tilde{X}})$. Now it suffices to show $A = E \otimes \mathcal{Q}_p \mathcal{O}_X$, which shows $\tilde{X} = X \otimes_{\text{Spec } \mathcal{Q}_p} \text{Spec}(E)$, and forces $E$ be an étale $\mathcal{Q}_p$-algebra by fpqc descent?. Equivalently, $A$ is trivial, and this is equivalent to $A$ being semistable of slope 0 by (14.9.4.27).

Because $\rho$ is finite étale, the trace pairing $A \times A \rightarrow A \stackrel{tr}{\rightarrow} \mathcal{O}_X$ is non-degenerate (check on stalks), which induces an isomorphism $A \cong A^\vee$, so deg$(A) = 0$, and if $A$ is not semistable, let $A'$ be the first term of the HN-filtration of $A$, then it is of slope $\lambda > 0$, So $A' \otimes A'$ is of slope $2\lambda$ by (14.9.4.28), so the composite $A' \otimes A' \rightarrow A \otimes A \rightarrow A$ must by 0(3.2.4.32), which is impossible, because if $U$ is an affine open that $A$ has a section, then this says $U \otimes X \tilde{X}$ has a section $s$ that $s^2 = 0$. But $U \otimes X \tilde{X}$ is reduced (check on stalks).
Cor. (14.9.5.2).

- The projection map induces equivalence of categories between Finite Abelian groups with \( \text{Gal}(\mathbb{Q}_p) \)-action and étale Local system on \( X \).
- If \( M \) is a finite Abelian group with a \( \text{Gal}(\mathbb{Q}_p) \)-action, then

\[
H^*(\text{Gal}(\mathbb{Q}_p), M) \rightarrow H^*_\text{ét}(X, u^*M)
\]

is an isomorphism for \( * = 0, 1 \).

Proof: 1 is trivial, and 2 Cf. [Lurie P102]. \( \square \)

6 Weakly Admissible \( \Rightarrow \) Admissible

Def. (14.9.6.1) [Notations]. Let \( K \) be a finite extension of \( \mathbb{Q}_p \), and \( K_0 = W(k)[\frac{1}{p}] \) be the maximal unramified subextension in \( K \), let \( C = \hat{\mathbb{K}} \) and \( F = C^0 \). Denote by \( \infty \in X \) the closed point determined by \( C \), which is just the vanishing locus of the Galois stable line \( \mathbb{Q}_pt \), where \( t = \log([\varepsilon]) \) and \( \varepsilon = (1, \xi_p, \xi_{p^2}, \ldots) \in C^0(14.9.2.32) \).

Notice \( G_K \) acts on \( \mathbb{Q}_p \log([\varepsilon]) \) by the cyclotomic character \( \chi_{\text{cycl}} \). Recall \( B^+_d \mathcal{R} = \hat{O}_X(\infty), B^+_\text{cris} = B^+_{\text{cris}}[t^{-1}], B_e = H^0(X - \{\infty\}, \mathcal{O}_X) = (B_{\text{cris}})^{\varphi=\text{id}} \).

Def. (14.9.6.2) [Equivariant Action of \( G_K \) on Vector Bundles]. Recall an equivariant action of \( G_K \) on a bundle \( \mathcal{E} \) on \( X \) is a data of isomorphisms \( \sigma^*(\mathcal{E}) \cong \mathcal{E} \) that \( c_{\sigma \tau} = c_\sigma \circ \tau^*(c_\sigma) \). Notice any equivariant action of \( G_K \) on \( \mathcal{E} \) induces a semilinear \( G_K \)-action on \( \mathcal{E}_\infty^\wedge = \mathcal{E} \otimes_{\mathcal{O}_X} B^+_d \mathcal{R} \), and here we require this action is continuous. The category of equivariant \( G_K \)-bundles are denoted by \( \text{Bun}^G_K \).

Cor. (14.9.6.3). By the slope 0 case of the classification of vector bundles on \( X(14.9.4.26) \) and(14.2.7.1), we see that the functor:

\[
\text{Rep}_{\mathbb{Q}_p} G_K \rightarrow \text{Bun}^G_K_X : V \mapsto V \otimes_{\mathbb{Q}_p} \mathcal{O}_X
\]

is fully faithful with essential image the category \( \text{Bun}^{G_K, \text{sst}, 0}_X \) of all \( G_K \) vector bundles on \( X \) that the underlying bundle is semistable of slope 0, i.e. trivial(14.9.4.27).

Prop. (14.9.6.4). There is a pullback diagram of categories:

\[
\begin{array}{ccc}
\varphi - \text{FilMod}_{K/K_0} & \rightarrow & \varphi - \text{Mod}_{K_0} \\
\downarrow \mathcal{E}(-) & & \downarrow V \\
\text{Bun}^{G_K}_X & \rightarrow & \text{Rep}_{B_e} G_K
\end{array}
\]

Where \( \mathcal{E}(-) \) maps a \( \varphi \)-filtered module \( (D, \varphi_D, \text{Fil}) \) to the bundle that is the bundle \( (\tilde{D}, \varphi_{D}) \) modified so that the fiber at \( \infty \) is \( \text{Fil}^0(D_K \otimes_K B^+_d \mathcal{R}) \).

Proof: 1: By lemma(14.2.7.7), \( \varphi - \text{FilMod}_{K/K_0} \) is equivalent to a \( \varphi \)-module \( V \) with a \( G_K \)-stable \( B^+_d \mathcal{R} \)-lattice in \( (V \otimes_{K_0} K) \otimes_K B^+_d \mathcal{R} = V \otimes_{K_0} B^+_d \mathcal{R} \).

2: By(14.2.7.5), \( \varphi \)-Mod is a full subcategory of \( \text{Rep}_{B_e} G_K \), where the \( G_K \)-stable \( B^+_d \mathcal{R} \)-lattice is choose to be \( V \otimes_{K_0} B^+_d \mathcal{R} \).
3: Clearly there is a functor

\[ \text{Bun}_X^{G_K} \to \text{Rep}_{B_C} G_K : \mathcal{E} \to H^0(X - \{\infty\}, \mathcal{E}). \]

and (5.4.2.14) says in this case \( \text{Bun}_X^{G_K} \) is equivalent to a \( B_C \)-module with continuous \( G_K \)-actions and and a \( B^+_{dR} \)-module with continuous \( G_K \)-actions that they corresponds as a \( B_{dR} \)-module with continuous \( G_K \)-actions.

4: The compatibility in 3 just says that the \( B^+_{dR} \)-lattice choosen in the definition of (14.2.7.4) just comes from that of 2, so this diagram is clearly a pullback. \( \square \)

**Lemma (14.9.6.5).** Let \( \text{Fil} V \in \text{VectFil}_K \) and \( W = \text{Fil}(V \otimes_K B_{dR}) \), if \( V \otimes B^+_{dR} = \{e_1, \ldots, e_n\} \) and \( \text{Fil}^0(V \otimes_K B_{dR}) = \{t^{-a_1}e_1, \ldots, t^{-a_n}e_n\} \), then the Hodge polygon of \( \text{Fil} V \) has slopes \( (a_1, \ldots, a_n) \).

**Proof:** Use (14.2.7.7), notice \( (t^a B^+_{dR})^G_K = 0 \) for \( a > 0 \), as in the proof of (14.2.7.2). \( \square \)

**Lemma (14.9.6.6).** The functor

\[ \mathcal{E}(-) : \varphi - \text{FilMod}_{K/K_0} \to \text{Bun}_X^{G_K} \]

defined in (14.9.6.4) preserves degree and HN-filtration, where the HN-filtration on the RHS is induces by the HN-filtration on \( \text{Bun}_X \) by canonicity.

**Proof:**

\[ \deg(\mathcal{E}(D, \varphi_D, \text{Fil})) = \deg(D, \varphi_D, \text{Fil}) - \dim_K[D \otimes_{K_0} B^+_{dR} : \text{Fil}^0(D_K \otimes_K B_{dR})] = \deg(D, \varphi_D, \text{Fil}) - \deg(D, \varphi_D). \]

Now the degree correspond, for the invariance of HN-filtration, it suffices to prove the subobjects are in bijection: Given a subobjects of \( \mathcal{E}(V) \), we want to show it is a \( \mathcal{E}(V') \), but this is because on the affine open \( \text{Spec}(B_C) \), by (14.2.7.5) any subbundle is also crystalline, i.e. comes from \( \varphi - \text{Mod}_{K_0} \).

\( \square \)

**Prop. (14.9.6.7) [Weakly Admissible implies Admissible].** The category of crystalline Galois representations of \( G_K \) is equivalent to the category \( \varphi - \text{FilMod}_{K/K_0}^{\text{wa}} \) of weakly admissible filtered \( \varphi \)-modules for \( K \).

**Proof:** By definition of weakly admissible and (14.9.6.6), there is a pullback diagram

\[ \begin{array}{ccc}
\varphi - \text{FilMod}^{\text{wa}}_{K/K_0} & \longrightarrow & \varphi - \text{FilMod}_{K/K_0} \\
\downarrow & & \downarrow_{\mathcal{E}(-)} \\
\text{Rep}_{Q_p} G_K \cong \text{Bun}_X^{G_K, \text{sst}, 0} & \longrightarrow & \text{Bun}_X^{G_K} 
\end{array} \]

Adjunction with (14.9.6.4), we get another pullback diagram

\[ \begin{array}{ccc}
\varphi - \text{FilMod}^{\text{wa}}_{K/K_0} & \longrightarrow & \varphi - \text{FilMod}_{K/K_0} \\
\downarrow & & \downarrow_{\mathcal{E}(-)} \\
\text{Rep}_{Q_p} G_K \cong \text{Bun}_X^{G_K, \text{sst}, 0} & \longrightarrow & \text{Bun}_X^{G_K} \\
\downarrow & & \downarrow_{\mathcal{E}(-)} \\
\text{Rep}_{Q_p} G_K \cong \text{Bun}_X^{G_K, \text{sst}, 0} & \longrightarrow & \text{Rep}_{B_C} G_K 
\end{array} \]

But this pullback is just the category of crystalline representations: by (14.9.6.3), for \( V \in \text{Rep}_{Q_p} G_K \), the condition \( \mathcal{V}(D)(M) \cong M \) in (14.2.7.5) is just saying that \( V \) is in the image of \( \mathcal{V} \) iff

\[ (V \otimes_{Q_p} B_{\text{crys}})^{\varphi = \text{id}} \otimes_{B_C} B_{\text{crys}} \cong V \otimes_{Q_p} B_{\text{crys}} \]

which is equivalent to \( V \) being crystalline. \( \square \)
14.10 Pro-Étale Sites on Perfectoids and Diamonds

Main references are [Sch17] and [Notes on Diamonds, David Hansen].

1 Properties of Perfectoid Spaces

Totally Disconnected Spaces

Def. (14.10.1.1) [Totally Disconnected Spaces]. A perfectoid space $X$ is called totally disconnected if it is qcqs and any open covering $\{U_i \to X\}$ splits, i.e. $\bigsqcup U_i \to X$ splits, or equivalently, there is a refinement covering $\{V_i \to X\}$ that $X \cong \bigsqcup V_i$.

A perfectoid space $X$ is called strictly totally disconnected if it is qcqs and every étale cover splits.

Prop. (14.10.1.2). Let $X$ be a qcqs perfectoid space, then $X$ is totally disconnected iff all its connected components are of the form $\text{Spa}(K, K^+)$ where $(K, K^+)$ are perfectoid affinoid fields. And it is strictly totally disconnected if moreover $K$ are all alg.closed.

Proof: Cf. [Sch17].P29, P35.

Prop. (14.10.1.3). if $X$ is a totally disconnected perfectoid space, then $X$ is affinoid.


Injections

Def. (14.10.1.4) [Injections]. A map $f : X \to Y$ of perfectoid spaces is called an injection if for any perfectoid space $Z$, $f_* : \text{Hom}(Z, X) \to \text{Hom}(Z, Y)$ is an injection.

Prop. (14.10.1.5) [Residue Field Map is Injection]. Let $X$ be a perfectoid space and $x \in X$, giving rise to a map of residue fields

$$i_x : \text{Spa}(\kappa(x), \kappa(x)^+) \to X,$$

then $i_x$ is an injection of perfectoid spaces.

Proof: To show this, firstly we can replace $X$ with an affinoid nbhd of $X$. Then notice that $\text{Spa}(\kappa(x), \kappa(x)^+)$ is the filtered limit over all rational nbhds $U$ of $x$ in $X$, and for each $U$, $U \to X$ is an injection by definition (14.8.3.1), so $i_x$ is also an injection.

Cor. (14.10.1.6). In particular, if $X$ is qcqs and has a unique closed point $x \in X$, then $X = \text{Spa}(\kappa(x), \kappa(x)^+)$, as in this case $X$ is the only quasi-compact open subset containing $x$.

Prop. (14.10.1.7) [Characterizations of Injections]. Let $f : Y \to X$ be a map of perfectoid spaces, then the following conditions are equivalent:

- $f$ is an injection.
- For any perfectoid adic field $(K, K^+)$, the map of sets $f_* : Y(K, K^+) \to X(K, K^+)$ is an injection.
- The map $|f| : |Y| \to |X|$ is injective, and for all rank 1 point $y \in Y$ with image $f(y) = x \in X$, the map of completed residue fields $\kappa(x) \to \kappa(y)$ is an isomorphism.
The map $|f| : |Y| \to |X|$ is injective, and $f$ is final in the category of maps $Z \to X$ that $|Z| \to |X|$ factors through the map $|Y| \to |X|$.

In particular, by item 4, an injection of perfectoid spaces is determined by its topological map.

Proof: Cf. [Sch17] P21. $4 \to 1 \to 2$ is trivial.

Prop. (14.10.1.8) [Injection and Base Change].
- Let $f : Y \to X$ be an injection of perfectoid spaces, and $X' \to X$ any map of perfectoid spaces, then the pullback $f' : Y' = Y \times_X X' \to X'$ is also an injection, and the induced map $|Y'| \to |Y| \times_{|X|} |X'|$ is a homeomorphism.
- A map of perfectoid spaces is an injection iff it is universally injective.


Immersions

Def. (14.10.1.9) [Immersion]. A map of perfectoid spaces $f : Y \to X$ is called an immersion if $f$ is an injection and $|f| : |Y| \to |X|$ is a locally closed immersion. If $|f|$ is moreover closed or open, then it is called closed/open immersion.

Def. (14.10.1.10) [Zariski Closed Immersion]. Let $f : Z \to X$ be a map of perfectoid spaces where $X = \text{Spa}(R, R^+)$ is affinoid perfectoid, then
- the map $f$ is called Zariski closed immersion if $f$ is a closed immersion and $|Z| = V(I) \subset |X|$, where $I \subset R$ is an ideal.
- the map $f$ is called strongly Zariski closed immersion if $Z = \text{Spa}(S, S^+)$ is affinoid perfectoid, $R \to S$ is surjective, and $S^+$ is the closure of $R^+$ in $S$.

Prop. (14.10.1.11).
- If $f$ is strongly Zariski closed, then $f$ is Zariski closed, in particular a closed immersion.
- If $f$ is Zariski closed, then $Z$ is affinoid.
- If $X$ is of characteristic $p$, and $f$ is Zariski closed, then $f$ is strongly Zariski closed.

Proof: Cf. [?] Section 2.5.

Prop. (14.10.1.12). For any map of perfectoid spaces $Y \to X$, the diagonal map $\Delta_f : Y \to Y \times_X Y$ is an immersion.

Proof: Clearly $\Delta_f$ is an injection, thus it suffices to show that $|\Delta_f|$ identifies $Y$ with a locally closed subset of $|Y \times_X Y|$. This can be checked locally on the target, so we can assume $X = \text{Spa}(R, R^+)$ and $Y = \text{Spa}(S, S^+)$, then the diagonal map is strongly Zariski closed, as $S \widehat{\otimes}_R S \to S$ is surjective and maps the integral closure of $S^+ \widehat{\otimes}_R S^+ \to S^+$ onto $S^+$. Thus by (14.10.1.11), $\Delta_f$ is a closed immersion in this case.

Def. (14.10.1.13) [Separated Map]. A map $f : Y \to X$ of perfectoid spaces is called separated if $\Delta_f$ is a closed immersion.
\textbf{Prop. (14.10.1.14) [Valuation Criterion].} Let \( f : Y \to X \) be a map of perfectoid spaces. The following are equivalent:

\begin{itemize}
  \item \( f \) is separated.
  \item \( |\Delta_f| : |Y| \to |Y \times_X Y| \) is a closed immersion.
  \item \( |f| \) is quasi-separated, and for any perfectoid adic field \((K, K^+)\) and any diagram
    \[
    \begin{array}{ccc}
    \text{Spa}(K, \mathcal{O}_K) & \to & Y \\
    \downarrow & & \downarrow f \\
    \text{Spa}(K, K^+) & \to & X
    \end{array}
    \]
    there exists at most one dotted arrow making the diagram commutative.
\end{itemize}

\textbf{Proof:} The equivalence of 1 and 2 is by (14.10.1.12).

2 \to 3: If \(|\Delta_f|\) is a closed immersion, then it is in particular quasi-compact, thus \( f \) is quasi-separated. Now if there are two dotted-arrow making this diagram commutative, they define a point \( z \in (Y \times_X Y)(K, K^+) \) s.t. \( z|_{\text{Spa}(K, \mathcal{O}_K)} \in \Delta_f(Y)(K, \mathcal{O}_K) \). But \(|\Delta_f([Y])|\) is closed in \(|Y \times_X Y|\), so \( z \) maps \( \text{Spa}(K, K^+) \) into \(|\Delta_f([Y])|\) iff it maps \( \text{Spa}(K, \mathcal{O}_K) \) into \(|\Delta_f([Y])|\), as \( \text{Spa}(K, \mathcal{O}_K) \subset \text{Spa}(K, K^+) \) is dense. Now \( \Delta_f \) is an injection, so by (14.10.1.7), \( z \) factors through \( \Delta_f \) thus the two maps are equal.

3 \to 2: The condition implies that \(|\Delta_f| : |Y| \to |Y \times_X Y|\) is a quasi-compact locally closed immersion of locally spectral spaces which is moreover specializing. But because \(|\Delta_f|\) is quasi-compact, the image of \(|\Delta_f|\) is pro-constructible, and it is also closed under specialization, thus it is closed, Cf.[Sch17]P25.

\section{Pro-Étale Site and v-Site}

\textbf{Prop. (14.10.2.1).} if \((R, R^+)\) is the completed filtered colimit of perfectoid Huber pairs \((R_i, R_i^+)\), \(X_i = \text{Spa}(R_i, R_i^+)\), \(X = \text{Spa}(R, R^+)\), then base change induce equivalences of categories:

\begin{itemize}
  \item 2 \to \lim_i X_{i, \text{ét}} \cong X_{\text{fét}}.
  \item 2 \to \lim_i X_{i, \text{aff}} \cong X_{\text{ét}, \text{aff}}.
  \item 2 \to \lim_i X_{i, \text{ét}, \text{qcqs}} \cong X_{\text{ét}, \text{qcqs}}.
  \item 2 \to \lim_i X_{i, \text{ét}, \text{qc}, \text{sep}} \cong X_{\text{ét}, \text{qc}, \text{sep}}.
\end{itemize}

\textbf{Proof:} Cf.[Sch17]P27.

1 follows from almost purity theorem. \( \square \)

\textbf{Def. (14.10.2.2) [Pro-étale Morphism].} A map of perfectoid Huber pairs \((A, A^+) \to (B, B^+)\) is called \textbf{pro-étale} iff it is the completed filtered colimit of étale ring maps \((A, A^+) \to (A_i, A_i^+)\).

A morphism of perfectoid spaces is \textbf{pro-étale} if there is an affinoid covering \( V_i = \text{Spa}(R_i, R_i^+) \) of \( X \) that \( f^{-1}(V_i) \) have coverings \( U_{ij} = \text{Spa}(R_{ij}, R_{ij}^+) \) that \((R_i, R_i^+) \to (R_{ij}, R_{ij}^+)\) are all pro-étale.

In fact, by (14.10.2.7), if this is true for one affinoid covering \( V_i \) of \( X \), then this is true for any affinoid covering of \( X \).

\textbf{Prop. (14.10.2.3).} If \( S \) is a profinite set and \( X \) is a perfectoid space, then we can define a new perfectoid space \( X \times S \) as the inverse limit of \( X \times S_i \), where \( S = \varprojlim S_i \). Then \( X \times S \) is pro-étale over \( X \).
Prop. (14.10.2.4) [Immersion are Pro-Étale]. If \( f : Z \hookrightarrow X \) be a Zariski closed immersion with image \( V(I) \), then \( f \) is affinoid pro-étale. Then \( f(Z) \) can be written as the intersection of rational subsets

\[
U_{f_1, \ldots, f_n} = \{|f_1|, \ldots, |f_n| \leq |\varpi|\}
\]

for various \( n \) and \( f_1, \ldots, f_n \in I \). Then \( Z = \lim_{\leftarrow} U_{f_1, \ldots, f_n} \rightarrow X \), as it is a closed immersion thus an injection\((14.10.1.11)\), which shows \( Z \rightarrow X \) is pro-étale.

In particular, an immersion is also pro-étale because pro-étale can be checked analytically locally.

Cor. (14.10.2.5) [Diagonal Map is Pro-Étale]. If \( f : Y \rightarrow X \) is a map of perfectoid spaces, then \( \Delta_f : Y \rightarrow Y \times_X Y \) is pro-étale, by\((14.10.1.12)\).

Prop. (14.10.2.6). If \( X \) is an affinoid perfectoid space, then the functor

\[
\text{Pro}(X_{\text{aff}} \rightarrow X_{\text{pro-ét}}) : \lim_{\leftarrow i} (X_i) \mapsto \lim_{\leftarrow i} X_i
\]

is an equivalence of categories.

Proof: This map is essentially surjective by definition, To show it is fully faithful, it suffices to show that for \( Y = \lim_{\leftarrow i} \text{Spa}(Y_i, Y_i^+) \), \( Z = \lim_{\rightarrow j} \text{Spa}(Z_j, Z_j^+) \),

\[
\text{Hom}_X(Y, Z) = \lim_{\leftarrow j} \lim_{\rightarrow i} \text{Hom}(Y_i, Z_j).
\]

We need to show for any \( Z \rightarrow X \),

\[
\text{Hom}_X(Y, Z) = \lim_{\leftarrow i} \text{Hom}(Y_i, Z).
\]

Because \( 2 - \lim_i X_i,_{\text{ét, qcqs}} \simeq X_{\text{ét, qcqs}} \), we have

\[
\text{Hom}_X(Y, Z) = \text{Hom}_Y(Y, Y \times_X Z) = \lim_{\rightarrow i} \text{Hom}_{Y_i}(Y_i, Y_i \times_X Z) = \lim_{\leftarrow i} \text{Hom}_X(Y_i, Z).
\]

Prop. (14.10.2.7) [Properties of Pro-Étale Morphisms].

- (Affinoid)Pro-Étale maps are stable under composition and pullbacks.
- Let \( f : Y \rightarrow X, f' : Y' \rightarrow X \) be (affinoid)pro-étale, then any map \( g : Y \rightarrow Y' \) over \( X \) is also (affinoid)pro-étale.
- For any affinoid perfectoid space \( X \), the category \( X_{\text{aff \, pro-ét}} \) has all finite limits.

Proof: 1: Composition is obvious, pro-étale maps are stable under pullbacks because étale maps do.

2: We can factor \( g \) as a section of the map \( Y \times_X Y' \rightarrow Y \) and the projection map \( Y \times_X Y' \rightarrow Y' \). Thus it suffices to show a section of a pro-étale map is pro-étale. But if \( Y = \lim_{\leftarrow i} Y_i \rightarrow X \) is pro-étale, then a section is given by compatible sections \( s_i : X \rightarrow Y_i \). Then \( X = \lim_{\leftarrow i} (X \times_Y Y_i) \rightarrow X \) is pro-étale.

3: This is because \( X_{\text{aff}} \) has finite limits, because it has a final object and fiber products\((10.3.9.17)\).
**Def. (14.10.2.8) [Big Pro-Étale Site].** Consider the following categories:
- Perf, the category of perfectoid spaces.
- $X_{\text{pro-ét}}$, the category of perfectoid spaces pro-étale over $X$, where $X$ is a perfectoid space.
- $X_{\text{aff, pro-ét}}$, the category of affinoid perfectoid spaces pro-étale over $X$.

The **big pro-étale site** is the category Perf endowed with the topology that a family of maps $\{f_i : Y_i \to X\}$ is a covering if all $f_i$ are pro-étale and for any quasi-compact open subset $U \subset X$, there is a finite set $J \subset I$ and quasi-compact opens $V_j \subset Y_j$ that $U = \cup_{j \in J} f_j(V_j)$.

These truly form sites by (14.10.2.7).

**Cor. (14.10.2.9).** The presheaf $\mathcal{O} : X \mapsto \mathcal{O}_X(X), \mathcal{O}^+ : X \mapsto \mathcal{O}_X^+(X)$ on the big étale site are sheaves. If $X$ is affinoid perfectoid, then $H^i(X_{\text{pro-ét}}, \mathcal{O}) = 0$ for $i > 0$, and $H^i(X_{\text{pro-ét}}, \mathcal{O}^+)$ is almost zero for $i > 0$. Moreover, the big pro-étale site is subcanonical.

**Proof:** Firstly we can assume $X$ is affinoid because we already know $\mathcal{O}, \mathcal{O}^+$ are sheaves w.r.t. the analytic topology. Let $Y \to X$ be an affinoid pro-étale covering of $X$, where $Y = \text{Spa}(R_{\infty}, R_{\infty}^+)$, $(R_{\infty}, R_{\infty}^+) = (\lim_{n \to \infty} (R_i, R_i^+))^\sim$. Then fixing a pseudo-uniformizer $\varepsilon$ of $R$, the complexes

$$0 \to R^+ / \varepsilon \to R_i^+ / \varepsilon \to \cdots$$

is almost exact, because $H^i(X_{\text{ét}}, \mathcal{O}_X^+ / \varepsilon)$ is almost zero for $i > 0$. Now take a direct limit over $i$, then

$$0 \to R^+ / \varepsilon \to R_{\infty}^+ / \varepsilon \to \cdots$$

is almost exact. Now by induction on $n$, we can prove

$$0 \to R^+ / \varepsilon^n \to R_{\infty}^+ / \varepsilon^n \to \cdots$$

is almost exact. Then by passing to the direct limit,

$$0 \to R^+ \to R_{\infty}^+ \to \cdots$$

is almost exact. Then by inverting $\varepsilon$,

$$0 \to R \to R_{\infty} \to \cdots$$

is exact. These give us the desired results. Notice $\mathcal{O}^+$ is a sheaf because it is the elements of valuations $\leq 1$ everywhere by (14.8.3.7).

For the final assertion, if $\{Y_i \to Y\}$ is a pro-étale covering of $Y$, and $g_i : Y_i \to X$ are maps that agree on $Y_i \times_X Y_j$, then firstly we can glue these maps together topologically to a map $|Y| \to |X|$. So this problem can be considered locally on $X$, so we may assume $X = \text{Spa}(R, R^+)$ is affinoid, and maps $(R, R^+) \to (\mathcal{O}(Y_i), \mathcal{O}^+(Y_i))$ that agree on the overlap (14.8.4.4), then they glue to a map $(R, R^+) \to (\mathcal{O}(Y), \mathcal{O}^+(Y))$, as $\mathcal{O}, \mathcal{O}^+$ are all sheaves, and this gives a morphism $Y \to X$.

**Prop. (14.10.2.10) [Strictly TotallyDisconnected Pro-Étale Cover].** Let $X$ be an affinoid perfectoid space, then there is an affinoid perfectoid space $\tilde{X}$ with an affinoid pro-étale surjective and universally open map $\tilde{X} \to X$ that $\tilde{X}$ is strictly totally disconnected.

**Proof:** Cf. [Sch17] P35.
**Prop. (14.10.2.11).** The presheaf $\mathcal{O}, \mathcal{O}^+$ are sheaves w.r.t. the $v$-topology. Moreover, the $v$-site is subcanonical.

*Proof:* Cf. [Sch17]P40.

**Prop. (14.10.2.12).** Let $X$ be an affinoid perfectoid space, then $H^i_v(X, \mathcal{O}) = 0$ for $i > 0$, and $H^i_v(X, \mathcal{O}^+)$ is almost zero for $i > 0$.

*Proof:* Cf. [Sch17]P41.

**Descent on Pro-Étale Site**

**Prop. (14.10.2.13) [Descent May Fail].** The question is whether the fibered category over $\text{Perfd}$:

$$X \mapsto \{\text{Perfectoid Spaces } Y \to X\}$$

is a stack for the pro-étale topology. This fails in general. An evidence is that the fibered category

$$X \mapsto \{\text{Affinoid Perfectoid Spaces } Y \to X\}$$

is not a stack on the category of affinoid Perfectoid spaces with the analytic topology, let along the pro-étale topology:

Let $X = \text{Spa} K(x, y)$, and $V \subset X$ be $\{(x, y)| |x| = 1 \text{ or } |y| = 1\}$, then $V$ is covered by two affinoids, but is not an affinoid itself: $H^1(V, \mathcal{O}_V) = \bigoplus_{m,n>0} Kx^{-m}y^{-n} \neq 0$. But there is a standard rational covering $X = \bigcup_i X(\frac{1}{f_i}f_i, f_i)$, where $f_1 = \infty, f_2 = x, f_3 = y$, and

$$U_0 \cap V = \emptyset, \quad U_1 \cap V = \{|x| = 1\} \subset U_1, \quad U_2 \cap V = \{|y| = 1\} \subset U_2$$

are all affinoid. There is a similar example in the perfectoid case, thus

$$X \mapsto \{\text{Affinoid Perfectoid Spaces } Y \to X\}$$

is not a stack.

**Prop. (14.10.2.14) [Pro-étale is not Pro-étale Local].** There is an example of a non-pro-étale map that is pro-étale locally pro-étale.


**Prop. (14.10.2.15) [Characterization of Locally pro-étale Maps].** Let $f : X \to Y$ be a morphism of affinoid perfectoid spaces, then the following are equivalent:

- There exists an affinoid pro-étale cover $Y' \to Y$ s.t. the base change $X' = X \times_Y Y' \to Y'$ is pro-étale.
- For all geometric points $\text{Spa} C \to Y, X \times_Y \text{Spa} C = \text{Spa} C \times S$ for some profinite set $S$.


**Prop. (14.10.2.16) [Descent].** Descent data of the the fibered category

$$X \mapsto \{\text{Perfectoid Spaces } Y \to X\}$$

of a perfectoid space $Y' \to X'$ along a pro-étale cover $X' \to X$ is effective in the following cases:
• If $X, X', Y'$ are affinoids and $X$ is totally disconnected.
• If $f$ is separated and pro-étale and $X$ is strictly totally disconnected.
• If $f$ is separated and étale. In particular, the fibered category
  \[ X \mapsto \{ \text{separated étale } X \to Y \} \]
  is a stack over the category of perfectoid spaces with the pro-étale topology.
• If $f$ is finite étale. In particular, the fibered category
  \[ X \mapsto \{ \text{finite étale } X \to Y \} \]
  is a stack over the category of perfectoid spaces with the pro-étale topology.

**Proof:** Cf.\[Sch17\]P9.3, 9.6, 9.7. \qed

### 3 Morphisms of $v$-Stacks

**Def.(14.10.3.1)[Étale Morphism of Stacks].** Let $f : Y' \to Y$ be a map of pro-étale stacks on the category $\text{Perfd}$,

- Assume $f$ is locally separated (i.e. there is an open cover of $Y'$ over which $f$ becomes separated), then $f$ is called **quasi-pro-étale** if for any strictly totally disconnected perfectoid space $X$ and a map $X \to Y$, the pullback $Y' \times_Y X$ is representable and $Y' \times_Y X \to X$ is pro-étale.
- Assume $f$ is locally separated, then $f$ is called **étale** if for any perfectoid space $X$ and a map $X \to Y$, the pullback $Y' \times_Y X$ is representable and $Y' \times_Y X \to X$ is étale.
- $f$ is called **finite étale** if for any perfectoid space $X$ and a map $X \to Y$, the pullback $Y' \times_Y X$ is representable and $Y' \times_Y X \to X$ is finite étale.

### 4 Diamonds

**Remark(14.10.4.1)[Motivation of Diamonds].** The idea of diamonds is that there should be a functor

\[ \diamond : \{ \text{analytic adic spaces over } \mathbb{Z}_p \} \to \{ \text{diamonds} \} \]

that forgets the structure morphism to $\mathbb{Z}_p$. For a perfectoid space $X$, $X \mapsto X^f-lat$ has this property, so this functor should coincides on these objects. Now any analytic adic space $X$ over $\mathbb{Z}_p$ is pro-étale locally perfectoid:

\[ X = \text{Coeq}(\tilde{X} \times_X \tilde{X} \Rightarrow X), \]

where $\tilde{X} \to X$ is a pro-étale perfectoid cover. The equivalence relations $R = \tilde{X} \times_X \tilde{X}$ is also perfectoid, so this functor should send $X$ to $\text{Coeq}(R^p \Rightarrow \tilde{X}^p)$.

For example, if $X = \text{Spa}(\mathbb{Q}_p)$, then a pro-étale cover of $X$ is $\text{Spa}(\mathbb{Q}^{cyc}_p \wedge)$, and then $R = \tilde{X} \times_X \tilde{X} = \tilde{X} \times \mathbb{Z}_p^*$ by Galois theory, and then $\mathbb{Q}^c_p$ should be defined as the coequalizer of $\text{Spa}(\mathbb{Q}^{cyc}_p)/\mathbb{Z}_p^*$, whose meaning is explained in (14.10.4.10).

**Def.(14.10.4.2)[Diamonds].** A **diamond** is a pro-étale sheaf $\mathcal{D}$ on $\text{Perf}$ that can be written as $\mathcal{D} = X/R$, where $X \in \text{Perf}$ and $R$ is a pro-étale equivalence relation in $X \times X$ (i.e. an equivalence relation that the maps $s, t : R \to X$ are pro-étale), and also $R$ is representable.
Prop. (14.10.4.3). Let $X \in \text{Perf}$ and $R \subset X \times X$ a representable pro-étale equivalence relation, then

- The quotient sheaf $Y = X/R$ is a diamond.
- The natural map of sheaves $R \to X \times Y$ is an isomorphism.
- Let $\tilde{X} \to X$ be a pro-étale cover by a perfectoid space $\tilde{X}$, and $\tilde{R} = R \times_{X \times X} (\tilde{X} \times \tilde{X})$ the induced equivalence relation, then $\tilde{R}$ is a representable pro-étale equivalence relation of $\tilde{X}$, and the natural map $\tilde{Y} = \tilde{X}/\tilde{R} \to Y = X/R$ is an isomorphism.
- The map $X \to Y$ is quasi-pro-étale(14.10.3.1).

Proof: 1 is by definition.

For 2, firstly $R \to X \times Y$ is injective as subsheaves of $X \times X$. Next, if $Z \to X \times Y$ is any map from a perfectoid space $Z$, then we have two maps $a, b : Z \to X$ that their composition with $X \to Y$ agree. This means after passing to a pro-étale covering $\tilde{Z} \to Z$, the composition map $\tilde{Z} \to Z \to X \times X$ factors through $R$. Now this map $\tilde{Z} \to R$ descends to a map $Z \to R$, because pro-étale site is subcanonical and the two projection maps $\tilde{Z} \times Z \to R$ coincides because they do after compositing with $R \to X \times X$.

3: Firstly $\tilde{R}$ is representable as fiber products of representable objects(14.8.5.9), and the two projections are pro-étale, as they are compositions of base changes of pro-étale morphisms. Also the map $\tilde{Y} \to Y$ of pro-étale sheaves is surjective, as the composition $\tilde{X} \to X \to Y$ is.

To show $\tilde{Y} \to Y$ is injective, let $Z$ be a perfectoid space with two maps $Z \to \tilde{Y}$ that coincide after compositing with $\tilde{Y} \to Y$, we need to show $a = b$. Now because pro-étale site is subcanonical, it suffices to show this after replacing $Z$ with a pro-étale cover $\tilde{Z}$, such that $a, b$ factors over $\tilde{a}, \tilde{b} : Z \to \tilde{X}$. The associated map $Z \to \tilde{X} \times \tilde{X} \to X \times X$ factors through $R$ by item2, so we get a map $Z \to R \times_{X \times X} (\tilde{X} \times \tilde{X}) = \tilde{R}$, which means $\tilde{a}, \tilde{b}$ induces the same map $Z \to \tilde{Y}$. So we are done.

4: By 3, we can replace $X \to \tilde{X} = \bigsqcup U_i \to X$, where $U_i$ is an affinoid cover of $\tilde{X}$, and $R$ by the the induced equivalence relation in $\tilde{X} \to X$, and to pro-étale is analytically local. In this way, we may assume $R \subset X \times X$ and $X \times X \to X$ are separated.

Let $X'$ be a strictly totally disconnected perfectoid space and $X' \to X$ be a map. Because $X \to Y$ is surjective as sheaves on Perf, there is a pro-étale cover $\tilde{X}' \to X'$ and a map $\tilde{X}' \to X$ lying over $X' \to Y$. We can assume $\tilde{X}'$ is affinoid. Let $W = X' \times_Y X \to X'$ be the fiber product, then

$$\tilde{X}' \times_X W = \tilde{X}' \times_X (X \times_Y X) = \tilde{X}' \times_X R$$

is representable and pro-étale over $\tilde{X}'$, and also separated. So by(14.10.2.16), $W$ is also representable, pro-étale and separated over $X$. □

Cor. (14.10.4.4)[Equivalent Characterization of Diamonds]. Let $Y$ be a pro-étale sheaf on Perf, then $Y$ is a diamond iff there is a surjective quasi-pro-étale morphism $X \to Y$ from a perfectoid space $X$. If $X$ is a disjoint union of strictly totally disconnected spaces, then $R \subset X \times_Y X \subset X \times X$ is a representable pro-étale equivalence relation with $Y = X/R$.

Proof: If $Y$ is a diamond, then $X \to Y$ is quasi-pro-étale by(14.10.4.3). Conversely, if there is a quasi-pro-étale morphism $X \to Y$, by(14.10.2.10), we can assume that $X$ is a disjoint union of strictly disconnected spaces. In this case, by the definition of quasi-pro-étale, $R$ is representable and the projections $R = X \times_Y X \to X$ is pro-étale, and $X/R \cong Y$: it suffices to show this map is injective: if $a, b : Z \to X$ are two maps that coincide after composing with $X \to Y$, then after replacing to a pro-étale covering $\tilde{Z} \to Z$, we can lift to maps $(\tilde{a}, \tilde{b}) : \tilde{Z} \to R$. And this map descend
to a map $Z \to R$, because the pullback to $\mathcal{Z} \times_Z \mathcal{Z} \to R$ coincides as they do after composing with $R \to X \times X$. So $X/R \to Y$ is injective. \qed

**Cor. (14.10.4.5).**
- Let $Y$ be a pro-étale sheaf on Perf and there is a quasi-pro-étale map $Y' \to Y$, where $Y'$ is a diamond, then $Y$ is also a diamond.
- Let $f : Y' \to Y$ be a quasi-pro-étale map of pro-étale sheaves on Perf and $Y$ is a diamond, then $Y'$ is also a diamond.

**Proof:**
1: By (14.10.4.4), we can choose a quasi-pro-étale map $X \to Y'$ where $X$ is a perfectoid space, then $X \to Y' \to Y$ is also quasi-pro-étale, so $Y$ is a diamond by (14.10.4.4) again.
2: Choose a surjective quasi-pro-étale map $X \to Y$ where $X$ is a perfectoid space, then $X' \times_X Y$ is representable and $X' \to Y'$ is quasi-pro-étale and surjective, thus $Y'$ is a diamond by (14.10.4.4). \qed

**Lemma (14.10.4.6).** The absolute product of two perfectoid spaces of char $p$ is also a perfectoid space.

**Proof:** Cf. [Sch17] P71. \qed

**Prop. (14.10.4.7) [Absolute Product of Diamonds].** Let $\mathcal{D}, \mathcal{D}'$ be diamonds, then the product sheaf $\mathcal{D} \times \mathcal{D}'$ is also a diamond.

**Proof:** Let $\mathcal{D} = X/R$ and $\mathcal{D}' = X'/R'$, then $R \times R'$ is also representable by (14.10.4.6), $R \times R' \to (X \times X') \times (X \times X')$ is also an injection, and the projections are pro-étale. Thus $\mathcal{D} \times \mathcal{D}' = (X \times X')/(R \times R')$ is a diamond, by (14.10.4.3). \qed

**Prop. (14.10.4.8) [Fiber Products].** Fiber products exist in the category of diamonds.

**Proof:** Let $Y_1 \to Y_2 \leftarrow Y_3$ be a diagram of diamonds. Choose representations $Y_i = X_i/R_i$, and after replacing $X_1, X_2$ with a pro-étale covering using (14.10.4.3), we can assume there are maps $X_i \to X_3$ lying over $Y_i \to Y_3$. Moreover, we can replace $X_i$ by $X_i \times X_3$ to assume that $X_i \to X_1 \times X_3$ is surjective in the pro-étale topology.

In this case, the map $X_1 \times X_3 \to Y_1 \times Y_3$ is surjective in the pro-étale topology, and the equivalence relation $R_4 = X_4 \times X_4$ can be calculated to be $R_4 = R_1 \times R_3 R_2$, which is representable. It remains to see that $R_4 \to X_4$ is pro-étale. But $R_1 \times R_2 \to X_1 \times X_2$ is pro-étale, so does its base change $R_1 \times X_3 R_2' \to X_1 \times X_3 X_2' = X_4$, and also $R_4 = R_1 \times R_3 R_2 \to R_1 \times X_3 R_2$ is pro-étale because it is the base change of $R_3 \to R_3 \times X_3 R_3$, which is pro-étale by (14.10.2.5). \qed

**Prop. (14.10.4.9).** Let $Y$ be a diamond, then $Y$ is a sheaf for the $\nu$-topology.

**Proof:** Cf. [Sch17] P54. \qed

$\text{Spd}(Q_p)$

**Prop. (14.10.4.10).** Let $\text{Spd}(Q_p)$ be defined as

$$\text{Spa}((Q_p^{\text{cycl}})^\gamma)/\mathbb{Z}_p^* = \text{Spa}(\mathbb{F}_p((t^{1/p^\infty}))/\mathbb{Z}_p^*),$$

where $\mathbb{Z}_p^*$ acts on $\mathbb{F}_p((t^{1/p^\infty}))$ via $\gamma(t) = (1 + t)^\gamma - 1$ (10.3.8.16). To be precise, it is the coequalizer of

$$\mathbb{Z}_p^* \times \text{Spa}(\mathbb{F}_p((t^{1/p^\infty}))) \Rightarrow \text{Spa}(\mathbb{F}_p((t^{1/p^\infty})))$$
where one map is projection and the other map is the group action. To show this is diamond, we first need to verify this is an injection thus an equivalence relation, which is by (14.10.4.11).

**Lemma (14.10.4.11).** Consider the map
\[ g : \mathbb{Z}_p^* \times \text{Spa}(\mathbb{F}_p((t^{1/p^\infty}))) \to \text{Spa}(\mathbb{F}_p((t^{1/p^\infty}))) \times \text{Spa}(\mathbb{F}_p((t^{1/p^\infty}))) \]
where the first map is group action and the second map is projection, then this is an injection map.

**Proof:** For any perfectoid affinoid field \((K, K^+), \mathbb{Z}_p^* \) acts freely on the topological nilpotent elements of \(K\), thus the map is an injection. \(\square\)

**Prop. (14.10.4.12) [Torsor over Affinoid Perfectoid Space].** Let \(G\) be a profinite group and \(f : \mathcal{F}' \to \mathcal{F}\) be a \(G\)-torsor, with \(G\) profinite, then for any affinoid \(X = \text{Spa}(B, B^+)\) and any morphism \(X \to \mathcal{F}\), the pullback \(\mathcal{F}' \times_{\mathcal{F}} X\) is representable by a perfectoid affinoid \(X' = \text{Spa}(A, A^+)\), where \((A, A^+)\) is the completed filtered colimit of \((A_H, A_H^+)\), where for each open normal subgroup \(H\) of \(G\), \(A_H/B\) is a finite étale \(G/H\)-torsor.

**Proof:** If \(H\) is an open normal subgroup of \(G\), then \(\mathcal{F}'/H \to \mathcal{F}\) is a \(G/H\)-torsor, and \(\mathcal{F}' = \varprojlim_H \mathcal{F}'/H\), thus we reduce to the case \(G\) is finite. But for this case, we use the fact \(\{\text{perfectoid spaces finite étale over } X\} = \text{stack}(14.10.2.16)\), and the definition of \(G\)-torsor. \(\square\)

**Prop. (14.10.4.13) [Description of \(\text{Spd}(\mathbb{Q}_p)\)].** If \(X = \text{Spa}(R, R^+)\) is an affinoid perfectoid space of characteristic \(p\), then \((\text{Spd}_p)\)(\(X\)) is the set of isomorphism classes of data of the following shape.

- A \(\mathbb{Z}_p^*\)-torsor \(R \to \bar{R}\), i.e. \(\bar{R} = (\lim \mathbb{Q}_p)\wedge, \) where \(R_n/R\) is finite étale with Galois group \((\mathbb{Z}/p^n\mathbb{Z})^*\).

- A topological nilpotent unit \(t \in \bar{R}\) s.t. for all \(\gamma \in \mathbb{Z}_p^*\), \(\gamma(t) = (1 + t)^\gamma - 1\).

**Proof:** Notice \(\text{Spa}(\mathbb{Q}_p^{cyd}) \to \text{Spd}(\mathbb{Q}_p)\) is a \(\mathbb{Z}_p^*\)-torsor by definition, so for any morphism \(X \to \text{Spd}(\mathbb{Q}_p)\), the pullback \(\text{Spa}(\mathbb{Q}_p^{cyd}) \times_{\text{Spd}(\mathbb{Q}_p)} X \to X\) is also a \(\mathbb{Z}_p^*\)-torsor, so it is isomorphic to a torsor \(\text{Spa}(\bar{R}, \bar{R}^+) \to \text{Spa}(R, R^+)\) by (14.10.4.12), and the map \(\text{Spa}(\mathbb{Q}_p^{cyd}) \times_{\text{Spd}(\mathbb{Q}_p)} X \to X \to \text{Spa}(\mathbb{Q}_p^{cyd})\) is an \(\mathbb{Z}_p^*\)-equivariant map, which is equivalent to a topologically nilpotent element \(t \in \bar{R}\) that is equivariant, i.e. \(\gamma(t) = (1 + t)^\gamma - 1\).

Conversely, for any such a \(\mathbb{Z}_p^*\)-torsor \(R \to \bar{R}\), an equivariant element \(t \in \bar{R}\) descends to a map \(X \to \text{Spd}(\mathbb{Q}_p)\). \(\square\)

**Prop. (14.10.4.14).** The category of perfectoid spaces over \(\mathbb{Q}_p\) is equivalent to the category of perfectoid spaces \(X\) of characteristic \(p\) equipped with a structure morphism \(X \to \text{Spd}(\mathbb{Q}_p)\).

**Proof:** Consider the category of triples \((X^\sharp, X, \iota)\), where \(X^\sharp\) is a perfectoid space over \(\mathbb{Q}_p\), \(X\) is a perfectoid space of characteristic \(p\), \(\iota : X^{\flat} \cong X\) is an isomorphism. A map of triples is a tuple \((f^\sharp, f) : (X^\sharp, X, \iota) \to (Y^\sharp, Y, \iota')\) that \(\iota' \circ f^\flat = f \circ \iota\).

This category is equivalent to the category of perfectoid spaces over \(\mathbb{Q}_p\) by the forgetful functor, where the quasi-inverse is given by \(X^\sharp \mapsto (X^\sharp, X^\flat, \text{id}_{X^\flat})\). And this category is also fibered in equivalent relations over Perf. So it is equivalent to a presheaf \(\text{Unilt}_\mathbb{Q}_p\), which maps \(X\) to the isomorphism classes of untilts \((X^\sharp, \iota)\) over \(\mathbb{Q}_p\), where \(\iota : X^{\flat} \cong X\) is an isomorphism, by (3.1.7.31).

Similarly we can show define a functor \(\text{Unilt}\) which maps \(X\) to the isomorphism classes of untilts \((X^\sharp, \iota)\) of whatever characteristic), where \(\iota : X^{\flat} \cong X\) is an isomorphism.
Let $X = \text{Spa}(R, R^+)$ be an affinoid perfectoid space of characteristic $p$. If $X^\sharp = \text{Spa}(R^\sharp, R^{\sharp+})$ is an untilt. Let $\tilde{X}^\sharp = X^\sharp \otimes_{Q_p} Q_p^{cyc}$, then $\tilde{X}^\sharp \to X^\sharp$ is a pro-étale $\mathcal{O}_p^*$-torsor, whose tilt $\tilde{X} \to X$ is a pro-étale $\mathcal{O}_p^*$-torsor equipped with a $\mathcal{O}_p^*$-equivariant map $\tilde{X} \to \text{Spa}(Q_p^{cyc})$; this is a morphism $X \to \text{Spd}(Q_p)$ by (14.10.4.13).

Conversely, let $\tilde{X} \to X$ be a pro-étale $\mathcal{O}_p^*$-torsor and $\tilde{X} \to \text{Spa}(Q_p^{cyc})$ a $\mathcal{O}_p^*$-equivariant map, then by tilting equivalence there exists a morphism $\tilde{X}^\sharp \to \text{Spa}(Q_p^{cyc})$ which is also $\mathcal{O}_p^*$-equivariant. The equivariance means that it is a descent datum along $\tilde{X} \to X$, so it descends to an untilt $X^\sharp$ of $X$ over $Q_p$.

Finally, for general affinoid perfectoid space $X$, as $\text{Untilt}_{Q_p}$ and $\text{Spd}(Q_p)$ are all sheaves on Perf, the above construction can be glued to give an isomorphism between them.

**Prop. (14.10.4.15) [Untilts is a Sheaf]**. $\text{Untilt}$ is a $v$-sheaf on the site Perf. So does $\text{Untilt}_{Q_p}$, because the invertibility of $p$ can be verified locally as $\mathcal{O}$ is sheaf.

**Proof**: Firstly $\text{Untilt}$ is clearly an analytic sheaf, so it suffices to show that if $X = \text{Spa}(R, R^+)$ is a perfectoid space of characteristic $p$ with a $v$-cover $Y = \text{Spa}(S, S^+) \to X$ and $Y^\sharp = \text{Spa}(S^\sharp, S^{\sharp+})$ is an untilt of $Y$ that the corresponding two untilts of $Z = Y \times_X Y$ agree, then there is a unique untilt $X^\sharp = \text{Spa}(R^\sharp, R^{\sharp+})$ whose pullback to $Y$ is $Y^\sharp$.

Cf. [Sch17] P86.
15 Representation Theory

15.1 Classical Representation Theory

In this section the representation theory over field $\mathbb{C}$ are studied (at least over a topological field of characteristic 0). Modular representations are studied in Modular Representations.

For classical representations, the theory of semisimple algebras should be kept in mind.

1 Topological Representations

Def. (15.1.1.1) [Representations]. Let $G$ be a topological group, $R$ be a topological ring with a $G$-action, then an $R$-representation of $G$ is a topological $R$-semi-linear on $M$ with an $R$-covariant action of $G$ on $M$ s.t. $G \times M \to M$ is continuous. The category of such representations is denoted by $\text{Rep}_R(G)$.

An irreducible representation is a representation that has no non-trivial invariant closed subspaces. An indecomposable representation is a representation that is not a direct sum of two subrepresentations.

Def. (15.1.1.2) [Constructing Representations]. Dual representations, tensor product, and symmetric and exterior tensors.

Def. (15.1.1.3) [Projective Representations]. A projective representation of a topological group $G$ on a TVS $V$ is a continuous map $G \times P(V) \to P(V)$, where the topology on $P(V)$ is induced from $V \setminus \{0\} \subset V$.

Prop. (15.1.1.4) [F.D. Schur’s Lemma]. Let $(\pi_1, V_1), (\pi_2, V_2)$ be an irreducible f.d. $\mathbb{C}$-representation of a topological group $G$, then $C(\pi_1, \pi_2) = \mathbb{C}$ if $\pi_1 \cong \pi_2$, and 0 otherwise.

Proof: This is because $\pi_i$ are irreducible as representations with discrete topology of $G$: Any subspace of $V_i$ is closed. So we reduce to (15.1.1.9). \qed

Def. (15.1.1.5) [Types of Representations]. Let $V$ be an irreducible f.d. $\mathbb{C}$-representation of a topological group $G$, then there are three possibilities:

- $V \not\cong V^*$, called a representation of complex type.
- There is an invariant symmetric form on $V$ inducing an isomorphism $V \cong V^*$, called a representation of real type.
- There is an invariant alternating form on $V$ inducing an isomorphism $V \cong V^*$, called a representation of quaternion type.

The category of representation of $K$-type is denoted by $\text{Rep}(G)_K$. 
Proof: By Schur’s lemma (15.1.1.4), either $V \not\cong V^*$ or there is a unique isomorphism $V \cong V^*$ up to scalar, which is equivalent to an invariant form $B$ on $V$. The two coordinate of this invariant form induces two isomorphisms $V \cong V^*$, which must be proportional, so $B(x,x) = cB(x,x)$, so $c = 0$ or $B(x,x) = 0$ for all $x$, which means $B$ is symmetric or alternating. □

**Def. (15.1.1.6) [Unitary Representations].** Usually we consider unitary representations on a Hilbert space. A unitary representation of a topological group $G$ on a Hilbert space $\mathcal{H}$ is defined to be a homomorphism from $G$ to the group $U(\mathcal{H})$ of unitary operators of $\mathcal{H}$ continuous in the strong operator topology (10.6.4.7). Notice by (10.6.4.8), this is equivalent to the unitary and continuous in the weak operator topology.

The category of unitary representations of $G$ is denoted by $\text{Rep.uni}(G)$.

**Def. (15.1.1.7) [Projective Unitary Representation].** A projective unitary representation of a topological group $G$ on a Hilbert space $\mathcal{H}$ is defined to be a continuous homomorphism from $G$ to the group $PU(\mathcal{H})$ of unitary operators of $\mathcal{H}$, where the topology of $PU(\mathcal{H})$ is induced from the strong operator topology of $U(\mathcal{H})$ (10.6.4.7). Notice by (10.6.4.8), this is equivalent to the unitary and continuous in the weak operator topology.

**Def. (15.1.1.8) [Character].** Let $\rho : G \to GL(n,V)$ be a linear representation of a group $G$. Then the character of $\chi_\rho$ is defined to be $\chi_\rho(g) = \text{tr}(\rho(g))$.

**Prop. (15.1.1.9) [Schur’s lemma].** If $(\pi,V)$ is an at most countable dimensional irreducible C-algebra representation of a topological C-algebra, then $\text{End}_A(V) \cong \mathbb{C}$. In particular this holds for $\dim A$ countable.

**Proof:** First the dimension of $\dim C \text{End}(V)$ is at most countable, because $V$ is acyclic by irreducibly, so $\dim C \text{End}(V) \leq \dim C V$. And $\text{End}(V)$ is a skew field, by irreducibility. So the result follows from (2.2.1.10). □

**Cor. (15.1.1.10).** Any irreducible representation of a commutative group has dimension 1.

**Cor. (15.1.1.11) [Index 2 Subgroup].** Let $G$ be a topological group and $H$ an open (normal) subgroup of index 2, $G = H \rtimes \{\sigma\}$. Let $(\pi,V)$ be an irreducible representation of $H$ of at most countable dimensional, then

1. $\text{res}_H^G \text{ind}_H^G \pi \cong \pi \oplus \pi^\sigma$.
2. $\pi \cong \pi^\sigma$ if $\pi$ is the restriction of an irreducible representation of $G$, called **type I**. And there are exactly two such extensions to $G$.
3. $\pi \not\cong \pi^\sigma$ if $\text{ind}_H^G \pi$ is an irreducible representation of $G$, called **type II**.

All these are true for unitarizable representations.

**Proof:**

1: This is clear.
2: If $\pi$ is a restriction of an irreducible smooth representation of $G$, then $\sigma$ intertwines $\pi$ and $\pi^\sigma$. Conversely, if $\pi \cong \pi^\sigma$, then there is an operator $A$ on $V$ that intertwines $\pi$ and $\pi^\sigma$, and then $A^2 = \text{id}$ by Schur’s lemma (15.1.1.9). Let $\sigma$ acts by $A$, then this representation extends to $G$.

3: If $\pi$ extends to $G$, then clearly $\pi$ appear in $\text{ind}_H^G \pi$ but not surjective, so $\text{ind}_H^G \pi$ is not irreducible. Conversely, if $\text{ind}_H^G \pi$ is not irreducible, notice $\text{res}_H^G \text{ind}_H^G \pi \cong \pi \oplus \pi^\sigma$, thus $\pi \cong \pi^\sigma$, otherwise any $G$-invariant subspace can only be $\pi$ or $\pi^\sigma$, so $\pi$ or $\pi^\sigma$ extends to representations of $G$, contradicting 2. □
Prop. (15.1.1.12). For any topological $G$ a topological ring $B$ with a $G$-action, $d \in \mathbb{N}$, there is a bijection between the set of equivalence classes of free $B$-representations $V$ of $G$ of rank $d$ and the category of $H^1(G, \text{GL}(d,B))$. Moreover, $V$ is trivial iff it is mapped to the distinguished point of $H^1(G, \text{GL}(d,B))$.

Proof: Cf. [Fontain-OuYang, P20]. □

Cor. (15.1.1.13). Let $L/K$ be a Galois extension of fields, then any f.d. $L$-representation of $\text{Gal}(L/K)$ is trivial.

Proof: □

Smooth Representations

Prop. (15.1.1.14) [Smooth Representations]. A smooth representation of a locally compact group $G$ on a complex vector space is a continuous representation w.r.t the discrete topology.

The category $\text{Rep}^{\text{alg}}(G)$ of smooth representations is a full Abelian subcategory of the category of continuous representations, and there is a right adjoint to the forgetful functor:

$$\text{Rep}(G) \to \text{Rep}^{\text{alg}}(G) : V \mapsto V^\infty = \bigcup_{K \leq G \text{ compact open}} V^K$$

So it preserves injectives and $\mathcal{M}(G)$ has enough injectives.

Def. (15.1.1.15) [Equivariant Sheaves]. Let $G$ be a locally compact group acting on a space $X$, let $p : G \otimes X \to X$ be the projection and $a : G \times X \to X$ be the action, then a equivariant sheaf on $X$ is a pair $(F, \rho)$, where $F$ is a locally constant complex sheaf on $X$ and $\rho$ is an isomorphism of sheaves $p^*(F) \cong a^*(F)$ that:

- $\rho$ is identity on $e \otimes X$.
- $p_{23}^* \rho \circ (\text{id}_G \times a)^* \rho = (m \times \text{id}_X)^* \rho$ on $G \times G \times X$.

Prop. (15.1.1.16). If $X$ is a pt with the trivial $G$-action, then a equivariant sheaf on $X$ is equivalent to a representation of $G$.

Proof: For any equivariant sheaf on $X$, the pullback are just locally constant functions of $G$ with value in $V$. Then $\rho$ on each stalk $g$ defines an action of $g$ on $V$. Compatibility with the $G$-action shows that this is a group action. And consider the stalk at $e$, because $\rho$ is id at $e$, for each $v$, there is an open nbhd $U$ that $\rho(u)v = v$ on for $u \in U$, thus it is smooth. The converse is obvious. □

Def. (15.1.1.17) [Coinvariants]. The Jacquet functor $J_G : \text{Rep}(G) \to \text{Vect}_C$ is the functor mapping a representation $V$ of $G$ to $V/V(G)$, where $V(G)$ is spanned by $\pi(g)v - v$. It is equivalent to the functor $V \mapsto V \otimes_G C$.

Let $\psi$ be a character of $G$, then we can more generally define $J_{G,\psi} : \text{Rep}(G) \to \text{Vect}_C$ is the functor mapping a representation $V$ of $G$ to $V/V_{G,\psi}$, where $V_{G,\psi}$ is spanned by $\pi(g)v - \psi v$. It is equivalent to the functor $V \mapsto V \otimes_G C_\psi$, or equivalently $J_{G,\psi} = J_G \circ (\psi^{-1} \otimes)$.

Prop. (15.1.1.18). If $G$ is compact, then $e_G V = V^G = V/V(G)$.

And if $G$ is a union of increasing family of compact groups, then $J_G$ is exact, so is $J_{G,\psi}$.
Proof: $J_G$ is clearly right exact. And if $G$ is compact, $e_G V = V^G = V/(G)$: if $\pi(G)v = v$, then $v = e_G v$, and if $e_G v = 0$, then because $v$ is smooth, $\sum_{h_i \in G/K} h_i v = 0$, thus $v = \frac{1}{|G/K|}(v - h_i v)$ is in $V(G)$.

If $G$ is a union of compact groups $K_i$, then $V/V(G) = \text{colim} V/V(K_i)$ is exact. \hfill \qed

**Prop. (15.1.1.19).** If $G$ is a union of increasing family of compact open subgroups $\{K_i\}$, then $v \in V(G, \psi)(\psi$ can be trivial) iff for some $K_\alpha$, $\int_{K_\alpha} \psi^{-1}(h)\pi(h)v dh = 0$.

**Proof:** We can assume $\psi$ is trivial. If $v = \pi(h)w - w$ and $h \in K_\alpha$, then $\int_{K_\alpha} \psi^{-1}(h)\pi(h)v dh = 0$.

Conversely, by the proof of (15.1.1.18), $V(G) = \cup V(K_\alpha) = \cup \ker(e_{K_\alpha})$, which is equivalent to $\int_{K_\alpha} \pi(h)v dh = 0$. \hfill \qed

**Def. (15.1.1.20)** **[Contragradient Representation]**. For a smooth representation $V$ of $G$, the **contragradient smooth representation** $V'^* = (V^*)^\infty$ is the smooth part of $V^*$.

**Prop. (15.1.1.21).** Let $E$ be a smooth or f.d. representation of a topological group $G$, then

- $E$ has an irreducible subquotient.
- If $E$ is f.g., then it has an irreducible quotient.

**Proof:** 2: Use Zorn’s lemma for the set of proper $G$-subspaces of $U$, the union of a chain of proper $G$-subspaces is proper, because it is f.g. So it has a maximal proper $G$-space, thus the quotient is irreducible.

1 follows from 2 by choosing a f.g. submodule. \hfill \qed

**Prop. (15.1.1.22)** **[Induced Representation]**. The induced and compactly induced representations have the following equivalent forms:

\[
\text{Ind}^G_H(V) = \text{Hom}_{Z[H]}(Z[G], V), \quad \text{ind}^G_H(V) = Z[G] \otimes_{Z[H]} V.
\]

I.e., if $H$ acts on $V$ by $\rho$, then $\text{ind}^G_H(\rho)$ is the space $\oplus_{\gamma \in G/H} V_{\gamma}$ where $V_{\gamma} \cong V \in \text{Mod}_H$, and that for $v_{\gamma} \in V_{\gamma}$, $(\text{Ind}(\rho)g)v_{\gamma} = \rho(h)v_{\gamma'} \in V_{\gamma'}$ where $g\gamma = \gamma'h$ that $\gamma' \in G/H, h \in H$.

**Proof:** Choose a set of left coset representatives $\Gamma$ of $G/H$, then $\Gamma^{-1}$ is a set of right coset representatives for $H\backslash G$. Now $Z[G] = \oplus_{\gamma \in \Gamma} Z[H] \gamma^{-1}$, and we define the space $V_{\gamma} \cong V$ of maps from $Z[H]$ to $V$ determined by: $v_{\gamma}(g) = \rho(g\gamma)v \in V$ if $g \in H\gamma^{-1}$ and 0 otherwise.

Then $\text{Ind}(\rho)(V) = \oplus_{\gamma \in \Gamma} V_{\gamma}$ that for $v_{\gamma} \in V_{\gamma}$, $(\text{Ind}(\rho)g)v_{\gamma}$ is the map $Z[G]$ to $V$ determined by: $(\text{Ind}(\rho)g)v_{\gamma}(g') = \rho(g'\gamma'h)v \in V$ if $g' \in H(\gamma')^{-1}$, and 0 otherwise, where $g\gamma = \gamma'h$. Then $(\text{Ind}(\rho)g)v_{\gamma} = \rho(h)v_{\gamma'}$, which is the same as the formula for $\text{Ind}(\rho)$ as in (15.1.1.22). So the map $v_{\gamma} \rightarrow v_{\gamma'} : \text{Ind}(\rho) \rightarrow \text{Ind}(\rho)$ is an isomorphism in $Z[G] - \text{Mod}$. \hfill \qed

**Prop. (15.1.1.23)** **[Clifford’s Theorem]**. If $\rho : G \rightarrow GL(V)$ is a semisimple smooth or f.d. representation and $H$ is a normal subgroup of $G$, then $\rho|_H$ is also semisimple.

In particular, a normal Abelian subgroup acts by scalars on any irreducible $C$-representation of $G$, by (15.1.1.10).

**Proof:** Use definition (2.4.1.4), we reduce to the case $\rho$ is simple. Now an $H$-subrepresentation is simple iff it has no proper $H$-subrepresentations, so clearly $G$ maps a simple $H$-subrepresentation to another simple $H$-subrepresentation. So if $W$ is the sum of all simple $H$-subrepresentations, then $G$ preserves $W$, which shows $W = V$, and $V$ is $H$-semisimple by (2.4.1.4). \hfill \qed
Prop. (15.1.1.24) [Restriction]. If $G$ is a group and $H$ is an open normal subgroup of $G$ of finite index $n$. Let $(\pi, V)$ be a smooth representation of $G$ of f.d. over a field of characteristic $p \nmid n$, then

- If $\pi|_H$ is completely reducible, then $\pi$ is also completely reducible.
- If $(\pi, V)$ is irreducible, then $\pi|_H = \pi_1 \oplus \ldots \oplus \pi_k$ where $\pi$ are irreducible representations of $H$ and $k \leq [G : H]$.
- If $(\pi, V)$ is irreducible, the isotopy parts of $H$ are all of the same dimension, and if there are more than 1 isotopy classes, then $G$ is an induced representation.

Moreover, item 2, 3 are also true for $H$ open normal in $G$ s.t. $H \mathbb{Z}(G)$ is of finite index $n$.

Proof: Let $g_1, \ldots, g_n$ be a coset representation of $G/H$.

1: If $V_1$ is a $G$-submodule of $V$, then $V_1$ has a complementary $H$-submodule $V^\perp_1$. Let $P_0$ be the projection of $V$ onto $V_1$ along $V^\perp$, then $P = \frac{1}{p} \sum \pi(g) P_0 \pi(g)^{-1}$ is a projection of $V$ onto $V_1$ that commutes with $G$-action. Therefore the kernel of $P$ is a $G$-submodule of $V$ that is complementary to $V_1$.

2: Let $v \in V$, then $\{\pi(g_i)v\}$ generates $V$ as a $H$-representation, thus by (15.1.1.21) there is an $H$-submodule $V' \subset V$ that $V/V'$ is irreducible. Let $V_i = \pi(g_i)V'$, then $V/V_i$ are also irreducible representations of $H$. Consider the $H$-invariant map $V \mapsto \oplus V/V_i$, its kernel is $G$-invariant, thus $V$ is a submodule of $\oplus V/V_i$, and the assertion follows.

3: The $G$-action permutes with isotopy classes. And if there are more than 1 classes, choose the stabilizer $G_\rho$ of one $V_\rho$, then $V = \text{Ind}_{G_\rho}^{G} V_\rho$ by (15.1.1.22). \qed

Prop. (15.1.1.25) [Kolchin]. Let $G$ be a discrete group acting on a f.d. vector space $V$ s.t. each $g \in G$ acts via a unipotent endomorphism, then there is a basis s.t. $G$ is mapped into $U(n, T)$.

Proof: Cf. [Mil17] P279. \qed

Unitary Representations of Locally Compact Groups

For unitary representations of locally compact groups, see 10.9.

2 Linear Representation of Finite Groups

Basic references are [Ser77], [A-B95]. [群表示论 notes 薛航].

Remark (15.1.2.1). The representations in this subsection is assumed to be of f.d. over a field of char0, in particular, over a subfield of $\mathbb{C}$. In particular, there is no need to consider topologies.

Because a finite group is compact, all results of compact groups apply to a finite group, see 4.

Because a finite group is locally profinite, all results of locally profinite groups apply to finite groups 1.

Prop. (15.1.2.2) [Orthogonality of Characters]. The characters $\chi_i$ of irreducible representations of $G$ form a basis of $\text{ZL}^2(G)$ by (10.9.4.30). Also, for $s \in G$, let $c(s)$ be the number of elements in the conjugacy class of $s$, then:

- $\int |\chi_i(s)|^2 = g/c(s)$.
- If $t$ is not conjugate to $s$, then $\sum_i \chi_i(s)^* \chi_i(t) = 0$.

Proof: The last assertion follows from the first one, if you consider a matrix with conjugacy classes as column and characters as rows, and place $\sqrt{c(s)/g} \chi_i(s)$ in the entries, then it is an orthogonal matrix. \qed
Cor. (15.1.2.3) [Representations Determined by Characters]. A representation of $G$ over $\mathbb{C}$ is determined by its character, by (2.4.1.13).

Cor. (15.1.2.4) [Number of Representations]. If $G$ is a finite group, then the cardinality of $\hat{G}$ is equal to the number of conjugates of $G$, and $\sum_{\pi \in \hat{G}} d_{\pi}^2 = |G|$.

Proof: Both $\{\chi_{\pi}\}$ and the characteristic functions of the conjugate classes of $G$ are basis for $L^2(G)$. And the second assertion follows from the Peter-Weyl theorem (10.9.4.15) as $\sum_{\pi \in \hat{G}} d_{\pi}^2$ is the dimension of $L^2(G)$.

Cor. (15.1.2.5). $G$ is Abelian iff every irreducible representation of $G$ is of dimension 1.

Proof: This follows immediately from the equation $\sum_{\pi \in \hat{G}} d_{\pi}^2 = |G|$ (15.1.2.4), as $G$ is Abelian iff it has $|G|$ conjugacy classes iff $|\hat{G}| = |G|$ iff $d_{\pi} = 1$ for any $\pi$.

Prop. (15.1.2.6). If $G$ is a finite $p$-group and $A$ is a nonzero $p$-torsion $G$-module, then $A^G \neq 0$.

Proof: We may consider $A$ generated by a single element. Because $A$ is $p$-torsion, $|A| = p^n$ for some $n$. Now consider the orbit, then if the orbit is not a single element, then its order is divisible by $p$, so $|A^G|$ is divisible by $p$. But 0 is fixed, so $A^G \neq 0$.

Group Algebra $C[G]$

Prop. (15.1.2.7) [Maschke’s Theorem]. If $F$ is a field of char $p$ and $G$ is a finite group of order prime to $p$, then for any representation $U$ of $F[G]$ and a submodule $V$, there exists a complement of $V$ in $U$.

Proof: Choose an arbitrary projection $\pi$ of $U$ to $V$, and let $\rho(v) = 1/|G| \sum g^{-1}(g(v))$, then it can be checked $\rho$ commutes with $G$-actions, thus its kernel is also a $G$-modules, and it is identity on $V$, so $U = V \oplus \ker \rho$.

Cor. (15.1.2.8) [Totally Decomposable]. Any such representation of $G$ is a direct sum of irreducible representations.

Prop. (15.1.2.9) [Brauer-Nesbitt]. For a finite group $G$, if two finite dimensional semisimple representations over a field has the same char poly for every element $g$ of $G$, then they are isomorphic.

Proof: Just use the irreducible representations are orthogonal and that they have the same and for char $p$, we can use divide by $p$ and the char poly becomes $p$-th power and we can do this forever, contradiction.

Prop. (15.1.2.10). Integral properties of characters.

Prop. (15.1.2.11) [Dimensions Divisor Order]. The dimension of the irreducible representations of $G$ divides the order of $G$.

Proof:

Cor. (15.1.2.12). The dimension of the irreducible representations of a $p$-group $G$ is a $p$-power.

Prop. (15.1.2.13) [Burnside’s Theorem]. Any group of order $n$ that $n$ has only two prime divisors are solvable.

Proof:
15.1. CLASSICAL REPRESENTATION THEORY

**Induced Representations and Mackey Theory**

**Remark (15.1.2.14).** When $G$ is a finite group, the induced representation $\text{Ind}_H^G$ (15.1.1.22) is the same as the (compact) induction in (15.1.4.41). In particular, all the results there holds in the finite group case.

**Prop. (15.1.2.15) [Character of Induced Representations].** Character of induced representations, Cf. [Serre, P30].

**Rationality Problems**

**Def. (15.1.2.16) [Ring $R_K(G)$].** We want to consider the representations over a subfield $K$ of $\mathbb{C}$.

Let $R_K(G)$ be the $\mathbb{Z}$-module generated by the characters of the representations of $G$ over $K$, then it is a subring of $R(G) = R_{\mathbb{C}}(G)$. And define the $\mathbb{Z}$-module $\bar{R}_K(G)$ to be the elements of $R(G)$ with values in $K$. Clearly $R_K(G) \subset \bar{R}_K(G)$.

**Prop. (15.1.2.17) [Induction and Restriction Morphism].** Let $H$ be a subgroup of $G$, then the induction induces an Abelian group homomorphism $R(H) \to R(G)$, and restriction induces a ring homomorphism $R(G) \to R(H)$. The formula $\text{Ind}(\varphi \cdot \text{res}(\psi)) = \text{Ind}(\varphi) \cdot \psi$ shows the image of Ind is an ideal of $R(G)$. Also by Frobenius reciprocity (15.1.4.44), Ind and Res are dual to each other:

$$(\varphi, \text{res } \psi)_H = (\text{Ind } \varphi, \psi)_G.$$

**Prop. (15.1.2.18).** Let $\rho_i$ be the isomorphism classes of all irreducible linear representations of $G$ over $K$ and $\chi_i$ there characters. Then

- $\chi_i$ form a basis of $R_K(G)$.
- $\chi_i$ are mutually orthogonal.

**Proof:**

**Cor. (15.1.2.19).** A representation of $G$ over $\mathbb{C}$ is realizable over $K$ iff its character belongs to $R_K(G)$.

**Proof:** One direction is trivial, for the other, if $\chi \in R_K(G)$, then $\chi = \sum n_i \chi_i$, and $(\chi, \chi_i) = n_i (\chi, \chi_i)$. As $(\chi, \chi_i) \geq 0$ as they are representations of $G$, we have $n_i \geq 0$, thus $\rho = \sum n_i \rho_i$ is realizable over $K$, by (15.1.2.3).

**Def. (15.1.2.20) [Schur Indices].** $K[G]$ is called quasisplit if the $D_i$ are all commutative, or equivalently, all $m_i = 1$.

**Prop. (15.1.2.21).** If $L/K$ is finite and $L[G]$ is quasisplit, then $[L : K]$ is divisible by each of the Schur indices $m_i$.

**Proof:**

**Prop. (15.1.2.22).** The characters $\psi = \chi_i/m_i$ form a basis of $\bar{R}_K(G)$.

**Proof:**

**Cor. (15.1.2.23).** $R_K(G) = \bar{R}_K(G)$ iff $K[G]$ is quasisplit.
Cor. (15.1.2.24) [Brauer]. If $m$ is the least common multiples of the orders of the elements of $G$ and $K$ contains the $m$-th roots of unity, then $R_K(G) = R(G)$.

Proof: □

Cor. (15.1.2.25). If $m$ is the least common multiples of the orders of the elements of $G$, then all the Schur indices of $G$ over any field $K$ divides the Euler function $\varphi(m)$.

Proof: This follows from (15.1.2.24) and (15.1.2.21) by considering the field $K[\mu_m]$ over $K$. □

Def. (15.1.2.26) [Galois-Action on $G$]. Let $L = K(\mu_m)$, where $m$ divides the order of any element in $G$, then $L/K$ is Galois and $G(L/K) = \Gamma_K$ is a subgroup of $(\mathbb{Z}/m\mathbb{Z})^\ast$. Then this group can act on $G$ by $\sigma_t(x) = x^n$ as a set, and we call two elements $s, s' \in G$ $\Gamma_K$-conjugate iff they are in the same $\Gamma_K$ orbits of $G$.

Prop. (15.1.2.27). A class function $f$ on $G$ with values in $L$ belongs to $K \otimes \mathbb{Z} R(G)$ iff

$$\sigma_t(f(s)) = f(s^t)$$

for $\sigma_t \in \Gamma_K$ and $s \in G$.

Proof: Cf. [Serre, P95]. □

Cor. (15.1.2.28). A class function $f$ on $G$ with values in $K$ belongs to $K \otimes \mathbb{Z} R_K(G)$ iff it is constant on the $\Gamma_K$-orbits of $G$.

Proof: Because the □

Prop. (15.1.2.29). For a finite group $G$, all representations of $G$ has characters in $\mathbb{Q}$ iff it all representations have characters in $G$, iff every two element generating the same subgroup of $G$ is conjugate.

Proof: Cf. [Serre P103]. □

Cor. (15.1.2.30). representations of $S_n$ all has characteristic in $\mathbb{Z}$.

Artin’s Theorem & Brauer’s Theorem

Prop. (15.1.2.31) [Generalized Artin Theorem]. Let $X$ be a family of subgroups of a finite group $G$. Let $\text{Ind} : \bigoplus_{H \in X} R_K(H) \rightarrow R_K(G)$ be the ring homomorphism induced by induction, then the following properties are equivalent:

- $G$ is the union of conjugates of the subgroups in $X$.
- the cokernel of $\text{Ind}$ is finite.

Proof: 2 $\rightarrow$ 1: By the character of induced representations (15.1.2.15), any function in the image of $\text{Ind}$ vanishes outside the union of conjugates of the subgroups in $X$, so if this is not $G$, then the cokernel cannot by finite.

1 $\rightarrow$ 2: Notice the duality of $\text{Ind}$ and $\text{Res}$ (15.1.2.17), it suffices to show that $\text{Res}$ is injective, but this is clear. □
Cor. (15.1.2.32) [Artin Theorem]. Choose $X$ as the family of cyclic subgroups of $G$, then every character of $G$ is a rational combination of characters induced from cyclic subgroups of $G$.

Proof:

Prop. (15.1.2.33) [Brauer’s Theorem]. Let $G \in Ab^{\text{fin}}$, then $K_0(\text{Rep}(G))$ is generated by $\text{Ind}_{H_i}(\chi_i)$, where $H_i \leq G, \chi_i \in \hat{H}_i$.

Proof:

Prop. (15.1.2.34) [Generalized Brauer’s Theorem].

Proof:

Important representations

Prop. (15.1.2.35) [Q_8]. There is a 2-dimensional representation of the quadratic group $Q_8 = \{\pm 1, \pm i, \pm j, \pm k\}$:

\[ i \mapsto \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad j \mapsto \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix}, \quad k \mapsto \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix} \]

Prop. (15.1.2.36). There is a representation of $S_n$ on the $n - 1$-dimensional hypersurface $\sum x_i = 0$.

3 Symmetric Groups

Main references are [The Symmetric Group, Sagan].

4 Locally Profinite Groups

Structure Sheaf and Distributions

Cf. [Representations of the Group GL(n,F) over Local Fields Bernstein/Zelevinsky] and [Bernstein, Representation of p-adic Groups, Bernstein].

Remark (15.1.4.1). For structure theory of locally profinite groups, Cf.1.

Def. (15.1.4.2) [Structure Sheaf and Distributions]. For a locally profinite space $X$, the structure sheaf $C^\infty(X)$ on $X$ is defined to be the locally constant sheaf $\mathcal{C}$ of $X$.

The space $C^\infty_c(X) = C_c(X)$ of test functions on $X$ is the set of locally constant continuous functions with compact supports.

The space $\mathcal{S}^*$ of distribution on $X$ consists of linear functionals on $C^\infty_c(X)$.

Prop. (15.1.4.3). If $X$ is locally profinite space and $\mathcal{F}$ is a $C^\infty$ sheaf, then for any open subset $U \subset X$, $Z = X \setminus U$, there is an exact sequence:

\[ 0 \rightarrow \Gamma_c(U, \mathcal{F}) \rightarrow \Gamma_c(X, \mathcal{F}) \rightarrow \Gamma_c(Z, \mathcal{F}) \rightarrow 0. \]

So if we define $\mathcal{D}(X, \mathcal{F})$ the space of distributions on $\mathcal{F}$ on $X$ to be the space of linear functional on $\Gamma_c(X, \mathcal{F})$, then there is an exact sequence

\[ 0 \rightarrow \mathcal{D}(Z, \mathcal{F}) \rightarrow \mathcal{D}(X, \mathcal{F}) \rightarrow \mathcal{D}(U, \mathcal{F}) \rightarrow 0. \]
Proof: The left exactness is clear. To show the right surjectivity, let $f \in \Gamma_c(Z, \mathcal{F})$, then for each $x \in \text{Supp}(f)$, there is a compact open nbhd $U_x$ that $f$ restricts to an element of $\Gamma(U_x, \mathcal{F})$. Then these $U_x$ cover $\text{Supp}(f)$, then by (3.6.4.7), there is a disjoint finite cover $\{U_i\}$ of $\text{Supp}(f)$ that $f$ are induced by $f_i \in \Gamma(U_i, \mathcal{F})$. Now we can replace $U_i$ by $U_i \cup \bigcup_{j<i} U_j$ to let $U_i$ be disjoint, then $f$ extends to an element of $\bigcup U_i$. \hfill \Box

Cor. (15.1.4.4). For $X$ locally profinite and $U \subset X$ open, $Z = X \setminus U$, there is an exact sequence:

$$0 \to C_c^\infty(U) \to C_c^\infty(X) \to C_c^\infty(Z) \to 0,$$

Thus also an exact sequence

$$0 \to \mathcal{S}^*(Z) \to \mathcal{S}^*(X) \to \mathcal{S}^*(U) \to 0,$$

Proof: The first is the exact sequence (15.1.4.3) applied to the constant sheaf (structure sheaf of $X$). The second is the dual of the first. \hfill \Box

Prop. (15.1.4.5). If $X, Y$ are both locally profinite, then

$$C_c^\infty(X \times Y) = C_c^\infty(X) \otimes C_c^\infty(Y)$$

Proof: Because the subspaces of the form $U \times V$ for $U, V$ open form a subbasis of $X \times Y$, so any compact open subset of $X \times Y$ is a disjoint union of sets of the form $U \times V$. \hfill \Box

Def. (15.1.4.6) [Cosmooth $C_c^\infty(X)$-Modules]. A cosmooth $C_c^\infty(X)$-module is a $C_c^\infty(X)$-module $M$ that for any $m \in M$, there exists some compact open $U \subset X$ that $m = \chi_U m$.

Prop. (15.1.4.7) [Cosmooth $C_c^\infty(X)$-Module and $C^\infty(X)$-Sheaves]. Let $\mathcal{F}$ be a $C^\infty$-sheaf on $X$, then the space $\Gamma_c(X, \mathcal{F})$ is a cosmooth $C_c^\infty(X)$-module (15.1.4.6), and this defines an equivalence of categories between the category of non-degenerate $C_c^\infty(X)$-modules and $C^\infty(X)$-sheaves.

Notice that in this case, a $C_c^\infty(X)$-module $M$ being non-degenerate is equivalent to: for any $m \in M$, there is a compact open subset $U$ that $\chi_U m = m$.

Proof: For any non-degenerate $C_c^\infty(X)$-module $M$, define a sheaf $\mathcal{F}_M$ of the compatible stalks in $\prod_{x \in X} M/M(x)$, where

$$M(x) = \{ m \in M | \chi_U m = 0 \text{ for some } x \in U \}.$$

Then we show these two functors are inverse to each other: One direction is clear, as the sheaf $\mathcal{F}$ is just the sheaf of compatible stalks in $\prod_{x \in X} \mathcal{F}_x$, and it is easy to see $\mathcal{F}_x \cong M/M(x)$. For the other direction, any element in $\Gamma_c(X, \mathcal{F}_M)$ is induced from $f_i \in \Gamma(U_i, \mathcal{F}_M)$, where $U_i$ are pairwise disjoint compact open subsets, by (3.6.4.7), and it is easy to see $\Gamma(U_i, \mathcal{F}_M) = \chi_U M$. Thus $\Gamma_c(X, \mathcal{F}_M) = C_c^\infty(X) M$, and the non-degeneracy of $M$ shows $\Gamma_c(X, \mathcal{F}_M) \cong M$. \hfill \Box

Remark (15.1.4.8). Notice that $M(x)$ can be equivalently defined to be the space spanned by the elements

$$\{ gm | g \in C_c^\infty(X), g(x) = 0, m \in M \}.$$

Prop. (15.1.4.9). If $G$ is a locally profinite group, any $\varphi \in C_c^\infty(G)$ is $K$-bi-invariant under some compact open subgroup $K$. 


Proof: \( \varphi \) must be of the form \( \sum a_i \chi_{U_i} \), where each \( U_i \) is open compact. Then for each element \( x \in U_i \), there is an open compact group \( U_x \) that \( U_x x \cup x U_x \subset U_i \), by (10.9.1.50). Now because \( \text{Supp} f \) is compact, f.m. of the \( U_x x \cap x U_x \) covers \( \text{Supp} \varphi \), thus we consider their intersection \( \cap U_{x_i} \), which is a compact open subgroup \( K_0 \) that \( \varphi \) is \( K_0 \)-bi-invariant. \( \square \)

Lemma (15.1.4.10). Let \( G \) be locally profinite and \( H \) a closed subgroup, then \( G/H \) is locally profinite space by (10.9.1.51). Then the projection \( P : C_c(G) \to C_c(G/H) \) defined in (10.9.1.36) restricts to a projection \( P^\infty : C_c^\infty(G) \to C_c^\infty(G/H) \), and it is surjective.

Proof: Firstly \( P \) maps \( C_c^\infty(G) \) into \( C_c^\infty(G/H) \) because if \( \varphi \) is left invariant under \( K \), then \( P\varphi \) is also left invariant under \( K \). For the surjectivity, let \( \varphi \in C_c^\infty(G/H) \), then \( V = \text{Supp} \varphi \) is open compact, then by (10.9.1.52) there is an open compact subspace \( V \) that \( P(V) = U \). Then we can define

\[ \psi(x) = \chi_V(x) \varphi(p(x))/P(\chi_V)(p(x)), \]

then it is supported on \( V \), and \( P(\psi) = \varphi \). Also, it is locally constant, as is easily verified. \( \square \)

Prop. (15.1.4.11) [Left Invariant Distribution]. Let \( G \) be a locally profinite group and \( T \) is a left invariant distribution on \( G \), then it is the restriction of a unique Haar measure.

Proof: Any element \( f \in C_c^\infty(G) \) is of the form \( \sum a_i \lambda(h_i)e_K \) for some \( K \), by (15.1.4.9), where \( e_K = \mu(K)^{-1} \chi_K \). Because \( T \) is left-invariant, \( T(f) = \sum a_i T(e_K) \), and \( \int f d\mu = \sum a_i \). Thus to show \( T \) is a multiple of \( d\mu \), it suffices to show \( T(e_K) \) is independent of \( K \).

If \( K_1 \leq K_2 \), then \( K_2 = \prod_{i=1}^{n} a_i K_1 \), where \( n = [K_2 : K_1] \), so \( e_{K_2} = \mu(K_1)/\mu(K_2) \sum_{i=1}^{n} \lambda(a_i)e_{K_1} \). Also \( \mu(K_2) = n\mu(K_1) \) by left invariance. Now it is clear \( T(e_{K_1}) = T(e_{K_2}) \) by left invariance of \( T \). Then for any two \( K, K' \), we can find an open compact group \( K'' \) in their intersection, thus \( T(e_{K}) = T(e_{K''}) \). \( \square \)

Cor. (15.1.4.12). If \( T \) is a distribution on \( G \) that satisfies \( \lambda(g)T = \xi(g)^{-1}T \) for \( g \in G \), then there is a unique Haar measure \( d\mu \) that \( T(f) = \int_G \xi(g)f(g)d\mu(g) \).

Proof: Consider the distribution \( T'(f) = T(\xi^{-1}f) \), then it is left invariant. \( \square \)

Cor. (15.1.4.13) [Invariant Quotient Distribution]. Let \( G \) be a locally profinite group and \( H \) a closed subgroup, then left \( H \)-invariant measures on \( G \) are identified with measures on \( G/H \).

And if there exists a left \( G \)-invariant distribution \( D \) on \( G/H \), then \( G/H \) admits a \( G \)-invariant measure (10.9.1.38), whose restriction to \( C_c^\infty(G/H) \) is \( D \).

Proof: Consider the distribution \( D \circ P^\infty \), which is a left invariant linear functional on \( C_c^\infty(G) \), (15.1.4.11) shows that it’s the restriction of a Haar measure on \( G \).

Then we can use the same method as in (10.9.1.38) to show \( \Delta_G|H = \Delta_H \), and the surjectivity of \( P^\infty(15.1.4.10) \) shows \( D \) is a quotient measure on \( G/H \). \( \square \)

Prop. (15.1.4.14) [Gelfand Pairs]. Let \( G \) be a locally profinite group and \( H \) a closed subgroup s.t. \( \Delta(G)|H = \Delta_H \). Suppose \( \iota \) is an involution on \( G \) that leaves \( H \) invariant and acts trivially on those distributions on \( G \) with are \( H \)-bi-invariant, then for any smooth irreducible representation \( V \) of \( G \),

\[ \dim(V^*)^H \cdot \dim((V^*)^H)^H \leq 1. \]

Proof: Given two \( H \)-invariant maps \( l : C \to \mathbb{C}, m : V^* \to \mathbb{C} \), by Frobenius reciprocity, we get two maps \( l' : C_c^\infty(H \backslash G) \to V, m' : C_c^\infty(H \backslash G) \to V^* \) that are surjective, and give rise to \( B : C_c^\infty(H \times H \backslash G \times G) \to V \times V^* \to \mathbb{C} \).
Then $B$ satisfies $B(f,g) = B(i(g),i(f))$, where $i(f)(x) = f(x^{-1})$: There is a commutative diagram
\[
\begin{array}{ccc}
G \times G & \xrightarrow{(x,y) \mapsto xy^{-1}} & G \\
\downarrow & & \downarrow \\
G \times G & \xrightarrow{(x,y) \mapsto y^{-1}x(y)^{-1}} & G \\
\end{array}
\]
and the horizontal arrows identify left $H$-invariant right $G$-invariant distributions on $G$ with left $H \times H$-invariant distributions on $G \times G$.

By the surjectivity of $l'$, $m'$, ker($l'$), ker($m'$) are left and right radicals of $B$ resp., and the above formula shows they determine each other, and $l', m'$ are determined by their kernels, thus we are done. □

**Prop. (15.1.4.15)** [Bernstein-Zelevinsky ?]. If $p : X \to Y$ is a continuous map of locally profinite groups, $\mathcal{F}$ be a cosmooth $C^\infty$-sheaf on $X'$. Let $G$ be a group acting on $X$ and the sheaf $\mathcal{F}$ that $p(gx) = p(x)$, and $\chi$ a character of $G$. Then

- Let $\Gamma_c(X,\mathcal{F})(\chi)$ be the $C^\infty_c(X)$-submodule of $\Gamma_c(X,\mathcal{F})$ generated by $gf - \chi(g)^{-1}f$, $g \in G$, $f \in \Gamma_c(X,\mathcal{F})$. Then $\Gamma_c(X,\mathcal{F})/\Gamma_c(X,\mathcal{F})(\chi)$ is a non-degenerate $C^\infty_c(Y)$-module by composing $p$, so we can define $\mathcal{G}$ the sheaf on $Y$ corresponding to this submodule by (15.1.4.7). Then if $y \in Y$ and $Z = p^{-1}(y)$, the stalk

$$\mathcal{G}_y \cong \Gamma_c(Z,\mathcal{F})/\Gamma_c(Z,\mathcal{F})(\chi).$$

- Assume there are no non-zero distributions $D \in \mathcal{D}(p^{-1}(y),\mathcal{F}|_{p^{-1}(y)})$ that satisfies $gD = \chi(g)D$ for any $y \in Y$, then no such $D$ exists in $\mathcal{D}(X,\mathcal{F})$.

**Proof:** 1: Firstly $\Gamma_c(X,\mathcal{F})/\Gamma_c(X,\mathcal{F})(\chi)$ is a $C^\infty_c(Y)$-module because $\varphi \circ p$ fixes $\Gamma_c(X,\mathcal{F})(\chi)$:

$$(\varphi \circ p)(gf - \chi(g)^{-1}f) = g((\varphi \circ p)f) - \chi(g)^{-1}((\varphi \circ p)f),$$

which uses the condition $p(gx) = p(x)$. The non-degeneracy is also clear, by (15.1.4.7).

Secondly $\Gamma_c(Z,\mathcal{F}) \cong \Gamma_c(X,\mathcal{F})/\Gamma_c(U,\mathcal{F})$ by (15.1.4.3), so $\Gamma_c(Z,\mathcal{F})/\Gamma_c(Z,\mathcal{F})(\chi)$ is isomorphic to the quotient of $\Gamma_c(X,\mathcal{F})$ by $\Gamma_c(U,\mathcal{F})$ and $\Gamma_c(X,\mathcal{F})(\chi)$, because $\Gamma_c(U,\mathcal{F})$ is stable under action of $f \mapsto gf - \chi(g)^{-1}f$ (this uses the condition $p(gx) = p(x)$).

We claim the space $\Gamma_c(U,\mathcal{F})$ is the space $L$ generated by elements of the form $(\varphi \circ p)f$, where $\varphi \in C^\infty_c(Y)$, $\varphi(y) = 0$, $f \in \Gamma_c(X,\mathcal{F})$: $L$ is clearly contained in $\Gamma_c(U,\mathcal{F})$, and if $f \in \Gamma_c(U,\mathcal{F})$, then $\operatorname{Supp} f$ is compact and disjoint from $Z$, so there is an open compact subset $U \subset Y$ containing $p(\operatorname{Supp} f)$ but not $y$. Let $\varphi = \chi_U$, then $f = (\chi_U \circ p)f \in L$.

Then by (15.1.4.7), the stalk $\mathcal{G}_y$ is isomorphic to $M/M(y)$, where $M = \Gamma_c(X,\mathcal{F})/\Gamma_c(X,\mathcal{F})(\chi)$. So $M(y)$ is just the image of the space $L$ in $M$ by (15.1.4.8), hence $\mathcal{G}_y$ is exactly $\Gamma_c(Z,\mathcal{F})/\Gamma_c(Z,\mathcal{F})(\chi)$.

2: this follows from 1, as $gD = \chi(g)D$ is just saying $D(g^{-1}f - \chi(g)f) = 0$, or that $D$ annihilates $\Gamma_c(Z,\mathcal{F})/\Gamma_c(Z,\mathcal{F})(\chi) = \mathcal{G}_y$ by item 1. So this is equivalent to $\mathcal{G}_y = 0$ for any $y$, which is equivalent to $\mathcal{G} = 0$, as $\mathcal{G}$ is a sheaf. □

**Cor. (15.1.4.16)** [Invariant Distribution On Orbits]. Let $\gamma$ be an action of a locally profinite group $G$ on a locally profinite space $X$ and a $C^\infty_c(X)$-sheaf. Assume the action is constructible (3.8.1.21) and there are no $G$-invariant distribution on any $G$-orbit in $X$, then there are no non-zero $G$-invariant distribution on $X$. 
Proof: Firstly, by (3.8.1.22) and (3.6.4.6) any orbit is locally profinite. If there is a $G$-invariant distribution on $X$, we may change $X$ to $\text{Supp} T$, which is $G$-invariant, thus by (3.8.1.22) there is an open subset $U \subset X$ that $G$ acts regularly, thus we reduce to the regular action case.

Then we can consider $X \to X/G$, $X/G$ is locally profinite by (3.8.1.10), so Bernstein-Zelevinsky (15.1.4.15) can be used. □

Prop. (15.1.4.17) [Gelfand-Kazhdan]. If $G$ is a locally profinite group, and $\gamma$ is an action of $G$ on a locally profinite space $X$, $\sigma$ is a homeomorphism $X \cong X$, $F$ is a $C^\infty$-sheaf on $X$, and we assume:

- $\gamma$ is constructible,
- for each $g \in G$, there is a $g^\sigma \in G$ that $\gamma(g)\sigma = \sigma\gamma(g^\sigma)$.
- For some $n \geq 0$ and $g_0 \in G$, $\gamma^n = \gamma(g_0)$.
- If there is a non-zero $G$-invariant $F$-distribution $T$ on a $G$-orbit $S$, then $\sigma(S) = S$ and $\sigma(T) = T$.

Then any $G$-invariant distribution on $X$ is invariant under $\sigma$.

Proof: Let $T$ be a $G$-invariant $F$-distribution that $\sigma T \neq T$, then $n > 1$, and for any $n$-th root of unity $\xi$, consider $T_\xi = \sum \xi^{-i}\sigma^i(T)$. Then

$$\sigma T_\xi = \xi T_\xi, \quad \sum \xi T_\xi = nT, \quad \sum \xi T_\xi = n\sigma(T).$$

so $\sum \xi(\xi - 1)T_\xi = n(\sigma(T) - T) \neq 0$, which shows there is a root $\xi \neq 1$ that $T_\xi \neq 0$. Notice $T_\xi$ is $G$-invariant by condition2. Consider the action $\sigma_{\xi i} = \xi \cdot \sigma$, then $T_\xi$ is invariant under $\sigma_{\xi}$.

Let $G'$ be the semi-direct product of $G$ with $\sigma_{\xi}$, under the action of $\sigma_{\xi}^{-1}g\sigma_{\xi} = g^\sigma$, then $G'$ is locally profinite and acts on $X, F$. Clearly this action is also constructible.

Now for any $G'$-orbit $S'$, we prove there are no $G'$-invariant distribution on $S'$, because it is in priori $G$-invariant, so some distribution exists on some $G$-orbit $S \subset S'$, but then condition4 shows $\sigma$ fixes $S$, then $S = S'$ and $\sigma(T) = T$. But $\sigma_{\xi}(T) = T$, contradiction. Finally, (15.1.4.16) shows there are no $G'$-invariant distribution on $X$, contradicting $T_\xi$. □

Cor. (15.1.4.18) [Gelfand-Kazhdan]. If $G$ is a locally profinite group that is $\sigma$-compact, and $\gamma$ is an action of $G$ on a locally profinite space $X$, $\sigma : X \cong X$ is a homeomorphism, and we assume:

- $\gamma$ is constructible,
- for each $g \in G$, there is a $g^\sigma \in G$ that $\gamma(g)\sigma = \sigma\gamma(g^\sigma)$.
- For some $n \geq 0$ and $g_0 \in G$, $\sigma^n = \gamma(g_0)$.
- For any $x$, $x$ and $\sigma(x)$ are in the same $G$-orbit.

Then any $G$-invariant distribution on $X$ is invariant under $\sigma$.

Proof: We use (15.1.4.18) and take $F$ to be just $C^\infty(X)$. Then we need to check condition4: for any $G$-orbit $S$ of $X$ let $s \in S$ and $\text{Stab}(s) = H$, $S \cong G/H$ by (3.8.1.22) and (10.9.1.53). Then (15.1.4.13) shows $T$ is just the $G$-invariant measure on $G/H : T\varphi = \int_{G/H} \varphi(\gamma(\varphi)s)$. Now condition4 and2 shows $\sigma T$ is also $G$-invariant, thus $\sigma T = cT$. Clearly $c \geq 0$, and condition3 shows $c^n = 1$, thus $c = 1$. □

Hecke Algebra

This is a continuation of Hecke Algebras.
Def. (15.1.4.19) [Hecke Algebras of Locally Profinite Groups]. The algebra \( \mathcal{H}(G) \) of test functions (15.1.4.2) on a locally profinite group \( G \) under convolution is an algebra, called the Hecke algebra of \( G \). And for a compact open subgroup \( K \) of \( G \), \( \mathcal{H}_K \) is the subspace of \( K \)-bi-invariant functions in \( \mathcal{H}(G) \).

Notice \( \mathcal{H} = \bigcup_K \mathcal{H}_K \) by (15.1.4.9). Also \( \mathcal{H}_K \) has a unit \( e_K = \mu(K)^{-1}\chi_K \). This is easily verified. Then \( \mathcal{H}_G \) is an idempotented algebra (2.4.4.2).

**Proof:** Define the set \( \mathcal{E} \) of idempotents in \( \mathcal{H}(G) \) as \( e_K \), where \( K \) is compact open in \( G \). The fact that \( \mathcal{H} \) is an idempotented algebra follows from (15.1.4.20) and (15.1.4.22). \( \square \)

Prop. (15.1.4.20) [Point Measure]. Consider the point measure \( \delta_g \) for \( g \in G \), it is not an element in \( \mathcal{H}(G) \), but it can convolute on \( \mathcal{H}(G) \): \( (\delta_g \ast \varphi)(x) = \varphi(g^{-1}x), (\varphi \ast \delta_g)(x) = \varphi(xg) \). Then

- If \( g \in K \), then \( \delta_g \ast e_K = e_K \ast \delta_g = e_K \).
- \( \delta_g \ast e_K \ast \delta_g^{-1} = e_{gKg^{-1}} \).
- If \( K = K_1K_2 \) is an open subgroup, then \( e_{K_1} \ast e_{K_2} = e_K \). In particular, \( e_K \ast e_K = e_K \).

**Remark** (15.1.4.21). In fact we should define the Hecke algebra as locally constant distributions on \( G \), then there equations are more natural. This algebra is equivalent to Hecke algebra by \( f \mapsto f\mu_G \).

Prop. (15.1.4.22). \( \mathcal{H}_K = e_K \ast \mathcal{H} \ast e_K = \mathcal{H}[e_K] \).

**Proof:** Notice by (15.1.4.20), functions in \( e_K \ast \mathcal{H} \ast e_K \) is clearly \( K \)-bi-invariant. For the other direction, notice if \( \varphi \) is left and right \( K \)-invariant, then \( \varphi = e_K \ast \varphi = \varphi \ast e_K = e_K \ast \varphi \ast e_K \). \( \square \)

Prop. (15.1.4.23) [Smooth Representations and \( \mathcal{H} \)-Modules]. For a smooth representation \( (\pi, V) \) of \( G \), for any \( v, g \mapsto \pi(g)v \) can be regarded as a locally constant function with value in \( V \), thus for any \( \varphi \in \mathcal{H}_G \), \( g \mapsto \varphi(g)\pi(g)v \) is locally constant with compact support, thus we can define a representation of the Hecke algebra \( \mathcal{H}_G \) by

\[
\pi(\varphi)v = \int_G \varphi(g)\pi(g)v \, dg
\]

which just has nothing to do with integration, and this is compatible with convolution by formal reason. Then this is a smooth \( \mathcal{H}_G \)-module, and this gives an equivalence between the category of smooth(admissible) representations of \( \mathcal{H}(G) \) (2.4.4.4) and the category of smooth(admissible) representations of \( G \).

**Proof:** For any \( v \in V \), there is an open compact subgroup \( K \) that \( v \in V[e_K] \), thus \( e_K v = v \), so \( V \) is smooth. For the equivalence of categories, for any \( \mathcal{H}(G) \)-module \( V \), we can define a \( G \)-action by linearly extending the action \( \pi(g)e_K v = (\delta_g \ast e_K)v \). Notice by associativity of representation and smoothness, this is well-defined on all of \( V \), and is a representation of \( G \). Also it is continuous because \( v = e_K v \) for some \( K \) thus \( \pi(g)v = (\delta_g \ast e_K)v = e_K v = v \) for any \( g \in K \). Finally these two funcors are inverse to each other is also easily checked. \( \square \)

Cor. (15.1.4.24). \((-)^K, (-)^\infty \) (15.1.1.14) are both exact, by (2.4.4.3).

Cor. (15.1.4.25). Let \((\pi, V)\) be a non-zero smooth representation of a locally profinite group \( G \), then the following are equivalent by (2.4.4.6) and (15.1.4.23):

- \( \pi \) is irreducible.
- \( V \) is simple as \( \mathcal{H} \)-module.
\begin{itemize}
\item $V^{K_0}$ is either zero or simple as a $\mathcal{H}_{K_0}$-module for all open compact subgroups $K_0$ of $G$.
\end{itemize}

**Prop. (15.1.4.26) [Fourier Transform].** If $G$ is a locally profinite Abelian group, then the Fourier transform induces an isomorphism

$$\mathcal{H}(\hat{G}) \cong C_c^\infty(G) : \varphi \mapsto \hat{\varphi}(\xi) = \int_G \varphi(y)\overline{\langle \xi, y \rangle}dy.$$  

**Proof:** By (10.9.3.8) this is an algebra homomorphism. It remains to show that the image are all locally compact, and this is clear from the fact $\hat{G}$ is given the compact-open topology (10.9.3.6). \hfill $\Box$

**Admissible Smooth Representations**

**Prop. (15.1.4.27).**

\begin{itemize}
\item For any compact open subset $K$ of $G$, $V^K = ((V^\wedge)^K)^*$.
\item $\text{Hom}_G(V, W^\wedge) = \text{Hom}(W, V^\wedge)$.
\item $V \mapsto (V^\wedge)^\wedge$ is an injection.
\end{itemize}

**Proof:**

1: Using (15.1.4.23), because $(\hat{V})^K = V^{*K}$. There is a homomorphism $V^{*K} \rightarrow V^{K*}$, it is injective, because if $f(v) = 0$ for each $v \in V^K$, then $f(w) = f(\varepsilon_K v) = 0$. It is also injective, because for each $f \in V^{K*}$, the inverse image is $g(w) = g(\varepsilon_K w)$.

2: $\text{Hom}(V, \hat{W}) = \text{Hom}(V, W^*) = \text{Hom}(V \otimes W, \mathbb{C})$.

3: by the proof of item1,

$$\hat{V} = \cup_K(\cup_K(\hat{V}^{*K})^*K) = \cup_K(\cup_K\hat{V}^{*K})^*K = \cup_K(V^{*K*}) = \cup_K(V^{K**}).$$

So the filtered colimits of the injections $V^K \rightarrow (V^{K*})^*$ gives an injection $\cup_K(\hat{V}^{*K*})$. \hfill $\Box$

**Cor. (15.1.4.28) [Contragradient Functor is Exact].** The contragradient functor $V \mapsto \hat{V}$ is exact. Because $(-)^*$, $(-)^\infty$ are all exact (15.1.4.24).

**Cor. (15.1.4.29).** If $P$ is projective in $\mathcal{M}(G)$, then $\hat{P}$ is injective in $\mathcal{M}(G)$.

**Proof:** $\text{Hom}(X, \hat{P}) = \text{Hom}(P, \hat{X})$, and notice that the contragradient functor is exact (15.1.4.28). \hfill $\Box$

**Def. (15.1.4.30) [Admissible Representations].** An admissible smooth representation of a locally profinite group $G$ is a smooth representation that for any compact open subgroup $K$ of $G$, $V^K$ is of f.d.. The category of admissible smooth representation of $G$ is denoted by $\text{Rep}^{\text{adm}}(G)$.

Then a smooth representation is admissible iff $V \cong (V^\wedge)^\wedge$. In particular, the contragradient of an admissible representation is admissible.

**Proof:** If $V^K$ is of f.d. for each $K$, then by the proof of item3 of (15.1.4.27), $V \cong \hat{V}$. Conversely, if $V \cong \hat{V}$, then $V^{K*} \cong V^{*K}$, thus $V$ must be finite, by (2.3.3.9). \hfill $\Box$

**Cor. (15.1.4.31).** For an irreducible admissible representation, the contragradient is also irreducible admissible.

Extensions of admissible representations are admissible, by (15.1.4.24).
Prop.(15.1.4.32)[Decomposition of Admissible Representations]. Let $K$ be a compact open subgroup of $G$, then any smooth representation of $G$ decomposes as

$$V = igoplus_{\rho \in \Rep(K)} V^\rho,$$

and $V$ is admissible iff each $V^\rho$ are all of f.d. In particular, this shows the two notations of admissible (locally compact group and locally profinite groups) are compatible for smooth representations.

**Remark (15.1.4.33).** WARNING: The decomposition theorem of compact groups cannot be directly used, as representation may not be of f.d. so may not be unitarizable.

**Proof:** Firstly $V \subset \sum_{\rho \in \hat{K}} V(\rho)$, because any $v \in V$ is fixed by some compact open subgroup $K_0$ of $K$, and we can choose $K_0$ to be normal in $K$ by (3.8.1.6), so for $\Gamma = K \ltimes K_0$,

$$v \in V^{K_0} = \bigoplus_{\rho \in \hat{\Gamma}} V(\rho) \subset \sum_{\rho \in \hat{K}} V(\rho).$$

Also this sum is direct, because otherwise $\sum_{\rho \in S} C^\rho v^\rho = 0$, but let $K_0$ be the intersection of kernels of $\rho$, then this is an equation of elements in representations of $\Gamma = K/K_0$ finite, so contradicting (15.1.2.8).

If $\pi$ is admissible, then $V(\rho) \subset V^{\ker \rho}$ is of f.d.. Conversely, if $V$ is not admissible, then $V^{K_0}$ is of infinite dimensional for some $K_0$ compact compact normal, so $V^{K_0}$ decomposes as direct sums of $V(\rho)$ for $\rho \in \hat{K}/K_0$, thus one of these space must be of infinite dimensional.

**Def.(15.1.4.34)[Character of Admissible Representations].** Let $(\pi, V)$ be an admissible representation of $G$, then for any $\varphi \in \mathcal{H}$, $\varphi \in \mathcal{H}_K$ for some compact open subset of $G$, by (15.1.4.19), so $\text{Im}(\pi(\varphi)) \subset V^K$, which is of f.d., so we can define the trace of $\varphi$ as $\text{tr}(\pi(\varphi)|V^K)$. Notice this is independent of $K$ chosen by linear algebra reasons. And this defines a distribution on $\mathcal{H}$, $\varphi \mapsto \text{tr}(\varphi)$, called the **character** of $V$.

**Cor.(15.1.4.35).** $\mathcal{M}(G)$ has enough injectives.

**Proof:** As $\mathcal{M}(G)$ has enough projectives (2.4.4.9)(15.1.4.23), there is a surjection $P \to \widetilde{X}$, thus an injection $\widetilde{X} \hookrightarrow \tilde{P}$ (15.1.4.28). Now $X \hookrightarrow \widetilde{X}$ by (15.1.4.27).

**Irreducible Admissible Representations**

**Prop.(15.1.4.36)[Separation Lemma].** If $G$ is a $\sigma$-compact locally profinite group, then for any $0 \neq h \in \mathcal{H}(G)$, there is an irreducible representation $\rho$ that $\rho(h) \neq 0$.

**Proof:** Cf.[Bernstein, P20], [Bernstein-Zelevinsky, P19].

**Prop.(15.1.4.37)[Shur’s Lemma].**

- If $G$ is a $\sigma$-compact locally profinite group, then any irreducible smooth representation $V$ is of at most countable dimension, thus $\text{End}_G(V) = \mathbb{C}$ by (2.2.1.10).

- If $G$ is a locally profinite group, then any irreducible admissible representation $V$ of $G$ satisfies $\text{End}_G(V) = \mathbb{C}$.
Prop. (15.1.4.38). Let \((\pi_1, V_1), (\pi_2, V_2)\) are two irreducible representations of a locally profinite group \(G\). If \(V_1^K \cong V_2^K \neq 0\) as \(\mathcal{H}_K\)-module for some compact open subgroup \(K\) of \(G\), then \(\pi_1 \cong \pi_2\). This follows immediately from (2.4.4.7).

Prop. (15.1.4.39) [Characters Determine Irreducible Admissible Representations]. Let \(\pi_1, \ldots, \pi_n\) be inequivalent irreducible admissible representations of a locally profinite group \(G\), then their characters \(\text{tr}(\pi_i)\) are linearly independent. In particular, an irreducible admissible representation is determined by its character.

Proof: Choose \(K\) that \(V_i^K \neq 0\) for any \(i\), the hypothesis together with (15.1.4.38) shows \(V_i^K \neq V_j^K\). Then we finish by (10.9.4.22).

Prop. (15.1.4.40) [Representations of Product Group]. If \(G_1, G_2\) are all locally profinite groups and \((\pi_i, M_i)\) are irreducible admissible representations of \(G_i\), then \(M_1 \otimes M_2\) is an irreducible admissible representation of \(G_1 \times G_2\), and any irreducible admissible representations of \(G_1 \times G_2\) comes like this.

Proof: By (15.1.4.23) and (2.4.4.15), this follows if we have \(\mathcal{H}_{G_1 \times G_2} \cong \mathcal{H}_{G_1} \otimes \mathcal{H}_{G_2}\). And this fact is easily deduced from (15.1.4.5).

Induced Representations and Mackey Theory

Def. (15.1.4.41) [Smooth Induced Representations]. Let \(G\) be a locally profinite group and \(H\) is a closed subgroup, \((\pi, V)\) be a smooth representation of \(H\), we can define the smooth induced representation \(\text{Ind}^G_H \pi\) as the space of locally constant \(f\) on \(G\) with values in \(V\)

\[
f(hg) = \sqrt{\frac{\Delta_G(h)}{\Delta_H(h)}} \pi(h)f(g).
\]

with the natural right \(G\)-representation. Notice this is similar to that of unitary representations of locally compact groups, in (10.9.5.3).

the induced representation \(\text{Ind}^G_H \pi\) has a subrepresentation \(\text{ind}^G_H\) consisting of functions that is compactly supported in \(H \setminus G\), called the compactly induced representation.

Remark (15.1.4.42). The normalized factor here is used to make the induction of a unitarizable representation unitarizable (15.1.4.52).

Prop. (15.1.4.43) [Description of the Induced Representations]. Situation as in (15.1.4.41). Let \(K \subset G\) be an open compact subgroup, and \(\Omega \subset G\) be a system of coset representations of \(H \setminus G/K\). For each \(g \in G\), denote \(N_g = H \cap gKg^{-1}\) the compact open subgroup of \(H\), then the restriction of functions from \(G\) to \(\Omega\) induces an isomorphism of \((\text{Ind}^G_H(V))^K\) with the \(\prod_{g \in \Omega} V^{N_g}\). And in this way, \((\text{ind}^G_H(V))^K\) is mapped to \(\bigoplus_{g \in \Omega} V^{N_g}\).

Prop. (15.1.4.44). Let \(G\) be a locally profinite group, \(H\) a closed subgroup of \(G\), and \(B\) a closed subgroup of \(H\), then
- \text{Ind}_H^G and \text{ind}_H^G are both exact functors Rep^{alg}(H) \to Rep^{alg}(G).

- \text{Ind}_H^G \circ \text{Ind}_H^H = \text{Ind}_H^G and \text{ind}_H^G \circ \text{ind}_H^H = \text{ind}_H^G.

- \text{ind}_H^G(\sigma)^\vee = \text{ind}_H^G(\sigma^\vee).

- (Smooth Frobenius Reciprocity) If \((\pi, W) \in \text{Rep}^{alg}(G), (\rho, V) \in \text{Rep}^{alg}(H),\) then there are functorial isomorphisms

\[\text{Hom}_G(\pi, \text{Ind}_H^G(\rho)) = \text{Hom}_H(\pi|_H, \rho \otimes \sqrt{\Delta_G/\Delta_H}), \quad \text{Hom}_G(\text{ind}_H^G(\sigma), \pi) = \text{Hom}_H(\rho \otimes \sqrt{\Delta_H/\Delta_G}, (\pi^\vee|_H)^\vee)\]

\textbf{Proof:}  
1: This follows from the description in (2.4.4.3) and (2.4.4.3) by taking colimits.

2: For simplicity we prove for \(G, H, B\) unimodular. An element in \(\text{Ind}_H^G \circ \text{Ind}_H^H(V)\) is an element \(\varphi : G \mapsto \text{Hom}(H, V)\) that satisfies \(\varphi(hg)(h') = (\pi(h)\varphi(g))(h') = \varphi(g)(hh')\), thus \(\varphi(g)(h) = \varphi(hg)(1)\). Let \(\Phi(g) = \varphi(g)(1)\), then \(\Phi\) satisfies \(\Phi(bg) = \pi(b)\Phi(g)\). So \(\varphi \mapsto \Phi\) is an isomorphism. Ind case follows from item 3.

3: For \(f : G \to V \in \text{Ind}_H^G(\sigma), f' \in G \to V' \in \text{ind}_H^G(\sigma')\), \(\langle f, f' \rangle\) is compactly supported in \(H\setminus G\), and \(\langle \pi(h)f, \pi(h)f' \rangle = \Delta_G(b)\Delta_H(b')\langle f, f' \rangle\), thus we can define a \(G\)-invariant pairing

\[\langle f, f' \rangle = \int_{H \setminus G} \langle f(g), f'(g) \rangle d\mu_{H \setminus G}(g) (10.9.1.44).\]

This map is a perfect pairing on the \(K\)-fixed part for any compact open \(K\) using description in (15.1.4.43), thus we are done.

4: Given a \(\Phi : W \to \text{Ind}_H^G V\), we have a map \(\varphi : W \to V : \varphi(w) = \Phi(w)(1)\), then it is verified that \(\varphi \in C(\pi|_H, \rho \otimes \sqrt{\Delta_G/\Delta_H})\). Conversely, if \(\varphi \in C(\pi|_H, \rho \otimes \sqrt{\Delta_G/\Delta_H})\) is given, we can define \(\Phi : W \to \text{Ind}_H^G V : \Phi(w)(g) = \varphi(\pi(g)w)\), then \(\Phi(w) \in \text{Ind}_H^G V\) and this is linear in \(w\) (remember to check smoothness). Finally, it is easily verified these maps are inverse to each other. The second assertion follows from item 3 and (15.1.4.27). \(\square\)

\textbf{Cor. (15.1.4.45).} If \(H\setminus G\) is compact, then \(\text{Ind}_H^G = \text{ind}_H^G\), and they map admissible representations to admissible representations, by the description in (2.4.4.3), as \(H\setminus G/K\) is both compact and discrete thus finite.

\textbf{Prop. (15.1.4.46).} If \(H\) is normal in \(G\) and for any \(\rho \in \text{Rep}(H)\), let \(\rho^\varnothing\) be \(\rho\) twisted by conjugation of \(g \in G\), then \(\text{Ind}_H^G(\rho) \cong \text{Ind}_H^G(\rho^\varnothing)\), and \(\text{ind}_H^G(\rho) \cong \text{ind}_H^G(\rho^\varnothing)\)

\textbf{Proof:} \(\square\)

\textbf{Prop. (15.1.4.47).} Let \(H \leq G, K \leq G, \rho \in \text{Rep}(H)\), then

\[(\text{Ind}_H^G(\rho))^K \cong \text{Ind}_{H/H\cap K}^{G/K}(\rho^{H \cap K}) \in \text{Rep}^{alg}(G/K)\]

\textbf{Proof:} \(\square\)

\textbf{Prop. (15.1.4.48).} Let \(G\) be a locally profinite group and \(H\) is a closed subgroup, \((\pi, V)\) be a smooth representation of \(H\), then there is a \(G\)-invariant map \(P_\pi : C_c^\infty(G) \otimes V \to \text{ind}_H^G(\pi)\):

\[P_\pi(\varphi, v)(g) = \int_H \varphi(b^{-1}g) \sqrt{\Delta_G(b)/\Delta_H(b)} \pi(b)v db.\]
And if \( \dim \pi < \infty \) and there is an open compact subgroup \( K \) of \( G \) that \( G = H K \), then this map is surjective.

Moreover,
\[
P(\lambda(b)^{-1} \varphi, v) = \sqrt{\Delta_G(b) \Delta_H(b)} P(\varphi, \pi(b)v), \quad b \in H
\]

**Proof:** It can be verified that \( P_\pi(\varphi, v)(bg) = \sqrt{\Delta_G(b) \Delta_H(b)} P_\pi(\varphi, v) \).

If \( H \setminus G \) is compact, by \((10.9.1.52)\), there is a compact open subset \( K \) of \( G \) that \( G = H K \), then for any \( f \in \text{Ind}_H^G(\pi) = \sum \varphi_i \otimes f_i \), consider \( \varphi_i = \chi_{K^{-1}} f_i \), then \( \sum P(\varphi_i, v_i) = \sum V(H \cap K) f_i v_i = V(H \cap K) f \).

**Prop. (15.1.4.49) [Mackey’s Decomposition].** Let \( H, K \) be closed subgroups of a locally profinite group \( G \), \( \rho \) is a smooth representation of \( H \). If \( s \in G \), then we can define a new representation of \( H_s = K \cap s H s^{-1} \) as \( \rho^s(g) \mapsto \rho(s^{-1}gs) \). Then if we use unnormalized induction,

- If either \( H \) or \( K \) is open in \( G \), then
  \[
  \text{res}_K^G \text{ind}_H^G \rho \cong \bigoplus_{s \in H \setminus G / K} \text{ind}_{H_s}^K \rho^s
  \]

- If \( K \) is open in \( G \), then
  \[
  \text{res}_K^G \text{Ind}_H^G \tau \cong \bigoplus_{s \in H \setminus G / K} \text{Ind}_{H_s}^K \tau^s \]

**Proof:** Cf.\([Yam22]\).

**Cor. (15.1.4.50) [Mackey’s Intertwining Theorem].** Let \( H \) be a closed subgroup of a locally profinite group \( G \), \( K \) an open subgroup of \( G \), \( \sigma \) (resp. \( \tau \)) be a smooth representation of \( K \) (resp. \( H \)), define \( \tau^s \) as in \((15.1.4.49)\), then if we use unnormalized induction,

- \( \text{Hom}_G(\text{ind}_K^G \sigma, \text{Ind}_H^G \tau) \cong \bigoplus_{s \in H \setminus G / K} \text{Hom}_{H_s}(\sigma, \tau^s) \).

- If moreover \( H \setminus HgK \cong H_s \setminus K \) is compact for any \( g \in G \) (e.g. \( K \) is compact) and \( \sigma \) is f.g. over \( K \), then
  \[
  \text{Hom}_G(\text{ind}_K^G \sigma, \text{ind}_H^G \tau) \cong \bigoplus_{s \in H \setminus G / K} \text{Hom}_{H_s}(\sigma, \tau^s).
  \]

**Proof:** 1: This is a direct consequence of Mackey’s decomposition \((15.1.4.49)\) and Frobenius reciprocity \((15.1.4.44)\):

\[
\text{Hom}_G(\text{ind}_K^G \sigma, \text{Ind}_H^G \tau) \cong \text{Hom}_K(\sigma, \text{res}_K^G \text{Ind}_H^G \tau) \cong \text{Hom}_K(\sigma, \bigoplus_{s \in H \setminus G / K} \text{Ind}_{H_s}^K \tau^s) \cong \text{Hom}_K(\sigma, \text{Ind}_{H_s}^K \tau^s) \cong \prod_{s \in H \setminus G / K} \text{Hom}_{H_s}(\sigma, \tau^s).
\]

2 is similar.

**Cor. (15.1.4.51) [Compact Induction Admissible].** If \( H \) is a subgroup of \( G \) that \( H \setminus G \) is compact, then \( \text{Ind}_H^G \) takes admissible representations to admissible representations.
Proof: For any compact open subgroup $K \subset G$, $H \backslash G / K$ is finite, as $H \backslash G$ is compact and $K$ is open, then by Mackey’s decomposition (15.1.4.49), $(\text{Ind}_H^G \rho)^K = \bigoplus_{s \in H \backslash G / K} s^{-1} K \rho s \cap H$ is of f.d. if $\rho$ is admissible.

Unitalizable Admissible Representations

Prop. (15.1.4.52). The induction of a unitarizable representation is unitarizable, by (10.9.5.3).

Prop. (15.1.4.53) [Converse of Schur’s Lemma]. If $(\pi, V)$ is a unitarizable admissible representation of a locally profinite group $G$ that $\text{Hom}_G(V, V) = \mathbb{C}$, then $\pi$ is irreducible.

Proof: Cf. [Bump, P523].

Compact Representations

Def. (15.1.4.54) [Compact Representations]. For a locally profinite group $G$, a **compact representation** is a smooth representation of $G$ s.t. for every $\xi \in V$ and every compact open subgroup $K \subset G$, the function $D_{\xi,K} : G \to V : g \mapsto \pi(e_K) \pi(g^{-1}) \xi$ has compact support.

Prop. (15.1.4.55). $V \in \text{Rep}^{\text{alg}}(G)$ is compact iff every matrix coefficient of $V$ is compactly supported. And every f.g. compact representation is admissible.

Proof: If $V$ is compact, for any $\xi \in V, \xi \wedge \in V^\wedge, \xi \wedge \in (V^\wedge)^K$, then $\text{Supp} \varphi_{\xi, \xi \wedge} \in \text{Supp} D_{\xi,K}$ is compact.

For the converse, Cf. [Bernstein Zelevinsky, P26].
15.2  Modular Representations

Main references are [Ser77] and [Bon11].

1  Block Theory
   See [Bon11].

2  Unequal Characteristic

3  Equal Characteristic

Prop. (15.2.3.1). The only irreducible representation of a $p$-group over a field of char $p$ is the trivial representation.

Proof: For any $v \in V$, consider the additive subgroup generated by $g(s)v$, then it is a finite group of prime power order. Then (2.1.7.4) shows it has an element other than 0 fixed by all $G$, thus it is not irreducible unless trivial representation. \qed
15.3 Representations of Algebraic Groups

References are [Mil17].

1 Basics

Throughout this subsection, $G$ is an affine algebraic group over a field $k$ if not said.

Def. (15.3.1.1) [Linear Representations of Algebraic Groups]. Let $R$ be a ring and $V$ a free $R$-module, let $GL(V)$ be the group functor

$$\mathfrak{c}Alg_R \to \mathfrak{g}rp : R' \mapsto \text{Aut}(V \otimes_R R').$$

Then a linear representation $(r, V)$ of an algebraic group $G$ over $R$ is a homomorphism of group functors $r : G \to GL(V)$. It is called faithful representation if $r$ is a monomorphism as natural transformation of functors.

If $V$ is of f.d., this is equivalent to a homomorphism $G \to GL(V)$. And by (7.1.5.6), it is faithful iff $G \to GL(V)$ is a closed embedding.

For a linear representation $(r, V)$, let $\text{End}(V) = \text{Aut}(r)$.

Prop. (15.3.1.2) [Representations and Co-modules]. A representation of $G$ on $V$ is equivalent to a right $\Gamma(G)$-comodule structure on $V$ (2.9.1.10).

Proof: Let $A = \Gamma(G)$. For any representation $r : G \to GL(V)$, it induces a map $G(A) \to GL_A(V \otimes A)$, which maps $\text{id}_A$ to a map $\rho : V \to V \otimes A$. Now if $\rho(e_j) = \sum e_i \otimes a_{ij}$, then by functoriality, the map $G(R') \to GL_R(V \otimes R')$ is given by $g \mapsto (e_j \mapsto e_i \otimes a_{ij}(g))$.

And it can be verified that this is a group homomorphism iff the comodule condition is satisfied. □

Def. (15.3.1.3) [Stabilizers]. Let $(r, V)$ be a representation of an affine group scheme $G$ over $R$, $W$ a subspace of $V$, consider the functor

$$\text{Stab}_G(W) : R' \mapsto \{g \in G(R')|g(W_{R'}) = W_{R'}\},$$

then if $V$ is of f.d., $\text{Stab}_G(W)$ is representable by a closed subgroup of $G$, called the stabilizer group scheme of $W$ in $V$.

Proof: Let $\rho : \Gamma(G) \to V \otimes \Gamma(G)$ be the comodule action corresponding to $r$, let $\{e_i\}_{i \in I}$ be a basis for $W$, and extends it to a basis $\{e_i\}_{i \in I, j \in J}$ of $V$, and

$$\rho(e_j) = \sum e_i \otimes a_{ij}, \quad a_{ij} \in \Gamma(G).$$

Let $g \in \text{Hom}(\Gamma(G), R')$, then $ge_j = \sum e_i \otimes g(a_{ij})$, and then clearly $G_W$ is represented by the quotient of $\Gamma(G)$ by the ideal generated by $\{a_{ij}|i \in I, j \in J\}$. □

Cor. (15.3.1.4). If $S$ is a scheme and $G$ is an affine group scheme over $S$, $\mathcal{V}$ a locally free sheaf on $S$ and $\mathcal{W}$ a locally free subsheaf of $\mathcal{V}$, then similarly $\text{Stab}_G(\mathcal{W})$ is representable by a closed subgroup of $G$ over $S$, by considering affine-locally.

Cor. (15.3.1.5). Let $(\rho, V)$ be a f.d. representation of $G$ and $S \subset G(k)$ be a subset schematically dense in $G$, then a subspace $W \subset V$ is stable under $G$ iff it is stable under $S$. 
Prop. (15.3.1.6) [Fixed Subspace]. Let \((r, V)\) be a linear representation of an algebraic group, define the fixed subspace by \(G\):

\[ V^G = \{ v \in V \mid gv_R = v_R, \forall R \in \mathcal{A}l_g_k, g \in G(R) \}. \]

Then for any \(R \in \mathcal{A}l_g_k\), \(V^G \otimes R\) is the submodule of \(V \otimes R\) that is fixed by elements of \(G(R')\) for any \(R' \in \mathcal{A}l_g_R\).


Cor. (15.3.1.7). The fixed subspace is compatible with base change of fields.

Def. (15.3.1.8) [Subrepresentations]. A subspace \(W\) of a linear representation \(V\) of an algebraic group \(G\) is called a subrepresentation of \(V\) if \(\tilde{G} = \text{Stab}_G(W)\).

A linear representation is called simple if has no non-trivial subrepresentations.

Prop. (15.3.1.9). Let \(U\) be a normal subgroup of an algebraic group \(G\), then for any representation \(V\) of \(G\), \(V^U\) is a subrepresentation of \(V\).

Prop. (15.3.1.10) [Union of F.D. Subrepresentations]. Let \((r, V)\) be a linear representation of \(G\), then \(V\) is a filtered union of its f.d. subrepresentations.

Proof: It suffices to consider comodules and prove any vector \(v \in V\) is contained in a f.d. subcomodule. Let \(\{e_i\}\) be a basis of \(\Gamma(G)\), let

\[ \Delta(e_i) = \sum_{i,k} r_{ijk} e_j \otimes e_k, \quad \rho(v) = \sum_i v_i \otimes e_i, \quad v_i \in V. \]

Because \((\text{id}_V \otimes \Delta) \circ \rho = (\rho \otimes \text{id}_{\Gamma(G)}) \circ \rho(2.9.1.10)\), thus

\[ \sum_{i,j,k} r_{ijk} v_i \otimes e_j \otimes e_k = \sum_k \rho(v_k) e_k \]

which means

\[ \rho(v_k) = \sum_{j,k} r_{ijk} v_i \otimes e_j. \]

Thus \(\text{span}\{e_i\}\) is a f.d. comodule of \(V\) containing \(v\).

Cor. (15.3.1.11). Any simple representations of an algebraic group is of f.d.

Prop. (15.3.1.12) [Schur’s Lemma]. Let \((V, r)\) be a simple representation of an algebraic group \(G\), then \(\text{End}(V)\) is a f.d. division algebra \(D\) over \(k\). In particular, if \(k = \overline{F}\), then \(\text{End}(V) = k\).

Prop. (15.3.1.13) [Simple Representations of Product Groups]. Let \(G_1, G_2\) be algebraic groups and \(V_1, V_2\) are simple representations of \(G_1, G_2\) resp., then \(V_1 \otimes V_2\) is a simple representation of \(G_1 \times G_2\).

Conversely, if \(\text{End}(V) = k\) for any simple representation \((V, r)\) of \(G_1\), then any simple representation of \(G_1 \times G_2\) is of this form.

Def. (15.3.1.14) [Semisimple Representations]. A linear representation \((r, V)\) of an algebraic group is called **semisimple** if it is a direct sum of simple representations. Equivalently, it is a sum of simple subrepresentation. (The proof is the same).

Or equivalently, every submodule has a complement.

Prop. (15.3.1.15) [Base Change]. Let \((V, r)\) be a f.d. linear representation of an algebraic group over a field \(k\), \(k' \triangleleft k\) a field extension, then \((V', r') = (V, r) \otimes_k k'\) is a representation of \(G_{k'}\), and
- If \((V', r')\) is simple, and \((V, r)\) is simple.
- If \((V, r)\) is simple and \(\text{End}(V) = k\), then \((V', r')\) is simple.
- If \((V, r)\) is semisimple and \(k' \triangleleft k\) is separable or \(\text{End}(V)\) is a separable algebra over \(k\), then \((V', r')\) is semisimple.


Prop. (15.3.1.16) [Constructing All F.D. Representations]. Let \(V\) be a faithful f.d. representation of \(G\), then every f.d. representation of \(G\) is a subquotient of \(V^m \otimes (V^\vee)^n\).


Def. (15.3.1.17) [Diagonalizable Representation]. A representation of an algebraic group is called **diagonalizable** if it is a direct sum of 1-dimensional representations.

Let \(G\) be an algebraic group over a field \(k\) and \(r : G \rightarrow GL(V)\) be a representation. If \(V\) is a sum of 1-dimensional representations, then \(r\) is diagonalizable (15.3.1.17).

Proof: Let \(V = \sum_{\chi \in X(G)} V_{\chi}\). If the sum is not direct, then there is are some relation \(v_1 + v_2 + \ldots + v_m = 0\) for \(v_i \in V_{\chi_i}\). Applying \(\rho\) shows
\[
0 = v_1 \otimes a(\chi_1) + \ldots + v_m a(\chi_m)
\]
so any coordinate of \(v_i\) is 0 by (7.1.1.13).

Prop. (15.3.1.18) [Chevalley]. Let \(G\) be an algebraic group, then every algebraic subgroup \(H \subset G\) arises as the stabilizer of a 1-dimensional subspace in a f.d. representation of \(G\).


Cor. (15.3.1.19). Let \(G\) be an algebraic group over a field of characteristic 0, then an algebraic subgroup \(H\) of \(G\) is normal in \(G\) iff for any linear representation \(V\) of \(G\) and a character \(\chi \in X(H)\), the eigenspace \(V_{\chi}\) is stable under \(G\).

Proof: 

Prop. (15.3.1.20). Let \(G\) be an algebraic group over a field \(k\) s.t. the order of \(\pi_0(G)\) is prime char \(k\), then any representation \(V\) of \(G\) is semisimple iff it’s semisimple when restricted to \(G^0\).

Linear Algebraic Group

Def. (15.3.1.21) [Linear Algebraic Groups]. Let \(k\) be a field, then a **linear algebraic group** over \(k\) is a closed subgroup scheme of \(GL_n\) for some \(n\).

Notice a linear algebraic group over a field of characteristic 0 is automatically smooth, by Cartier theorem (7.1.4.2).
Prop. (15.3.1.22) [Affine Algebraic Group is Linear]. If $G$ is an affine group scheme, then the regular representation (7.2.1.2) contains a faithful f.d. subrepresentation. In particular, the regular representation is itself faithful.

Proof: Let $e_i$ be a generator of $\Gamma(G)$ as a $k$-algebra, let $V$ be a f.d. subrepresentation of the regular representation containing $e_i(15.3.1.10)$, let $v_i$ be a basis for $V$, and suppose $\Delta(e_j) = \sum e_i \otimes a_{ij}$, then the image of $\Gamma(GL(V)) \to \Gamma(G)$ contains $a_{ij}$. Now because $\varepsilon : A \to k$ is the counit,

$$e_j = (\varepsilon \otimes \text{id})\Delta(e_j) = \sum \varepsilon(e_i)a_{ij},$$

so the image contains $V$, so it contains $\Gamma(G)$, so this is a closed immersion, thus a faithful representation, by (15.3.1.1).

2 Tannakian Duality

In this subsection, let $G$ be an affine group scheme, and $k$ is a field.

Lemma (15.3.2.1). Let $G$ be an affine group scheme over ring $R$ corresponding to a Hopf algebra $A$. If $u$ is an $R$-endomorphism of $A$ that the following diagram commutes:

$$
\begin{array}{c}
A \xrightarrow{\Delta} A \otimes A \\
\downarrow{u} \quad \downarrow{1 \otimes u} \\
A \xrightarrow{\Delta} A \otimes A
\end{array}
$$

then there exists a $g \in G(R)$ that $u = r_A(g)$, where $r_A$ is the regular action of $G$ on $A$.

Proof: Let $\varphi : G \to G$ be the morphism corresponding to $u$, then the commutative diagram shows $\varphi_S(xy) = x\varphi_S(y)$ for $x, y \in G(S)$. Then $\varphi_S(x) = xg_S$ where $g_S = \varphi_S(e)$.

Then for $f \in A, x \in G(R)$, $x(uf) = \varphi_R(x)(f) = (xg)(f) = x(r_A(f))$, thus $u = r_A(g)$.

Prop. (15.3.2.2). Let $G$ be an algebraic group over $k$ and $R$ is a $k$-algebra. Suppose that for any f.d. representation $(V, r_V)$ of $G$, we are given an $R$-linear map $\lambda_R : V_R \to V_R$ that satisfies:

- $\lambda_{V \otimes W} = \lambda_V \otimes \lambda_W$.
- $\lambda_1 = \text{id}$.
- For $G$-invariant maps $u : V \to W$, $\lambda_W \circ u_R = u_R \circ \lambda_V$.

then there exists a unique $g \in G(R)$ that $\lambda_V = r_V(g)$ for any $V$.

Proof: Cf. [Milne, P164].

Cor. (15.3.2.3) [Reconstruction Theorem]. Let $\omega : \text{Rep}_k(G) \to \text{Vect}_k$ be the forgetful functor, and for any $k$-algebra $R$, let $\omega_R = R \otimes \omega$, then this proposition says the canonical morphism $G(R) \to \text{End}^\otimes(\omega_R)$ is an isomorphism. Now if $\text{Aut}^\otimes(\omega)$ is the functor $R \mapsto \text{End}^\otimes(\omega_R)$, then $G \cong \text{Aut}^\otimes(\omega)$.

Cor. (15.3.2.4). Let $G, G'$ be affine algebraic groups over $k$ and let $F : \text{Rep}_k(G') \to \text{Rep}_k(G)$ be a tensor functor that $\omega^G \circ F = \omega^{G'}$, then there exists a unique homomorphism $f : G \to G'$ that $F = \omega^f$.  

Proof: Such a tensor functor defines a homomorphism
\[ F^* : \text{Aut}^\otimes(\omega^G)(R) \to \text{Aut}^\otimes(\omega^{G'})(R) \]
functorial in \( R \), thus defines a homomorphism \( f : G \to G' \) by Yoneda lemma and (15.3.2.4).

Lemma (15.3.2.5). Let \( \mu \) be a cocharacter \( G_m \to G \) over \( \overline{\mathbb{Q}_p} \), then the conjugacy class \{ \( \mu \) \} of \( \mu \) is defined over a finite extension \( E/\mathbb{Q}_p \).

Proof: By Tannakian duality, two cocharacters are conjugate over a field \( K \) iff the filtrations they defined on \( V \otimes \overline{\mathbb{Q}_p} \) for some faithful \( V \in \text{Rep}_{\mathbb{Q}_p}(G) \) are isomorphic by an action of \( G(K) \). Now this action of \( G(\overline{\mathbb{Q}_p}) \) on \( V_{\overline{\mathbb{Q}_p}} \) is defined over a f.d. field extension \( E/\mathbb{Q}_p \), so the filtrations are isomorphic by an action of \( G(E) \).

Prop. (15.3.2.6) [Abstract Jordan Decompositions]. Let \( G \) be an algebraic group over a perfect field \( k \) and \( g \in G(k) \), then there exists unique elements \( g_s, g_u \in G(k) \) that for any representation \( (V, r_V) \) of \( G \), \( r_V(g_s) = r_V(g)_s \) and \( r_V(g_u) = r_V(g)_u \). Furthermore,
\[ g = g_sg_u = g_ug_s. \]
The elements \( g_s, g_u \) are called the semisimple and unipotent parts of \( g \), and this decomposition is called the abstract Jordan decomposition of \( g \). \( g \in G(k) \) is called a semisimple or unipotent element if \( g = g_s \) or \( g = g_u \).

Proof: This follows from the functoriality of Jordan decompositions (2.3.6.7) and the reconstruction theorem (15.3.2.2).

Cor. (15.3.2.7). To check a decomposition is Jordan decomposition, it suffices to check for a single faithful representation of \( G \).

Remark (15.3.2.8). Let \( G \) be a group variety over an alg.closed field \( k \). In general, the set \( G(k)_s \) of semisimple elements in \( G(k) \) is not closed for the Zariski topology, but the set \( G(k)_u \) of unipotent elements are closed for the Zariski topology. To see this, embed \( G \) into \( GL_n \) for some \( n \), then the set of unipotent elements are the matrices with characteristic polynomial \( (T - 1)^n \), and this is a polynomial condition.

**Tannakian Reconstruction**

Prop. (15.3.2.9) [Tannakian Reconstruction]. Let \( (\mathcal{C}, \otimes) \) be a rigid Abelian tensor category that \( k = \text{End}(1) \) and \( \omega : \mathcal{C} \to \text{Vect}_k \) an exact faithful \( k \)-linear tensor functor, then the functor \( \text{Aut}^\otimes(\omega) \) is representable by an affine groups scheme \( G \), and \( \mathcal{C} \cong \text{Rep}_k(G) \).

Proof: Cf. [Milne, Tannakian category, P21].

Cor. (15.3.2.10) [Tannakian Reconstruction]. Let \( \mathcal{C} \) be a \( k \)-linear Abelian category where \( k \) is a field, and \( \otimes : \mathcal{C} \times \mathcal{C} \to \mathcal{C} \) a \( k \)-bilinear functor. Suppose there are given a faithful exact \( k \)-linear functor \( \mathcal{C} \to \text{Vect}_k \) and functorial isomorphisms \( \varphi_{X,Y,Z} : X \otimes (Y \otimes Z) \to (X \otimes Y) \otimes Z \) and \( \psi_{X,Y} : X \otimes Y \to Y \otimes X \) that
- \( F \) commutes with \( \otimes \), and maps \( \varphi \) and \( \psi \) to the natural associativity and commutativity isomorphism in \( \text{Vect}_k \).
• There exists an identity object \( 1 \in \mathcal{C} \) that \( k \to \text{End}(1) \) is an isomorphism and \( F(1) \) has dimension 1.

• Any object \( L \in \mathcal{C} \) that \( F(L) \) has dimension 1 is an invertible object.

Then \( \mathcal{C} \) is equivalent to \( \text{Rep}_k(G) \) for some affine group scheme \( G \) over \( k \). In fact, \( G \cong \text{Aut}^\otimes(\omega) \) as in (15.3.2.3)

Proof: The proof of (15.3.2.9) shows \( F \) defines an equivalence of categories \( \mathcal{C} \to \text{Rep}_k(G) \) where \( G \) is an affine monoid scheme representing \( \text{End}_k^\otimes(\omega) \). Thus we may assume \( \mathcal{C} = \text{Rep}_k(G) \).

For the rest, Cf.[Tannakian Categories, Milne, P24]. □

Cor. (15.3.2.11) [Real Algebraic Envelope]. Let \( K \) be a topological group, then the category \( \text{Rep}_R(K) \) of f.d. continuous real representations, together with the forgetful functor satisfies the hypothesis of (15.3.2.10), thus there is an algebraic group \( \widetilde{K} \) over \( R \), called the real algebraic envelope of \( K \), and an equivalence of categories

\[
\text{Rep}_R(\tilde{K}) \to \text{Rep}_R(K)
\]

induced by a homomorphism \( K \to \tilde{K}(R) \), which is an isomorphism when \( K \) is compact.

Cor. (15.3.2.12) [Hochschild-Mostow Group]. Similar as (15.3.2.11), if \( G \) is a complex Lie group or a f.g. abstract group, and \( \mathcal{C} \) the category of f.d. complex representations, then it satisfies the hypothesis of (15.3.2.10), thus it is the category of representations of an affine group scheme \( A(G) \) over \( \mathbb{C} \), together with a homomorphism \( P : G \to A(G) \), called the Hochschild-Mostow group of \( G \).

Prop. (15.3.2.13). Let \( \mathcal{C} \) be a small \( k \)-linear Abelian category, and let \( \omega : \mathcal{C} \to \text{Vect}_k \) be an exact faithful \( k \)-linear functor, then there exists a coalgebra \( C \) s.t. \( \mathcal{C} \) is equivalent to the category of \( C \)-comodules of f.d.

Proof: Cf.[Mil17] P175. □

Properties of \( G \) and \( \text{Rep}_k(G) \)

Prop. (15.3.2.14). Let \( G \) be an affine group scheme over \( k \), then

• \( G \) is finite iff there exists an object \( X \in \text{Rep}_k(G) \) that every object of \( \text{Rep}_k(G) \) is isomorphic to a subquotient of \( X^n \) for some \( n > 0 \).

• \( G \) is algebraic iff there exists an object \( X \in \text{Rep}_k(G) \) that every object of \( \text{Rep}_k(G) \) is isomorphic to a subquotient of \( X^n \otimes (X^\vee)^m \) for some \( m, n \geq 0 \).

Proof: Cf.[Milne, Tannakian categories, P25]. □

Prop. (15.3.2.15). Let \( f : G \to G' \) be a homomorphism of affine group schemes over \( k \), and let \( \omega^f \) be the corresponding functor \( \text{Rep}_k(G') \to \text{Rep}_k(G) \). Then

• \( f \) is faithfully flat iff \( \omega^f \) is fully faithful and each \( \omega^f \) induces an equivalence of subobjects of \( X' \) and \( \omega^f(X') \).

• \( f \) is a closed immersion iff every object of \( \text{Rep}_k(G) \) is isomorphic to a subquotient of an object \( \omega^f(X') \).

Proof: Cf.[Milne, Tannakian categories, P25]. □
Cor. (15.3.2.16). Let \( k \) has characteristic 0, then \( G \) is connected iff for any non-trivial representation \( X \) of \( G \), \( \langle X \rangle \) is not stable under \( \otimes \).

\( \text{Proof:} \quad \text{Cf.[Milne, Tannakian categories, P25].} \)

3 Unipotent Groups

Def. (15.3.3.1) [Unipotent Groups]. A unipotent algebraic group is an algebraic group \( G \) s.t. for any non-zero linear representation \( V \) of \( G \), \( V^G \neq 0 \). Equivalently, every such representation sends \( G \) into \( \text{Unip}(n) \) in some coordinates.

Prop. (15.3.3.2). Let \( G \) be an algebraic group over \( k \) and \( k'/k \) a field extension, then \( G \) is unipotent iff \( G_{k'} \) is unipotent.

\( \text{Proof:} \quad \text{This follows from the fact that for any representation } V \text{ of } G, (V \otimes k')^{G_{k'}} = V^G \otimes k'(15.3.1.7). \)

Prop. (15.3.3.3). For an affine algebraic group \( G \) over a field \( k \), the following are equivalent:

- \( G \) is unipotent.
- \( G \) is isomorphic to a subgroup of \( \text{Unip}(n) \) for some \( n \).
- The Hopf algebra \( \Gamma(G) \) is coconnected.

\( \text{Proof:} \quad \text{Cf.[Mil17]P281.} \)

Prop. (15.3.3.4). If \( U \) is a normal unipotent subgroup of an algebraic group \( G \), then for any semisimple representation \( V \) of \( G \), \( U \) acts trivially.

\( \text{Proof:} \quad \text{Consider a simple subrepresentation } W \text{ of } V, \text{ then } W^U \neq 0 \text{ is a subrepresentation of } G \text{ by(15.3.1.9), thus } U \text{ acts trivially on } W. \text{ As } V \text{ is a sum of simple representations(15.3.1.14), } U \text{ acts trivially on } V. \)

4 Reductive Groups

Prop. (15.3.4.1). A group variety \( G \) is reductive if it has a faithful representation that is semisimple over \( k \), by(15.3.3.4).

Prop. (15.3.4.2). Let \( k \in \text{Field}^0, G \in \text{AlgGrp}/k \) is connected, then the following are equivalent:

- \( G \) is a reductive group.
- Every f.d. representation of \( G \) is semisimple(15.3.1.14).
- Some faithful representation of \( G \) is semisimple(15.3.1.14).

\( \text{Proof:} \)
15.4 Complex Representations of Finite Groups of Lie Type

Main references are [Bon11], [Introduction to Deligne-Lustig Theory, David Schwein], [Representations of finite groups of Lie type, Dign/Michel, 1991].

Notations (15.4.0.1).

• Use notations defined in Étale Cohomology Theory.
• Let $p \in \mathbb{P}, q \in p\mathbb{Z}^+, k \in \text{Field}, \#k = q, G \in \text{AlgGrp}/k$.
• Let $\ell \in \mathbb{P}\backslash p, K$ an $\ell$-adic local field with ring of integers $\mathcal{O}_K$ and residue field $k$.

1 Finite Groups of Lie Type

Def. (15.4.1.1) [Finite Groups of Lie Type]. For a reductive group $G/\bar{k}$, if $F \in \text{End}(G)$ satisfies the fixed point of $F(\bar{k})$ is finite, then its fixed points $G^F$ is called a finite group of Lie type.

If $G$ is defined over some finite subfield $k$, i.e. $G = G_0 \times_k \bar{k}$, and $F = Fr_{G_0}$, then $G^F = G_0(k)$ is called a Chevalley group. If moreover $G_0 \in \text{AlgGrp}/k$ is reductive and simply-connected, then $G_0(k)$ is called a universal finite group (of Lie type).

If $G$ is a a finite group of Lie type that is not a Chevalley group, then it is called a twist group (of Lie type).

Prop. (15.4.1.2) [Steinberg]. If $G \in \text{AlgGrp}/\bar{k}$ is simple reductive group, and $F \in \text{End}(G)$ satisfies the fixed point of $F(\bar{k})$ is finite, then there are exactly two cases:

• (Chevalley Groups) $F$ is a standard Frobenius: $A_n, B_n, C_n, D_n, G_2, F_4, E_6, E_7, E_8$.
• (Steinberg Groups) $2A_n, 2D_n, 3D_4, 2$.
• (Suzuki Groups) $2B_2, p = 2$.
• (Ree Groups) $2G_2, p = 3$.
• (Ree Groups) $2F_4, p = 2$.

Proof: □

Examples

Prop. (15.4.1.3) [SL(n)]. $\text{PSL}(n, \mathbb{F}_q)$ is simple except for $n = 2$ and $q = 2$ or 3.

$\text{SU}(n)_{\mathbb{F}_q}$ is a twist of $\text{SL}(n)_{\mathbb{F}_q}$, denoted by $2A_{n-1}(\mathbb{F}_{q^2})$.

Proof: □

Prop. (15.4.1.4).

2 Conjugacy Classes

3 Deligne-Lustig Varieties

Def. (15.4.3.1) [Deligne-Lustig Varieties].
Affineness of Deligne-Lustig Varieties

4 Deligne-Lustig Theory

Main references are [Finite Groups of Lie Type, Carter], [D-L76], https://www.dpmms.cam.ac.uk/~dbms2/deligne_lusztig/.

Deligne and Lustig used the $\ell$-adic étale cohomology theory to construct all cuspidal representations of $G(\mathbb{F}_q)$.

Remark (15.4.4.1). Because $G(\mathbb{F}_q)$ is finite and $\mathbb{C} \cong \overline{\mathbb{Q}}_\ell$, we can consider representations $\text{Rep}(G(\mathbb{F}_q)) = \{\theta : G(\mathbb{F}_q) \to \text{GL}(\mathbb{Q}_\ell)\}$.

Def. (15.4.4.2) [Induction Pairs]. A induction pair for $G(\mathbb{F}_q)$ is a pair $(T, \theta)$, where $T \subset G$ is a maximal torus and $\theta$ is an $\ell$-adic character $T(\mathbb{F}_q) \to \overline{\mathbb{Q}}_\ell^\times$.

Deligne-Lustig Inductions

Def. (15.4.4.3) [Deligne-Lustig Inductions]. Let $(T, \theta)$ be an induction pair (15.4.4.2), the action of $G(\mathbb{F}_q)$ and $T(\mathbb{F}_q)$ on $\tilde{X}_S$ commutes, so for any $\theta \in \text{Irr}(T(\mathbb{F}_q))$, the $\theta$-isotopic part of $H^1_{\text{ét},c}(\tilde{X}_T, \overline{\mathbb{Q}}_\ell)$ is $G(\mathbb{F}_q)$-invariant, thus we can define a Deligne-Lustig Induction map that on $\text{Irr}(G(\mathbb{F}_q))$ is defined by

$$R^T_G : \text{Irr}(T(\mathbb{F}_q)) \to \text{K}_0(\text{Rep}(G(\mathbb{F}_q))) : \theta \mapsto \sum_i (-1)^i H^1_{\text{ét},c}(\tilde{X}_T, \overline{\mathbb{Q}}_\ell)^\theta.$$ 

Prop. (15.4.4.4). Let $(T, \theta)$ be an induction pair, if $\theta^w \neq \theta$ for any $w \in W$, then $R^T_G(\theta) \in \text{Irr}(G(\mathbb{F}_q))$.

Proof:

Prop. (15.4.4.5). If $(T, \theta), (T', \theta')$ are two induction pairs that are note $G(\mathbb{F}_q)$-conjugate, then $(R^T_G(\theta), R^T_G(\theta')) = 0$.

Proof:

Def. (15.4.4.6) [Geometrically Conjugate Pairs]. If $(T, \theta), (T', \theta')$ are two induction pairs, they are called geometrically conjugate if $(T_{k'}, \theta \circ Nm_{k'/k}), (T'_{k'}, \theta' \circ Nm_{k'/k})$ are $G(k')$-conjugate for some finite extension $k'/\mathbb{F}_q$.

Prop. (15.4.4.7). If $(T, \theta), (T', \theta')$ are two induction pairs that are not geometrically conjugate, then $R^T_G(\theta), R^T_G(\theta')$ are disjoint.

Proof: Cf. [D-L76] Cor6.3.

Def. (15.4.4.8) [Dual Groups].

Prop. (15.4.4.9). The geometric conjugacy classes of induction pairs of $G$ corresponds to the geometric conjugacy classes of semisimple elements of $G^*(15.4.4.8)$.

Proof:

Def. (15.4.4.10) [Lustig Series]. Let $S$ be a semisimple conjugacy class of $G^*$, the Lustig series $\mathcal{E}(G, S)$ is the set of irreducible representations of $G$ occurring in $R_G^T(\theta)$ for any $(T, \theta)$ in the geometric conjugacy class corresponding to $S$ via (15.4.4.9). By (15.4.4.7),

$$\text{Irr}(G(\mathbb{F}_q)) = \prod_{S \in G^*_\text{ss-conj}} \mathcal{E}(G, S).$$

$\mathcal{E}(G, (1))$ is called the set of unipotent representations, which are all the irreducible representations appearing in $R^T_G(1)$ for various $T$. 

5 Howlett-Lehler Theory

This theory decomposes Deligne-Lustig inductions into irreducible components.

6 Character Sheaves (Lustig)

References are [Introduction to character sheaves, Lustig], [Algebraic And Geometric Methods In Representation Theory, Lustig, 2014].

Remark (15.4.6.1). Let \((S, \theta)\) be an induction pair (15.4.4.2), there is in fact an isomorphism

\[
H^i_{\text{ét}, c}(\tilde{X}_S, \mathcal{O}_\ell) \cong H^i_{\text{ét}, c}(X_S, \mathcal{F}_\theta) \in \text{Rep}(G(F_q))
\]

where \(\mathcal{F}_\theta\) is the \(\ell\)-adic local system on \(X_S\) corresponding to the \(S(F_q)\)-torsor and \(\theta\). Thus much of the Deligne-Lustig theory can be interpreted in the language of sheaves, called character sheaves.

7 Gelfand-Graev representations

8 Alvis-Curtis Duality

Cf. [Duality for representations of a reductive group over a finite field, I, II, Deligne-Lustig].

9 Deligne-Lustig Varieties

Prop. (15.4.9.1). Let

10 GL(n)

Notations (15.4.10.1). The notation is the same as in (15.8.0.1).

Principal Series Representations

Prop. (15.4.10.2). Let \((\pi, V) \in \text{Rep}^{fd}(GL(2, k))\), then

- if the representation \((\pi_1, V)\) is defined by \(\pi_1(g) = \pi(g^{-t})\), then \(\pi_1 \cong \pi\).
- if \(n = 2\) and \((\pi, V)\) is irreducible, let \(\omega\) be the central character of \(\pi\). If \((\pi_2, V)\) is defined by \(\pi_2(g) = \omega(\deg g)^{-1}\pi(g)\), then \(\pi_2 \cong \pi\).

Proof: The proof of (15.8.1.15) applies to this case, noticing a finite group is profinite hence locally profinite.

Lemma (15.4.10.3). Let \(\chi_1, \chi_2, \mu_1, \mu_2\) be characters of \(F^*\), consider the principal representations \(\mathcal{B}(\chi_1, \chi_2), \mathcal{B}(\mu_1, \mu_2)\) of \(GL(2, k)\) defined in (15.8.4.6), then

\[
\dim \text{Hom}_{GL(2, k)}(\mathcal{B}(\chi_1, \chi_2), \mathcal{B}(\mu_1, \mu_2)) = \delta_{\chi_1, \mu_1} \delta_{\chi_2, \mu_2} + \delta_{\chi_1, \mu_2} \delta_{\chi_2, \mu_1}.
\]

Proof: Let \(\chi, \mu\) be characters of \(B(k)\) defined as in (15.8.4.6), then by ??, the dimension is just the dimension of space of functions \(\Delta : GL(2, k) \to \mathbb{C}\) that

\[
\Delta(b_2gb_1) = \mu(b_1)\Delta(g)\chi(b_1), \quad b_1, b_2 \in B(k).
\]

Then by the Bruhat decomposition (11.6.6.5), \(\Delta\) is determined by its values on 1 and \(w_0\). Notice that if \(\chi_1 \neq \mu_1\) or \(\chi_2 \neq \mu_2\), we can use this condition to show \(\Delta(1) = 0\), and if \(\chi_1 \neq \mu_2\) or \(\chi_2 \neq \mu_1\), we can use this condition to show \(\Delta(w_0) = 0\), and also the construction of \(\Delta\) is clear in other cases.

□
Prop.(15.4.10.4)[Principal Series Representations]. Let \( \chi_1, \chi_2, \mu_1, \mu_2 \) be characters of \( F^* \), then \( B(\chi_1, \chi_2) \) is an irreducible representation of degree \( q = |F| + 1 \) unless \( \chi_1 = \chi_2 \), in which case it is the direct sum of two irreducible representations having degree 1 and \( q \). And \( B(\chi_1, \chi_2) \cong B(\mu_1, \mu_2) \) if \( \{\chi_1, \chi_2\} = \{\mu_1, \mu_2\} \).

Proof: Use(15.4.10.3), then

\[
\dim \text{End}_{GL(2,k)}(B(\chi_1, \chi_2)) = 1 + \delta_{\chi_1, \chi_2}.
\]

Now by Peter-Weyl, if a representation \( V \) is isomorphic to \( \sum d_i \pi_i \), where \( \pi_i \) are irreducible, then

\[
\dim_G(V) = \sum d_i^2 \text{[10.9.4.5]}.\]

Then we now \( B(\chi_1, \chi_2) \) decomposes into two representations if \( \chi_1 = \chi_2 \) and is irreducible if \( \chi_1 \neq \chi_2 \).

In case \( \chi_1 = \chi_2 \), there is an invariant subspace of dimension 1, generated by the function

\[ f(g) = \chi(\deg g). \]

so the rest representation is of dimension \( q \), because \( G(2,k)/B(k) = q + 1 \).

\[ \square \]

Def.(15.4.10.5) [Steinberg Representation]. We call the \( q \)-dimensional subrepresentation of \( B(1,1) \) the Steinberg representation. It is verified that the \( q \) dimensional subrepresentation of \( B(\chi, \chi) \) is the twist of the Steinberg representation.

Weil Representations

Prop.(15.4.10.6) [Weil Representation for \( SL(2,k) \)]. In situation(15.14.4.5), let \( W = L^2(E) \), define the modified Fourier transform w.r.t. \( \psi \) as in(10.9.3.33):

\[
\hat{\Phi}(x) = q^{-1} \sum_{y \in E} \Phi(y) \psi(\text{tr}(xy)).
\]

Then there is a Weil representation \( \omega : SL(2,k) \to \text{End}(W) : \)

\[
(\omega(t(a))\Phi)(x) = \Phi(ax), \quad w(n(z))\Phi(x) = \psi(zN(x))\Phi(x), \quad (\omega(w_1)\Phi)(x) = \varepsilon \Phi(x).
\]

where we are using the presentation as in6, and \( \varepsilon = 1 \) is \( E/F \) is split, and \( -1 \) if it is anisotropic.

Remark(15.4.10.7). When \( F \) has characteristic\( \neq 2 \), this is just the Weil representation in(15.14.4.3).

Proof: This follows from direct verification, Cf.[Bump, P407]. \[ \square \]

Prop.(15.4.10.8) [Dihedral Weil Representations for \( GL(2,k) \)]. Situation as in(15.14.4.5), Define

\[
W(\chi) = \{ \Phi \in W|\Phi(yx) = \chi(y)^{-1}\Phi(x), y \in E_1^* \},
\]

then by considering the order of \( E_1^* \), \( \dim W(\chi) = q + \varepsilon \). Also it is verified that \( W(\chi) \) is stable under the Weil representation of \( SL(2,k)(15.4.10.6) \).

Now we want to extend this representation to \( GL(2,k) \) by defining

\[
(\omega(\begin{bmatrix}a & \cr & 1 \end{bmatrix})\Phi)(x) = \chi(b)\Phi(bx)
\]

where \( b \) is arbitrary that \( N(b) = a \).

Remark(15.4.10.9). This is related to(15.14.4.7) and Howe duality.
Proof: It must be shown that this is truly a representation of \( GL(2, k) \), it suffices to show that
\[
\omega\left(\begin{bmatrix} a \\ 1 \end{bmatrix}\right)\omega(g)\omega\left(\begin{bmatrix} a^{-1} \\ 1 \end{bmatrix}\right) = \omega\left(\begin{bmatrix} a \\ 1 \end{bmatrix} g \begin{bmatrix} a^{-1} \\ 1 \end{bmatrix}\right),
\]
where \( g \) is a generator of \( SL(2, k) \). This is clear for \( g = t(a) \), and also clear for \( g = n(z) \). For \( g = w_1 \), it suffices to check
\[
\omega\left(\begin{bmatrix} a \\ 1 \end{bmatrix}\right) \circ \wedge \circ \omega\left(\begin{bmatrix} a^{-1} \\ 1 \end{bmatrix}\right) \Phi(x) = \hat{\Phi}(ax)
\]
which is subtle but also clear. \(\square\)

Prop. (15.4.10.10) [Split Weil Representation]. In the split case, the character \( \chi \) of \( E^* \) is of the form \( \chi((x, y)) = \chi_1(x)\chi_2(y) \), and then condition in (15.14.4.5) just says \( \chi_1 \neq \chi_2 \). Then:
\[
(\pi(\chi), W(\chi)) \cong B(\chi_2, \chi_1)
\]

Proof: The intertwining operator is given by
\[
L : W(\chi) \to B(\chi_2, \chi_1) : (L\Phi)(g) = (\omega(g)\Phi)((1, 0)).
\]
Firstly \( L\Phi \in B(\chi_2, \chi_1) \) by direct verification for \( t(a), T_1(k) \) and \( n(z) \). Then it is an intertwining operator is clear.

Then this is an isomorphism because both are of dimension \( q + 1 \) and \( B(\chi_2, \chi_1) \) is irreducible (15.4.10.4). \(\square\)

Def. (15.4.10.11) [Cuspidal Representation]. \( (\pi, V) \in \text{Rep}^{\text{fd}}(GL(2, k)) \) is called a cuspidal representation if the Jacquet module \( J(V) = 0 \). Notice in this finite case, this is equivalent to \( V \) has no \( N(k) \)-fixed vector, because the contragradient is well-known as \( \text{Rep}(G) \) is semisimple, and the trivial isotropic parts correspond, unlike the \( p \)-adic case.

Lemma (15.4.10.12). If \( (\pi, V) \) is a cuspidal representation of \( GL(2, k) \), then the dimension of \( V \) is a multiple of \( q - 1 \).

Proof: Because \( N(k) \cong F \), any character of \( N(k) \) is of the form \( \psi_a(n(x)) = \psi(ax) \). Now decompose the contragradient representation \( V^* \) of \( G \) into isotypic parts of \( N(k) ; V^* = \oplus_{a \in F} V^*(a) \), then the hypothesis implies \( V^*(0) = 0 \).

Notice that the group \( T_1(k) \) acts transitively on the spaces \( V^*(a), a \neq 0 \) by \( \hat{\pi}\left(\begin{bmatrix} t \\ 1 \end{bmatrix}\right)l \), because
\[
\begin{bmatrix} t \\ 1 \end{bmatrix}\begin{bmatrix} 1 & x/t \\ 1 & 1 \end{bmatrix} = \begin{bmatrix} 1 & x \\ 1 & 1 \end{bmatrix}\begin{bmatrix} t \\ 1 \end{bmatrix}.
\]
So the dimension of \( V \) is a multiple of \( q - 1 \). \(\square\)

Prop. (15.4.10.13) [Anisotropic Representation]. In the anisotropic case, the Weil representation \( (\pi(\chi), W(\chi)) \) is cuspidal and irreducible.
Prop. (15.4.10.14) [Classification of Representations of $GL(2, k)$]. There is a list of all irreducible representations of $GL(2, k)$:

- $q - 1$ 1-dimensional representations $\chi(\deg g)$, where $\chi$ is a character of $k^\times$.
- $\frac{(q-1)(q-2)}{2}$ principal series representations of dimension $q + 1$.
- $q - 1$ Steinberg representations (with twists) of dimension $q$.
- $\frac{q(q-1)}{2}$ cuspidal Weil representations of dimension $q - 1$.

Proof: All these are irreducible representations by (15.4.10.4)(15.4.10.5) and (15.4.10.13). It suffices to show they are not isomorphic. Notice different kind of representation have different dimensions, thus it suffices to compare the same representations.

For principal series representations $B(\chi_1, \chi_2), \chi_1 \neq \chi_2$, their isomorphisms are known by (15.4.10.4). For Steinberg representations, twisting are clearly different. For cuspidal Weil representations, there are $q^g - q$ way of choosing $\chi(15.14.4.5)$ and \textup{Cf.} [Local Langlands For GL(2)].

Finally, they are all the irreducible representations by the fact $\sum d^2_\sigma = |G| = (q - 1)^2q(q + 1) (15.1.2.4)$. □

Whittaker Models

Def. (15.4.10.15) [Whittaker Functionals & Whittaker Models]. Let $(\pi, V)$ be an irreducible representation of $GL(2, k)$, then the notion of Whittaker functional and Whittaker model is defined as in (15.8.3.1).

Prop. (15.4.10.16) [Existence and Uniqueness of Whittaker Models]. Let $\mathcal{G}$ be the representation of $GL(2, k)$ induced from the character $\psi_N(n(z)) = \psi(z)$ on $N(k)$, then it is multiplicity-free, and every irreducible representation of dimension $> 1$ occurs in it. Notice that this is just the existence and uniqueness of Whittaker models.

Proof: To show multiplicity free, it suffices to show $\text{End}_{GL(2, k)}(\mathcal{G})$ is commutative, by Shur’s lemma (10.9.2.4). Then we use \textup{??}, which says this ring is isomorphic to the ring of functions $\Delta$ on $G$ that

$$\Delta(n_2gm_1) = \psi_N(n_2)\Delta(g)\psi_N(n_1).$$

where the multiplication is convolution \textup{??}.

Notice it follows from the the Bruhat Decomposition (11.6.6.5) that the double coset $N(k)\backslash GL(2, k)/N(k)$ is uniquely represented by matrices with exactly two non-zero entries. Then it is clear a diagonal coset can support a function $\Delta$ iff it is a scalar multiple of $I$. In other words, the representatives are

$$\begin{bmatrix} a & \ast \\ a & \ast \end{bmatrix}, \quad \begin{bmatrix} b & \ast \\ c & \ast \end{bmatrix}.$$
Consider the involution of $G$ given by

$$\iota(g) = w_1 g^t w_1^{-1},$$

then it is an anti-involution of $G$ and it induces isomorphism on $N(k)$, so it induces an anti-involution of order two on the ring of functions $\Delta$ by $\iota(\Delta)(g) = \Delta(\iota(g))$. Notice this is an anti-involution because of (10.9.1.27) and the fact a finite group is unimodular. But this anti-involution fixes the representatives as above, so it is in fact identity on these $\Delta$, which proves the convolution is commutative.

For the last assertion, just notice the dimension of $G$ is $(q - 1)(q^2 - 1)$, and the sum dimensions of irreducible representations of dimension $> 1$ is just $(q - 1)(q^2 - 1)$ by (15.4.10.14).

**Cor. (15.4.10.17).** Frobenius reciprocity (10.9.5.5) implies that the space of Whittaker functionals is of dimension 1 for any irreducible representation of dimension $> 1$.

### 11 SL$(n)$

**Def. (15.4.11.1) [Drinfeld Curves].** The Drinfeld curve is defined to be the affine plane curve $Dri/A_q^2$

$$Dri : x^q y - xy^q = 1$$

with completion $\overline{Dri} = Dri \cup \{\infty\} \subset \mathbb{P}_q^2$.

**Prop. (15.4.11.2).** There is a natural $\mu_{q+1} \times SL(2, \mathbb{F}_q)$-action on $Dri$, which induces a map on $H^*_c(Dri, \mathbb{Q}_\ell)$. Then we get the Deligne-Lustig induction

$$R^G_{T'} : \mu_{q + 1}^* \to K_0(\text{Rep}^{fd}(SL(2, \mathbb{F}_q))).$$

**Proof:**

<table>
<thead>
<tr>
<th>Reps\Classes</th>
<th>1</th>
<th>-1</th>
<th>1</th>
<th>-1</th>
<th>1</th>
<th>-1</th>
<th>1</th>
<th>-1</th>
<th>1</th>
<th>-1</th>
<th>1</th>
<th>-1</th>
</tr>
</thead>
<tbody>
<tr>
<td>size</td>
<td>1</td>
<td>1</td>
<td>6</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
<td>4</td>
</tr>
<tr>
<td>$\chi^2$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>$\omega$</td>
<td>$\omega^2$</td>
<td>$\omega^2$</td>
<td>$\omega$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\chi^2 \rho$</td>
<td>2</td>
<td>-2</td>
<td>0</td>
<td>-1</td>
<td>-1</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\chi^2 \rho$</td>
<td>2</td>
<td>-2</td>
<td>0</td>
<td>$-\omega$</td>
<td>$-\omega^2$</td>
<td>$\omega^2$</td>
<td>$\omega$</td>
<td></td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
<tr>
<td>$\pi$</td>
<td>3</td>
<td>3</td>
<td>-1</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td>0</td>
<td></td>
<td></td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Figure (15.4.11.1): Character Table of $SL(2, \mathbb{F}_3)$

### 12 GL$(n)$

References are [Representations of the Finite Classical Groups, Zelevinsky, 1981].

**Thm. (15.4.12.1) [Irreducible Characters of $GL(n, \mathbb{F}_q)$, Green].**
13 $Sp_{2n}$

Thm. (15.4.13.1) [Irreducible Characters of $Sp(2n, F_q)$, Green].
15.5 Bruhat-Tits Theory

1 Buildings
Main references are [Serre, Trees].

2 Bruhat-Tits Buildings
Main references are [Reductive Groups over Local Fields, Tits] and [A Compatification of the Bruhat-Tits Building], [the Bruhat-Tits Buildings of a $p$-adic Chevalley Group and an Application to Representation Theory, Rabinoff].

Def. (15.5.2.1) [Bruhat-Tits Buildings]. For a Chevalley group $G = G(F)$, the Bruhat-Tits building $B(G)$ is a building that
- vertices of $B(G)$ corresponds to the set of compact open subgroups of $G$.
- $B(G)$ is a union of subcomplexes called apartments, corresponding to the set of split maximal tori $T$ of $G$.

Prop. (15.5.2.2)[$B(SL(2, Q_p))$]. The Bruhat-Tits building $B(SL(2, Q_p))$ is a $(p+1)$-regular tree where
- vertices of $B(SL(2, Q_p))$ corresponds to homothety classes of lattices $[\Lambda]$ in $Q_p^2$.
- edges of $B(SL(2, Q_p))$ corresponds to adjacent pairs of lattices in $Q_p^2$.

3 Compactifications
15.6 Representations of (Non-Compact)Lie Groups

Remark (15.6.0.1)[Non-compact Lie Groups]. The feature of representations of non-compact Lie groups is most intersecting representations are $\infty$-dimensional and involves topologies. The vector space $V$ is assumed to be Hausdorff, second countable and complete, locally convex, and separable.

1 Basics

Prop. (15.6.1.1)[Left Invariant Differential Operators]. For a connected Lie group $G$, consider its left and right regular action $\lambda, \rho$ on $C^\infty(G)$. We will write $dX$ for $X \in g$ as the representation of Lie algebra of $G$ via $\rho$, then it commutes with $\lambda$. So it induces a map of $U(g)$ to the ring of left $G$-invariant differential operators on $G$.

Prop. (15.6.1.2)[Center element Bi-invariant]. If $G$ is a connected Lie group with Lie algebra $g$ and $D \in Z(U(g))$, then the differential operator $D$ defined in (15.6.1.1) is invariant under both left and right regular representations of $G$.

Proof: The left invariance is general from (15.6.1.1), for the right invariance, Because $G$ is connected, it suffices to prove invariance for a nbhd of identity of $G$, thus suffices to prove

$$\rho(g_t)D = D\rho(g_t), \quad g_t = \exp(tX).$$

For this, let $\varphi(g, t) = (\rho(g_t)D - D\rho(g_t))(g)$ and take derivative w.r.t $t$, then it reads:

$$\frac{\partial}{\partial t}\varphi(g, t) = (DdX\rho(g_t)f - dX\rho(g_t)Df)(g) = dX\varphi(g, t)$$

because $dX$ commutes with $D$. And also $\varphi(g, 0) = 0$, so by lemma (15.6.1.3), $\varphi(g, t) = 0$ for any $t, g$. □

Lemma (15.6.1.3). If $G$ is a connected Lie group with Lie algebra $g$, and $\varphi \in C^\infty(G \times \mathbb{R})$ satisfies

$$\frac{\partial}{\partial t}\varphi(g, t) = dX\varphi(g, t)$$

for some $X \in g$ and $\varphi(g, 0) = 0$, then $\varphi = 0$.

Proof: Let $\varphi_g(u, v) = \varphi(g \exp(uX), v)$, then the condition says

$$\frac{\partial}{\partial u}\varphi_g(u, v) = \frac{\partial}{\partial v}\varphi_g(u, v),$$

which means $\varphi_g(u, v) = F(u + v)$, and the fact $\varphi_g(u, 0) = 0$ shows $F = 0$. □

Cor. (15.6.1.4). If $G = GL(2, \mathbb{R})^+$, then $g = gl_2(\mathbb{R})$, and the Casimir element (2.5.8.20) $\Delta = -1/2(1/2h^2 + ef + fe)$ corresponds to a bi-invariant differential operator on $C^\infty(G)$, and it is called the Laplace-Beltrami operator.
Differential Vectors

Def. (15.6.1.5) [Smooth Vectors]. Let $V$ be a continuous representation of $G$ on a locally convex TVS. we define the space $V^\infty$ of smooth vectors of $V$ as $V^\infty = \cap_n V^n$ where

$$V^0 = \{ v \in V^{n-1}, \frac{d}{dt} \exp(t\xi)v \text{ exists} \}, \quad V^n = \{ v \in V^{n-1}, T_\xi(v) \in V^{n-1}, \forall \xi \in \mathfrak{g} \}.$$ 

And $V^\infty$ is given the inverse limit topology.

Prop. (15.6.1.6) [Action of Distribution on Smooth Vectors]. There is a continuous action of $\text{Distr}_c(G)$ on $V^\infty$: $T \mapsto \pi(T)$ compatible with the convolution structure on $\text{Distr}_c(G)$.

Proof: For $v \in V^\infty$, define $F^v(g) = g(v)$. For $T \in \text{Distr}_c(G)$, define

$$\pi(T)v = (T, F^v)$$

. For example,

- $\pi(\delta_\xi) = \pi(x)$.
- $\pi(u) = u$ for $u \in U(\mathfrak{g})$.
- $\pi(f\,dg)v = \int_G f(g)\pi(g)vdg$ for $f \in C_c(G)$.
- $\pi(f \ast g) = \pi(f)\pi(g)$.

Cor. (15.6.1.7). If $f \in C_c^\infty(G)$, then for any $v \in V$, the vector $T_{f_\mu_{\text{Haar}}}(v) \in V^\infty$.

Proof: Notice $X\pi(f)v = \pi(X \ast f)v$, and we calculate $X \ast f$:

$$(X \ast f, v) = \int \frac{d}{dt}\pi(e^{tX}y)v f(y)dy = \frac{d}{dt} \int f(y)\pi(e^{tX}y)vdv = \frac{d}{dt} \int f(e^{-tX}y)\pi(y)vdv = \pi(f_X)v$$

where $f_X(g) = \frac{d}{dt}(e^{-tX}g)|_{t=0}$ is smooth. Iterating, we can show $\pi(f)v \in V^\infty$.

Cor. (15.6.1.8) [Smooth Vectors Dense]. $V^\infty$ is dense in $V$.

Proof: Choose a Dirac sequence $\{f_n\}$, then $T_{f_n\mu_{\text{Haar}}}v \in V^\infty$ converges to $v$, by (15.6.1.6).

Cor. (15.6.1.9). If $V$ is a f.d. vector space, then $V^\infty = V$.

Prop. (15.6.1.10) [Smooth Vectors in $S^1$]. Let $K = S^1$ and $\rho$ be the regular representation on the Hilbert space $L^2(K) = L^2[0, 2\pi]$, then the smooth vectors in $\rho$ are just precisely the elements of $C^\infty(K)$.

Proof: Take a Fourier expansion $f(x) = \sum a_n e^{2\pi inx}$. Suppose $f$ is a $C^1$ vector, then there is a $g(x) = \sum b_n e^{2\pi inx}$ that $\lim \frac{1}{t}(f_t - f) = g$, so

$$\lim_n \sum_n |\frac{1}{t}(e^{2\pi int} - 1)a_n - b_n|^2 = 0.$$ 

which means $b_n = 2\pi ina_n$.

So if $f$ is a $C^\infty$ vector, then $|a_n|$ decay rapidly, and $f$ and all its derivatives converge absolutely so $f$ is smooth. Conversely, integration shows the Fourier coefficients of any smooth function $f$ decay rapidly.
Examples

Prop.(15.6.1.11)[Store-Newmann]. The Heisenberg representation of $H$ acting on $L^2(\mathbb{R})$ is unitary and irreducible, where $\pi(p_a) = e^{iax}$, and $\pi(r_b) = T_b$.

Prop.(15.6.1.12)[SL$^2(\mathbb{R})$]. Let $\widetilde{SL}_2(\mathbb{R})$ be the universal covering of $SL_2(\mathbb{R})$. Then $\text{Rep}_f(\widetilde{SL}_2(\mathbb{R})) = \text{Rep}_f(SL_2(\mathbb{R}))$. In particular, $SL_2(\mathbb{R})$ admits no f.d. faithful representations, and the only quotients of it that admit f.d. faithful representations are $SL_2(\mathbb{R})$ and $PSL_2(\mathbb{R})$.

Proof: Let $\rho : \widetilde{SL}_2(\mathbb{R}) \to GL(n, \mathbb{R})$ be a representation inducing a real Lie algebra representation $\rho_*$. Consider its complexification $\rho \otimes \mathbb{C} : \widetilde{SL}_2(\mathbb{R}) \to GL(n, \mathbb{C})$. Because $SL(2, \mathbb{C})$ is simply connected by(11.6.4.17), $\rho_* \otimes \mathbb{C}$ corresponds to a complex representation $\rho' : SL(2, \mathbb{C}) \to GL(n, \mathbb{C})$ by(11.6.3.13). Now because $\widetilde{SL}_2(\mathbb{R})$ is simply connected, so there is a real Lie group homomorphism $\gamma : SL_2(\mathbb{R}) \to SL(2, \mathbb{C})$ that $\rho' \circ \gamma = \rho$. But because $\rho, \rho'$ both commutes with conjugation, so does $\gamma$. Thus the image of $\gamma$ is in $GL(2, \mathbb{R})$, and $\rho$ factors through $SL(2, \mathbb{R})$.

There is a quotient map $\pi : \widetilde{SL}_2(\mathbb{R}) \to PSL_2(\mathbb{R})$, and $PSL_2(\mathbb{R})$ has trivial center, so the center of $SL_2(\mathbb{R})$ is contained in $\ker(\pi)$, which is isomorphic to $\pi_1(PSL_2(\mathbb{R})) = \mathbb{Z}$, and is central in $SL_2(\mathbb{R})$ by(11.6.1.6), so the center of $\widetilde{SL}_2(\mathbb{R})$ is just $\mathbb{Z}$. By what has been proved, for any representation of other covering space of $PSL_2(\mathbb{R})$, the induced representation on $\widetilde{SL}_2(\mathbb{R})$ factors through $SL_2(\mathbb{R})$, thus trivial on the subgroup $2\mathbb{Z} \subset \mathbb{Z}$, and the original representation factors through $SL_2(\mathbb{R})$ or $PSL_2(\mathbb{R})$. So the only possibility of faithful representation is $SL_2(\mathbb{R})$ or $PSL_2(\mathbb{R})$. For $PSL_2(\mathbb{R})$, take the

Prop.(15.6.1.13)[F.D. Representations of $SL_2(\mathbb{K})$]. Let $\mathbb{K} = \mathbb{C}$ or $\mathbb{R}$, then the representations of $SL(2, \mathbb{K})$ are isomorphic to direct representations $(\rho_n, V_n)$, where $V_n$ = homogeneous polynomials of degree $n$ in indeterminants $x, y$, and

$$\rho_n \begin{bmatrix} a & b \\ c & d \end{bmatrix} (x^ky^{n-k}) = (ax + by)^k(cx + dy)^{n-k}.$$  

Proof: We can check these representations truly induce irreducible representations of their Lie algebras $\mathfrak{sl}_2(\mathbb{K})$. Notice $SL(2, \mathbb{C})$ is simply connected by(11.6.4.17), so(15.6.1.12) and(11.6.3.13) gives the result.

2 Finite-Dimensional Representations

Prop.(15.6.2.1). Finite dimensional representations of a semisimple Lie group is completely reducible.

Proof: This is because its Lie algebra representation is completely reducible by(15.15.1.2), and each subrepresentation corresponds to a Lie group subrepresentation.

3 $(\mathfrak{g}, K)$-Modules

$(\mathfrak{g}, K)$-Modules

Def.(15.6.3.1)[$(\mathfrak{g}, K)$-Modules]. If $G$ is a Lie group that may not be connected, and $K \subset G$ be a maximal compact Lie subgroup by(7.3.6.11), then $K$ acts on $\mathfrak{g}$. Then a $(\mathfrak{g}, K)$-module is a $C$-vector space that has a $K$-finite action and a $\mathfrak{g}$ action that satisfies:
for $k \in K, \eta \in \mathfrak{g}$, $T_k \eta T_k^{-1} = T_{\text{Ad}_k(\eta)}$.

2. The action of $\mathfrak{h}$ on $V$ induced by $K$ agrees with the restriction of the action of $\mathfrak{g}$.

A $(\mathfrak{g}, K)$-module is called **admissible** iff every $V^\rho$ is of f.d..

**Def. (15.6.3.2)[Contragradient $(\mathfrak{g}, K)$-Module].** If $M$ is an admissible $(\mathfrak{g}, K)$-module, then we can define its **contragradient $(\mathfrak{g}, K)$-module** as

$$M^\vee = (M^*)^\infty = \bigoplus \rho(M^\rho)^*,$$

which is the $K$-finite part of the usual dual of $M$, and $\mathfrak{g}$ clearly acts on it.

**$(\mathfrak{g}, K)$-Modules and $\mathfrak{g}$-Modules**

**Def. (15.6.3.3).** Let $K_0$ be the unital component of $K$, then there are forgetful functors

$$\text{Mod}_{(\mathfrak{g}, K)} \to \text{Mod}_{(\mathfrak{g}, K_0)} \to \text{Mod}_{\mathfrak{g}}.$$

**Prop. (15.6.3.4).** The functor $(\mathfrak{g}, K_0) - \text{mod} \to \mathfrak{g} - \text{mod}$ is fully faithful, and its essential image is stable under taking submodules.

**Proof:** Cf. [Gaitsgory P39].

**Cor. (15.6.3.5).** If $M \in (\mathfrak{g}, K) - \text{mod}$ is irreducible as a $\mathfrak{g}$-module, then it is irreducible.

**Prop. (15.6.3.6).** The functor $\text{Mod}_{(\mathfrak{g}, K)} \to \text{Mod}_{\mathfrak{g}}$ sends f.g. objects to f.g. objects.

**Proof:** By (15.6.3.4), it suffices to consider the functor $(\mathfrak{g}, K) - \text{mod} \to (\mathfrak{g}, K_0) - \text{mod}$. Let $M$ be f.g. $(\mathfrak{g}, K)$-module, and $\bigcup M_i = M$ be a chain of $(\mathfrak{g}, K_0)$-submodules. Pick $k \in K$ for each element of $\pi_0(K)$(f.m.), then each $M'_i = \sum k(M_i)$ is a $(\mathfrak{g}, K)$-submodule, thus $M'_i = M$ for some $i$. Now we can choose $j$ large that $k(M_i) \in M_j$ for any $k$, then $M_j = M$(because we may choose $M_i$ be f.g. $(\mathfrak{g}, K_0)$-modules).  

**Cor. (15.6.3.7).** The category $\text{Mod}_{(\mathfrak{g}, K)}$ is Noetherian.

**Proof:** If $M \in (\mathfrak{g}, K) - \text{mod}$ is f.g. and $M_1 \subset M$, then $M$ is f.g. as $\mathfrak{g}$-module, then $M_1$ is f.g. as $\mathfrak{g}$-module by (2.5.8.16). So clearly it is also f.g. as a $(\mathfrak{g}, K)$-module.

**Prop. (15.6.3.8).** For an irreducible $(\mathfrak{g}, K)$-module $M$, the underlying $\mathfrak{g}$-module is a direct sum of f.m. irreducibles.

**Proof:** By (15.6.3.4), it suffices to prove $M$ is a direct sum of f.m. irreducible $(\mathfrak{g}, K_0)$-modules. $M$ is f.g. as a $(\mathfrak{g}, K_0)$-modules by the proof of (15.6.3.6), so it has a maximal submodule $M'$ that $N = M/M'$ is irreducible. Pick $k \in K$ for each component of $K$, consider

$$M'' = \cap k(M')$$

which is a proper $(\mathfrak{g}, K)$-submodule of $M$, so it is 0. Hence the map

$$M \to \oplus (N)^k$$

is injective, where $N^k$ is $N$ twisted by conjugate action of $k$, so it is a submodule of a semisimple-module, thus semisimple.
Properties of \((\mathfrak{g}, K)\)-Modules

Cor. (15.6.3.9)[Schur’s Lemma]. Schur’s lemma holds for irreducible \((\mathfrak{g}, K)\)-modules.

**Proof:** It suffice to show any endomorphism \(S\) of an irreducible \((\mathfrak{g}, K)\)-module \(M\) has an eigenvalue. But \(S\) preserves \(M^\rho\) for any \(\rho\), and \(M^\rho\) is of f.d, thus it has an eigenvalue over \(\mathbb{C}\). \(\square\)

Cor. (15.6.3.10)[Irreducible Unitary Representation Determined by Finite Part]. If \(V_1, V_2\) are two irreducible unitary representations of \(G\) that are infinitesimal equivalent, then they are isomorphic.

**Proof:** Firstly they are admissible by (15.6.4.7), so we can talk about their corresponding \((\mathfrak{g}, K)\)-modules \(M_i\), then \(V_i\) are the Hilbert space completion of \(M_i\) by (15.6.3.24).

Now \(M_i\) has Hermitian forms, so \(M_i \cong (M^*)^{alg}\), and if \(S : M_1 \cong M_2\), then \(S^*S\) is an automorphism of \(M_1\), thus by (15.6.3.25) it is a scalar map, so after a scalar change, we may assume \(S\) preserves Hermitian structure thus induces an isomorphism of vector spaces \(V_1 \cong V_2\), so by (15.6.3.24) it is an isomorphism of \(G\)-representations. \(\square\)

Prop. (15.6.3.11). Any irreducible \((\mathfrak{g}, K)\)-module has a Banach space structure.

**Proof:**

**Action of** \(Z(U(\mathfrak{g}))\)

Prop. (15.6.3.12). Let \(M\) be an admissible \((\mathfrak{g}, K)\)-module, then

\[ M \cong \bigoplus_{\chi \in \text{Spec}(Z(\mathfrak{g}))} M_\chi \]

s.t. \(Z(\mathfrak{g})\) acts on each \(M_\chi\) with a generalized character \(\chi\).

Now let \((\mathfrak{g}, K) – \text{Mod}_\chi\) be the full subcategory of \((\mathfrak{g}, K)\)-modules on which \(Z(\mathfrak{g})\) acts with a generalized character \(\chi\). Cf.[Gaitsgory P42].

**Proof:** \(Z(\mathfrak{g})\) commutes with \(G\) thus \(K\) action, so it preserves each \(M^\rho\), which are of f.d.. \(\square\)

Prop. (15.6.3.13). The category \((\mathfrak{g}, K) – \text{Mod}_\chi\) has only f.m. isomorphism classes of irreducible objects.

**Proof:** Cf.[Gaitsgory]. \(\square\)

Prop. (15.6.3.14). If \(M\) is a f.g. \((\mathfrak{g}, K)\)-module, then for any \(\rho\) of \(K\), \(M^\rho\) is f.g. over \(Z(\mathfrak{g})\).

**Proof:** Cf.[Gaitsgory P43]. \(\square\)

Prop. (15.6.3.15). For \(M \in (\mathfrak{g}, K) – \text{mod}_\chi\), the following are equivalent:

- \(M\) is f.g.
- \(M\) is of finite length.
- \(M\) is admissible.

**Proof:** 2 \(\rightarrow\) 1 is trivial, 1 \(\rightarrow\) 3 is by (15.6.3.14).

For 3 \(\rightarrow\) 2: Use (15.6.3.13), there are only f.m. irreducible classes \(\rho_\alpha\), let \(\rho = \oplus \alpha \rho_\alpha\), then if there is a chain of length \(n\), then there are at least \(n\) linearly independent morphisms in \(\text{Hom}_K(\rho, M)\). Thus \(n\) is bounded, because \(\dim_K \text{Hom}_K(\rho, M)\) is finite because \(M\) is admissible. \(\square\)
15.6. REPRESENTATIONS OF (NON-COMPACT)LIE GROUPS

Cor. (15.6.3.16). The category $(\mathfrak{g}, K) - \text{mod}_\chi$ is Artinian (3.3.2.19).

Cor. (15.6.3.17). Every irreducible $(\mathfrak{g}, K)$-module is admissible.

Proof: Firstly irreducible module are in $(\mathfrak{g}, K) - \text{mod}_\chi$ for some $\chi$, and then use the proposition and (15.6.3.8). □

Cor. (15.6.3.18) [Harish-Chandra Modules]. For a $(\mathfrak{g}, K)$-module, the following conditions are equivalent:

- $M$ is f.g. and admissible.
- $M$ is f.g. and its support over Spec$(Z(\mathfrak{g}))$ is finite.
- $M$ is admissible and its support over Spec$(Z(\mathfrak{g}))$ is finite.
- $M$ is of finite length.

Then such modules are called a Harish-Chandra module.

Proof: 

Real Reductive Groups

Def. (15.6.3.19) [Admissible Representation]. Let $G$ be a connected real reductive group (which is relevant, thus the complex representations of $G$ and $G(\mathbb{R})$ are the same (7.3.6.8)), Let $K \subset G(\mathbb{R})$ be a maximal compact subgroup. Define $V^\infty, V^\rho, V^{K-\text{fin}}$ as in (10.9.4.7) (15.6.1.5).

An admissible representation of $G$ is a representation $V$ that for any f.d. irreducible representation $\rho$ of $K$, $V^\rho$ is of f.d.

Prop. (15.6.3.20). For any $\rho$, $V^\infty \cap V^\rho$ is dense in $V^\rho$.

Proof: 

Cor. (15.6.3.21). If $V$ is admissible, then $V^{K-\text{fin}} \subset V^\infty$ by (15.6.1.9).

Prop. (15.6.3.22). If $V$ is admissible, then $V^{K-\text{fin}}$ is a $(\mathfrak{g}, K)$-module (15.6.3.1), and the map $V \mapsto V^{K-\text{fin}}$ induces a functor $\text{Rep}(G)_{\text{adm}} \to (\mathfrak{g}, K) - \text{mod}_{\text{adm}}$.

And we call two admissible representations $V_1, V_2$ of $G$ infinitesimal equivalent iff they are isomorphic after this functor.

Proof: By (15.6.3.21), $\mathfrak{g}$ can act on $V^{K-\text{fin}}$, and $U(\mathfrak{g})$ fixes $V^{K-\text{fin}}$: if $f \in V^{K-\text{fin}}$, let $R$ be a f.d. $K$-subspace of $V$ containing $f$, then $\mathfrak{f} f \in R$. Let $R_1$ be the f.d. vector space spanned by $\mathfrak{g} R$, then $R_1$ is invariant under $\mathfrak{f}$: for $X \in \mathfrak{f}, Y \in \mathfrak{g}, \varphi \in R$

$$X(Y \varphi) = [X, Y] \varphi + Y(X \varphi) \in R_1$$

so $R_1 \subset V^{K-\text{fin}}$, so $\mathfrak{g}$ fixes $V^{K-\text{fin}}$.

Also we check

$$T_k T_\eta T_k^{-1} = T_{Ad \eta}$$

which is by definition, and the second condition in (15.6.1.9) is also obvious. □
Lemma (15.6.3.23). Let $V$ be an admissible representation of $G$, and $v \in V^{K-f\text{in}}$, then for any $\eta \in V^*$, the function $g \mapsto \eta(g(v))$ is real analytic.

Proof: Cf. [Gaitsgory P37]. □

Prop. (15.6.3.24) [Rep$^{\text{adm}}(G)$ and $(\mathfrak{g}, K)$-Modules].

- If $V_1, V_2$ be two admissible representations of $G$, if $S : V_1 \to V_2$ is a continuous map of TVS. Assume $S(V_1^{K-f\text{in}}) \subset V_2^{K-f\text{in}}$ and induces a $(\mathfrak{g}, K)$-module map, then the initial $S$ is a map of $G$-representations.
- If $V \in \text{Rep}(G)_{\text{adm}}, M = V^{K-f\text{in}}$, then the functions $$(V_1 \subset V) \mapsto (V_1)^{K-f\text{in}} \subset M; \ (M_1 \subset M) \mapsto \overline{M}_1 \subset V$$ induces mutually inverse bijections between closed $G$-subrepresentations of $V$ and $(\mathfrak{g}, K)$-submodules of $M$.

Proof: 1: It suffices to show for $v_1 \in V^{K-f\text{in}}, T_gS(v_1)ST_g(v_1)$. So by Hahn-Banach it suffices to show for any $\eta \in V_2^*$, $$\eta(T_gS(v_1)) = \eta(ST_g(v_1))$$ Both sides are analytic in $g$ by (15.6.3.23), so it suffices to show all their derivatives at 1 are equal, and use the fact $\pi_0(K) \to \pi_0(G)$ is surjective (7.3.6.11). And the derivatives equal because $S$ commutes with $\mathfrak{g}$-action.

2: Firstly $\overline{M}_1$ is a $G$-representation: because $\overline{M}_1 = ((M_1)^{\perp})^{\perp}$ by Hahn-Banach, so it suffices to show for $v_1 \in M_1, \eta(g(v_1)) = 0$ for any $\eta \in (M_1)^{\perp}$. Then this uses analyticity (15.6.3.23) as above and the fact $M_1$ is a $(\mathfrak{g}, K)$-subrepresentation.

For the bijection, notice $V_1^{K-f\text{in}}$ is dense in $V_1$ by (10.9.4.17). Conversely, for a submodule $M_1$, it suffices to show the image of $T_{s_{\mu, \mu}}(\overline{M}_1) \subset M_1^0$ by (10.9.4.13). However $T_{s_{\mu, \mu}}(M_1) \subset M_1^0$ by (10.9.4.13), so this is true by continuity. □

Cor. (15.6.3.25) [Irreducibility of $(\mathfrak{g}, K)$-Modules]. An admissible $G$-representation $V$ is irreducible iff $V^{K-f\text{in}}$ is irreducible as $(\mathfrak{g}, K)$-modules.

Irreducible Admissible $(\mathfrak{g}, K)$-Modules of $GL(2, \mathbb{R})$

Prop. (15.6.3.26) [Lie Theory]. Let $V$ be an irreducible admissible $(\mathfrak{g}, K)$-module for $GL(2, \mathbb{R})^+$, then

- $V^k$ is the space of all vectors $x \in V$ that $Rx = kx$.
- If $x \in V^k$, then $Rx \in V^{k+2}, Lx \in V^{k-2}$.
- If $0 \neq x \in V^k$, then $Cx = V^k, CR^n x = V^{k+2n}, CL^n V^{k-2n}$ and $$V = Cx \oplus \bigoplus_{n>0} CR^n x \oplus \bigoplus_{n>0} CL^n x.$$  
- Suppose $\Delta = \lambda$ on $V$, then if $x \in V^k$, then $$LRx = (-\lambda - k \left(1 + \frac{k}{2}\right))x, \quad RLx = (-\lambda + \frac{k}{2} \left(1 - \frac{k}{2}\right)x.$$
Proof: 1: Let $W = iH$. If $x \in V^k$, then
\[ Wx = \frac{d}{dt} \pi(e^{iW})x = \frac{d}{dt} \pi(k_t)x = \frac{d}{dt} e^{ikt}x = ikx \]
thus $Hx = kx$. And we know $V$ decomposes as direct sums of representations of $K(10.9.4.4)$, thus the result follows.

2: clear from (2.5.2.11).

3: Because the RHS is a $\mathfrak{g}$-submodule, by representation of $\mathfrak{sl}_2(\mathbb{C})(15.15.1.11)$. And it is also a $K$-subrepresentation, by item1.  

4: By (15.15.1.11). \(\square\)

Cor. (15.6.3.27) [Non-Discrete Case]. For any $\lambda, \mu \in \mathbb{C}$ that $\lambda \neq \frac{k}{2}(1 + \frac{1}{2})$ for $k$ even/odd, there exists at most one isomorphism class of irreducible admissible even/odd $(g, K)$-module $V$ on which $\Delta, I$ acts by $\lambda, \mu$ respectively, and the $K$-type is one vector $f_k$ for each $k \in \mathbb{Z}$.

Proof: This follows from the classification of representation of $\mathfrak{sl}_2(\mathbb{C})(15.15.1.11)$. Notice the action of $K$ is controlled by (15.6.3.26) item1. \(\square\)

Cor. (15.6.3.28) [Discrete Case]. Let $k \geq 1$ be an integer and $\lambda = \frac{k}{2}(1 + \frac{1}{2})$. Let $V$ be an irreducible admissible $(g, K)$-module with parity equals $k$, Let $\Sigma$ be the $K$-types of $V$, then $\Sigma$ is one of the following sets:
- $\Sigma^+(k) = \{ l \in \mathbb{Z}| l \equiv k \mod 2, l \geq k \}$
- $\Sigma^-(k) = \{ l \in \mathbb{Z}| l \equiv k \mod 2, l \leq -k \}$
- $\Sigma^0(k) = \{ l \in \mathbb{Z}| l \equiv k \mod 2, -k < l < k \}$
And there are at most one isomorphism class with each $\Sigma$.

Proof: This follows from the classification of representation of $\mathfrak{sl}_2(\mathbb{C})(15.15.1.11)$. Notice the action of $K$ is controlled by (15.6.3.26) item1. \(\square\)

Def. (15.6.3.29) [$H(s_1, s_2, \varepsilon)$]. If $\lambda \geq 1/4$, let $s - 1/2$ be the square root of $1/4 - \lambda$ which is imaginary, and let $s_1, s_2$ be determined that $\mu = s_1 + s_2, s = \frac{1}{2}(s_1 - s_2 + 1)$.

Consider the 1-dimensional representation $\sigma$ of $B(\mathbb{R})^+$ that
\[ \sigma(\begin{bmatrix} y_1 & x \\ y_2 \end{bmatrix}) = \text{sgn}(y_1)^{\varepsilon}|y_1|^{s_1}|y_2|^{s_2}, \]

If $s_1, s_2$ are purely imaginary (i.e. $\mu$ is purely imaginary), then this representation is unitary, and we can consider the induced representation on $GL(2, \mathbb{R})^+(10.9.5.3)$, then it is a unitary representation of $GL(2, \mathbb{R})^+$. For $f \in \text{ind}^G_{B(\mathbb{R})^+}$,
\[ f(\begin{bmatrix} y_1 & x \\ y_2 \end{bmatrix}) = \text{sgn}(y_1)|y_1|^{s_1+1/2}|y_2|^{s_2-1/2} f(g) \]
and
\[ (f_1, f_2) = \frac{1}{2\pi} \int_0^{2\pi} f_1(k_\theta)f_2(k_\theta) d\theta. \]
so $H(s_1, s_2, \varepsilon)$ is identical to $L^2[-\pi/2, \pi/2]$ by Iwasawa decomposition (15.7.1.3). Then its $K$-finite vectors can be determined, which are sums of
\[ f_l(g) = u^{s_1+s_2}y^l e^{il\theta}, l \equiv \varepsilon \mod 2. \]
so \(H(s_1, s_2, \varepsilon)\) is admissible.

Even if \(\mu\) is not purely imaginary, we can still define \(H(s_1, s_2, \varepsilon)\) as above, and we consider its smooth vectors \(H^\infty(s_1, s_2, \varepsilon)\), which are just the smooth functions in \(H(s_1, s_2, \varepsilon)\), by (15.6.1.10).

**Prop. (15.6.3.30).** We can define the regular action of \(G\) on \(H(s_1, s_2, \varepsilon)\) (but may not be unitary), and the subspace \(H^\infty(s_1, s_2, \varepsilon)\) is the space of smooth vectors for this representation.

**Proof:** It suffices to define the regular action of \(G\) on \(H^\infty(s_1, s_2, \varepsilon)\) and show it is a bounded operator, so that it can be extended to \(H(s_1, s_2, \varepsilon)\) by continuity.

By Cartan decomposition (11.6.6.1), \(G\) is generated by \(K\) and diagonal matrices of positive entries. \(\rho(K)\) clearly preserves the inner product, so it suffices to consider these matrices.

By (15.7.2.1) and the calculation \(d\theta' = y_1 y_2 D(\theta)^{-2} d\theta\), we have

\[
\int_0^{2\pi} |\pi(\text{diag}(y_1, y_2)) f(k\theta)|^2 d\theta = (y_1 y_2)^{s_1-1/2} \int_0^{2\pi} D(\theta)^{-s_1+s_2+1} |f(k\theta)|^2 d\theta'.
\]

where

\[\theta' = \arctan\left(\frac{y_1}{y_2} \tan \theta\right), \quad D(\theta) = \sqrt{y_1^2 \sin^2 \theta + y_2^2 \cos^2 \theta}.\]

\(D(\theta)\) is bounded above and below, thus \(\pi(\text{diag}(y_1, y_2))\) is a bounded operator. Also to show this representation is continuous, it suffices to show for \(|f|_2\) small and \(y_1, y_2\) small, \(|\pi(\text{diag}(y_1, y_2)) f|_2\) is small. And this is also a consequence of the above formula. \(\Box\)

**Lemma (15.6.3.31).** For \(f_1 \in H(s_1, s_2, \varepsilon)\) as in (15.6.3.29), we have

\[H f_1 = l f_1, \quad R f_1 = (s + \frac{l}{2}) f_{i+2}, L f_1 = (s - \frac{l}{2}) f_{i-2}, \Delta f_1 = \lambda f_1, \quad I f_1 = \mu f_1\]

**Proof:** Clear from (15.7.1.5) and definition of \(f_1(15.6.3.29)\). \(\Box\)

**Prop. (15.6.3.32) [Existence of \((g, K)\)-Modules].** Let \(s = \frac{1}{2}(s_1 - s_2 + 1), \lambda = s(1 - s), \mu = (s_1 + s_2)\), then (subquotients) of the \((g, K)\)-module \(\mathfrak{S}\) of \(H(s_1, s_2, \varepsilon)\) afford classes in (15.6.3.27) and (15.6.3.28). More precisely, \(\Delta\) and \(I\) acts by scalars \(\lambda, \mu\) respectively, and

- If \(s\) is not of the form \(k/2, k \equiv \varepsilon \mod 2\), then \(\mathfrak{S}\) is irreducible.
- If \(s \geq 1/2\) and \(s = \frac{k}{2}\) where \(k \geq 1\) is an integer that \(k \equiv \varepsilon \mod 2\), then \(\mathfrak{S}\) has two irreducible invariant subspaces \(\mathfrak{S}_+, \mathfrak{S}_-\) with \(K\)-types \(\Sigma_+, \Sigma_-\) respectively, and the quotient \(\mathfrak{S}/\mathfrak{S}_+ \oplus \mathfrak{S}_-\) is irreducible and has \(K\)-type \(\Sigma^0(k)\).
- If \(s \leq 1/2\) and \(s = 1 - \frac{k}{2}\) where \(k \geq 1\) is an integer that \(k \equiv \varepsilon \mod 2\). Then \(\mathfrak{S}\) has an invariant subspace \(\mathfrak{S}_0\) with \(K\)-types \(\Sigma^0(k)\) and the quotient \(\mathfrak{S}/\mathfrak{S}_0\) decomposes into two irreducible invariant subspaces \(\mathfrak{S}_+, \mathfrak{S}_-\) with \(K\)-types \(\Sigma_+, \Sigma_-\) respectively.

**Proof:** The action of \(H, R, L, \Delta, I\) is all clear from (15.6.3.31), and the decomposition and irreducibility is all clear from the representation theory of \(sl_2\) and (15.6.3.27)(15.6.3.28). \(\Box\)

**Prop. (15.6.3.33) [List of Irreducible Admissible \((g, K)\)-Modules for GL(2, R)\(^+\)].** Every irreducible admissible \((g, K)\)-module may be realized as the space of \(K\)-finite vectors in an admissible representation of \(G\) on a Hilbert space. Let \(\lambda, \mu \in \mathbb{C}\), and \(\varepsilon = 0, 1\).

- If \(\lambda\) is not of the form \(\frac{1}{2}(1 - \frac{k}{2})\), where \(k \equiv \varepsilon \mod 2\), then there exists a unique irreducible admissible \((g, K)\)-module of parity \(\varepsilon\) on which \(\Delta, I\) acts by scalars \(\lambda, \mu\), denoted by \(P_\mu(\lambda, \varepsilon)\). These are called the **principal series**.
• If $\lambda = \frac{k}{2}(1 - \frac{k}{2})$ for some $1 \leq k \equiv \varepsilon \mod 2$, then there exists three (two for $k = 1$) irreducible admissible $(g, K)$-module of parity $\varepsilon$ on which $\Delta, I$ acts by scalars $\lambda, \mu$. Their $K$-types are $\Sigma^{\pm}, \Sigma^{0}$ respectively. The irreducible admissible $(g, K)$-modules of $K$-types $\Sigma^{\pm}$ are denoted by $D^{\pm}_{\mu}(k)$. If $k > 1$, $D^{\pm}_{\mu}(k)$ are called discrete series and for $k = 1$ they are called limits of discrete series.

Proof: This is a consequence of (15.6.3.27)(15.6.3.28) and (15.6.3.32).

Prop.(15.6.3.34) [List of Irreducible Admissible $(g, K)$-Modules for $GL(2, \mathbb{R})$]. Let $\mu \in \mathbb{C}$, and $\varepsilon = 0, 1$.

• The f.d. representations are obtained by tensoring the symmetric powers of the standard representation of $G$ with the 1-dimensional representation of the form $\chi \circ \det$.

• If $\chi_{1}, \chi_{2}$ are quasi-characters of $\mathbb{R}^{*}$ that $\chi_{1}\chi_{2}^{-1}$ is not of the form $y \mapsto \sgn(y)^{\varepsilon}|y|^{k-1}$, where $k \equiv \varepsilon \mod 2$, then there is a irreducible $(g, O(2, \mathbb{R}))$-module $\pi(\chi_{1}, \chi_{2})$.

• If $\mu \in \mathbb{R}$ and $k \geq 1$ is an integer, then there are representations $D_{\mu}(k) = (D^{+}_{\mu}(k) \oplus D^{-}_{\mu}(k))$, called discrete series if $k \geq 2$ and limits of discrete series if $k = 1$.

Proof: Use (15.1.1.11) on $SO(2, \mathbb{R}) \subset O(2, \mathbb{R})$. It turns out $P_{\mu}(\lambda, \varepsilon)$ can be extended in two ways to a representation of $O(2, \mathbb{R})$: $H(s_{1}, \varepsilon_{1}, s_{2}, \varepsilon_{2})$, corresponding to item2. It is unitarizable as $H(s_{1}, s_{2}, \varepsilon)$ is unitarizable.

The (limits of) discrete series are conjugate in pairs and combined to give a representation of $O(2, \mathbb{R})$, which is item3. It is unitarizable as it is just $H(s_{1}, s_{2}, \varepsilon)/\mathbb{S}^{0}$.

The case $D^{0}_{\mu}(k)$ are also of type $I$ and can be extended, and this irreducible representation are exactly the smooth parts of the symmetric representation of $GL(2, \mathbb{R})$ twisted by $\chi \circ \det$.

Cor.(15.6.3.35) [Contragradient]. Let $G = GL(2, \mathbb{R}), K = O(2, \mathbb{R}), (\pi, V)$ be an irreducible admissible $(g, K)$-module, then the contragradient $\hat{\pi}$ is isomorphic to the $(g, K)$-module $T'_{k} = T_{k-1}$ and $T'_{X} = T_{X^{-1}}$.

And it is also isomorphic to $\pi \otimes (\omega \circ \det)$.

Proof: This is a consequence of the classification of irreducible $(g, K)$-modules (15.6.3.33), where the $K$-type are unchanged, eigenvalues of $\Delta$ are unchanged, and eigenvalue of $I$ is changed to $-\mu$, so they are isomorphic.

4 Unitary Representations

The theory of abstract harmonic analysis applies in this case 10.9.

Lemma (15.6.4.1) [Auxiliary Compact Supported Function Approximation]. Let $G$ be a locally compact Lie group and $K$ a compact subgroup. If $\mathcal{H}$ is a unitary representation of $G$ on a Hilbert space, and let $f \neq 0 \in \mathcal{H}$, then for any $\varepsilon > 0$, there is a $\varphi \in C_{c}^{\infty}(G)$ s.t. $\pi(\varphi)$ is self-adjoint and $|\varphi(\rho)f - f| < \varepsilon$.

Moreover, if $f \in \mathcal{H}^{k}$ which is the decomposition part for $K$, we can assume $\varphi(kg) = \varphi(gk) = \xi(k)^{-1}\varphi(g)$. In particular if $\mathcal{H}^{k}$ is f.d., we find a $\varphi$ that $\pi(\varphi)f = f$.

Proof: By continuity, there is a nbhd $H$ of 1 that $|\pi(g)f - f| < \varepsilon$, then we can choose a $\varphi$ positive real valued with support in $U$ with integral 1, then $|\pi(\varphi)f - f| < \varepsilon$ by (10.7.3.22). We can also choose $\varphi(g) = \varphi(g^{-1})$, then $\pi(\varphi)$ is self-adjoint.
For the second case, notice first there is a nbhd $V$ of 1 that $kVk^{-1} \in U$ for any $k \in K(3.8.1.6)$, so let $\varphi_1$ be a positive real valued function supported in $V$, and let

$$\varphi_0(g) = \int_K \varphi_1(kgk^{-1})dk$$

then $\varphi_0$ is supported in $U$ and $\varphi(kgk^{-1}) = \varphi_0(g)$ for any $k \in K$. Assume now that $\pi(k\theta) = e^{ik\theta}f$, then we can use (10.9.1.39) for $P = G$ to see that

$$\pi(\varphi_0)f = \int_G \varphi_0(h)\pi(h)f dh = \int_G \int_K \varphi_0(hk)\pi(hk)f dk dh = \int_G \int_K \xi(k)\varphi_0(hk)\pi(h)f dh = \pi(\varphi)f$$

where

$$\varphi(g) = \int_K \xi(k)\varphi_0(gk)dk = \int_K \xi(k)\varphi_0(kg)dk$$

so $\varphi(k) = \varphi(gk) = \xi^{-1}(k)\varphi(g)$ as required. □

**Unitary Irreducible Representation is Admissible**

$G$ appearing in this subsection are assumed to be a Lie group.

**Prop.(15.6.4.2).** If $V$ is an irreducible unitary representation of $G$, then the image of the induced action of $Meas_c(G)$ is dense in $\text{End}(V)$ in the strong topology (10.6.3.4).

**Proof:** This follows immediately from the von Neumann theorem (10.8.3.14) and Schur’s lemma (10.9.2.4): if we denote the algebra generated by $Meas_c(G)$ by $A$, then

$$\overline{A} = (A^c)^c = (C)^c = \text{End}(V).$$

□

**Prop.(15.6.4.3).** If $V$ is a representation of $G$ that the image of the induced action of $Meas_c(G)$ is dense in $\text{End}(V)$ in the strong topology, then

$$\dim(V^\rho) \leq \dim(\rho)^2.$$ 

**Proof:** Follows directly from the following two lemmas (15.6.4.5)(15.6.4.6). □

**Cor.(15.6.4.4)[Irreducible Unitary Representation is Admissible].** For any irreducible unitary representation of $G$, the $K$-finite part is an irreducible admissible $(g, K)$-module, and $\dim(V^\rho) \leq \dim(\rho)^2$.

**Proof:** Follows directly from (15.6.3.25), (15.6.4.2) and (15.6.4.3). □

**Lemma(15.6.4.5).** For any $\rho \in \text{Irrep}(K)$, let $A_\rho = \xi_\rho \cdot Meas_c(G) \cdot \xi_\rho$, this is an algebra that acts on $V^\rho$ by (10.9.4.13). Then there exists a family of f.d. representations $\pi$ of $A_\rho$ that:

- Each $\pi$ is of dimension $\leq n = \dim(\rho)^2$.
- For every element $a \in A_\rho$, there exists a $\pi$ that $\pi(a)$ is non-trivial.

**Proof:** Consider the set of all irreducible f.d. representations of $G$, and $\pi^\rho$ their $\rho$-isotopic parts. Then these are representations of $A_\rho$, and for any $\varphi \in Meas_c(G)$, there is a $\pi$ that $T_\varphi \neq \text{Id}$, and each $\pi^\rho$ has dimension $\leq \dim(\rho)^2$. Cf.[Gaitsgory P46]. □
Lemma (15.6.4.6). If $A$ is an associative algebra equipped with a family of f.d. modules satisfying conditions in (15.6.4.5), then if $V$ is a representation of $A$ that the image of $A$ is dense in $\text{End}(V)$ in the strong topology, then $\dim V \leq n$.

Proof: For an associated algebra $A$, consider the minimal integer $r$ that the property $P(r):$

$$\sum_{\sigma \in \Sigma_r} \text{sgn}(\sigma)a_{\sigma(1)} \cdots a_{\sigma(r)} = 0$$

for any $a_1, \ldots, a_r$, then Amitsur-Levitski showed that for $A = GL(n, \mathbb{C})$, $r = 2n(2.5.11.7)$.

Now the condition of $A$ in (15.6.4.5) shows that $P_{2n}$ is true for $A$. If $\dim V \geq n + 1$, then the image of $A$ satisfies $P(2n)$, so also $\text{End}(V)$ satisfies $P(2n)$ because $A$ is dense in $\text{End}(V)$. But $V$ contains a subgroup $GL(n + 1, \mathbb{C})$, so it cannot satisfy $P(2n)$ by (2.5.11.7), contradiction. □

Cor. (15.6.4.7). Let $V$ be an irreducible unitary representation of $G$, then for any $\rho \in \text{Irrep}(K)$,

$$\dim(V^\rho) \leq \dim(\rho)^2.$$ 

In particular, every unitary irreducible representation of $G$ is admissible.

Proof: Directly from Lemmas (15.6.4.2) and (15.6.4.3) above, as the action of $A_\rho$ on $V^\rho$ is also have dense image in the strong topology. □

Prop. (15.6.4.8). If $M$ is an irreducible $(g, K)$-module equipped with an invariant inner product $((km_1, km_2) = (m_1, m_2), (\xi m_1, m_2) + (m_1, \xi m_2) = 0)$, then the Hilbert space completion of $M$ carries a unique unitary $G$-representation s.t. $V^{K-fin} = M$ as $(g, K)$-modules.

Proof: By (15.6.4.9), the Hermitian form can be extended continuously to the Banach space completion of $M$. It suffices to prove the extended Hermitian form is continuous, because then we can choose its completion w.r.t. $(-, -)$.

For the invariance, consider $f(g) = (gm_1, m_2) - (m_1, g^{-1}m_2)$, then notice $(a, -)$ are continuous functional on $V$, thus by (15.6.3.23) and similar analytic method as in (15.6.3.24) using the invariance of inner product. □

Lemma (15.6.4.9). Situation as in (15.6.4.8), $M$ has a Banach norm that $(m, m) \leq ||m||^2$.

Proof: (15.6.3.11) shows $M$ does have a Banach norm. Then let $M \cong V^{K-fin}$ and $M^{*\text{alg}} \cong (V^*)^{K-fin}$. However the Hermitian form induces $M \cong M^{*\text{alg}}$, thus we can form

$$M \overset{\Delta}{\to} M \oplus M \to V \oplus V^*$$

let $V'$ be the closure of the image of $M$, then it is a $G$-representation by (15.6.3.24), and then

$$(m, m) \leq ||i_1(m)||||i_2(m)|| \leq (||i_1(m)|| + ||i_2(m)||)^2.$$ 

Cor. (15.6.4.10). The above proposition (15.6.4.8) is true for $M$ admissible.
Hecke Algebras

Prop.(15.6.4.11)[Hecke Algebras of Lie Groups].

- If \( K \) is a compact Lie group, then the Hecke algebra \( \mathcal{H}_K \) is defined to be the ring of smooth functions on \( K \) that is \( K \)-finite under both left and right translations, where the algebra is given by convolution. By Peter-Weyl theorem, these functions are dense in \( C(K) \) and \( L^2(K) \), and it is an idempotented algebra over \( \mathbb{C} \)? Cf.[Bump, P309].

- If \( G \) is a real reductive group and \( K \) is a maximal compact subgroup, then the Hecke algebra \( \mathcal{H}_G \) is defined to be \( \mathcal{H}_G = \mathcal{H}_K \otimes_{U(k)} U(g) \), where the right action of \( U(k) \) on \( \mathcal{H}_K \) is given by \( f \ast D = \rho(D)f \), ? Cf.[Bump, P312].

Proof: □

Prop.(15.6.4.12)[Equivalence of Representations Lie Group Case].

- For a compact Lie group \( K \), the category \( \mathcal{M}(K) \) of smooth representations of \( \mathcal{H}_K \) is equivalent to the category of unitary representations of \( K \).

- For a real reductive group \( G \) and a maximal compact subgroup \( K \), the category of (admissible)(\( g, K \))-modules is equivalent to the category of smooth(admissible) modules of \( \mathcal{H}_G \).

Proof: Cf.[Cohomological Induction and Unitary Representations, P75]. □

Irreducible Unitary Representations of \( GL(2, \mathbb{R})^+ \)

Lemma(15.6.4.13)[Finite Dimensional Case]. The only irreducible f.d. unitary representations of the group \( GL(n, \mathbb{R})^+ \) are the 1-dimensional characters \( g \mapsto \det(g)^r \) where \( r \) is purely imaginary.

Proof: Such a representation defines a continuous map of \( GL(n, \mathbb{R})^+ \) into the compact unitary group \( U(n) \). Now it induces a Lie algebra map \( \mathfrak{sl}_n(\mathbb{R}) \to \mathfrak{u}_m \). This map must be trivial because otherwise this is an embedding because \( \mathfrak{sl}_n(\mathbb{R}) \) is simple. But this is impossible because the adjoint action of \( \mathfrak{sl}_n(\mathbb{R}) \) has real eigenvalues but the adjoint action of \( \mathfrak{u}_m \) are all purely imaginary by(2.5.5.4). So the action is trivial on \( SL(n, \mathbb{R})^+ \), so induces an irreducible representation of \( \det(g) \), which is clearly 1-dimensional. □

Lemma(15.6.4.14). Because for a unitary representation \( \mathcal{H} \) of \( G \), for \( X \in \mathfrak{g} \), we have \( (Xu,v) = -(u,Xv) \),

so \( (Xv,w) = -(v,X\overline{w}) \) when complexified. So

\[ (Rv,w) = -(v,Lw) \]

for any \( v, w \in \mathcal{H} \), by(15.7.1.1).

Lemma(15.6.4.15)[Principal Series]. For the principal series \( P_\mu(\lambda, \varepsilon) \) of \( GL(2, \mathbb{R})^+ \), there exists an irreducible unitary representation in this class if \( \mu \) is purely imaginary and \( \lambda \geq 1/4 \) real.

Proof: Consider the unitary representation \( H(s_1, s_2, \varepsilon) \) defined in(15.6.3.29), then it is irreducible and its class is \( P_\mu(\lambda, \varepsilon) \) by(15.6.3.32) and(15.6.3.25). □
Lemma (15.6.4.16) [Possibilities of Unitary Representations]. Let $\mathcal{H}$ be a unitary representation of $GL(2, \mathbb{R})^*$. Assume $\Delta, I$ acts by scalars $\lambda, \mu$ respectively, then

- $\mu$ is purely imaginary and $\lambda$ is real.
- If the $(g, K)$-module type of $\mathcal{H}$ is a principal series $P_\mu(\lambda, \epsilon)$, then $\lambda > 0$, and if $\epsilon = 1$, $\lambda > 1/4$.

Proof: 1: This follows from (15.6.4.14), as action of $I$ is skew-symmetric and action of $\Delta$ is symmetric.

2: By (15.6.3.27), $V^k \neq 0$ for $k \equiv \epsilon \mod 2$, let $f_k \in V^k$. Because $-4\Delta - H^2 + 2H = 4RL(15.7.1.1)$, take $k = \epsilon$, then

\[
(-4\lambda - \epsilon^2 + 2\epsilon)f_\epsilon = 4RLf_\epsilon.
\]

But by (15.6.4.14),

\[
(4RLf_\epsilon, f_\epsilon) = -4(Lf_\epsilon, Lf_\epsilon) < 0
\]

thus $4\lambda > 2\epsilon - \epsilon^2$. \qed

Cor. (15.6.4.17) [Reduction of $\mu$]. The infinitesimal equivalence class of representations $P_\mu(\lambda, \epsilon)$ or $D_\mu^\pm(k)$ contains an irreducible unitary representation iff $\mu$ is purely imaginary and the corresponding class $P(\lambda, \epsilon)$ or $D^\pm(k)$ contains an irreducible unitary representation.

Proof: $\mu$ must be purely imaginary by the proposition. And we may tensoring a unitary representation by a deg$(g)^r$, it is also unitary iff $r$ is purely imaginary, and this increases the value of action of $I$ by $2r$ and doesn't affect $\mu$ and $\epsilon$ because $\Delta$ has nothing to do with $u(15.7.1.5)$. \qed

Prop. (15.6.4.18) [Intertwining Integral]. Let $s = \frac{1}{2}(s_1 - s_2 + 1)$, define for $f \in V$,

\[
M(s) : H^{\infty}(s_1, s_2, \varepsilon) \to H^{\infty}(s_2, s_1, \varepsilon) : (M(s)f)(g) = \int_{f(F)} f(w_0^u g) du.
\]

Then if $\text{Re}(s_1 - s_2) > 0$, the integral is absolutely convergent, and commutes with the action of $G$.

Proof: Replacing $f$ with $\rho(h)f$, we see that the convergence of $M(s)(f)(h)$ is equivalent to the convergence of $M(s)(\rho(h)f)$, so we assume $h = 1$.

We use the identity

\[
\begin{bmatrix}
1 & -1 \\
1 & 1
\end{bmatrix}
\begin{bmatrix}
1 & x \\
1 & 1
\end{bmatrix}
= \begin{bmatrix}
\Delta_x^{-1} & -x\Delta_x^{-1} \\
-x\Delta_x & \Delta_x
\end{bmatrix} k_{\theta(x)}
\]

similar to (15.7.2.1) where

\[
\Delta_x = \sqrt{1 + x^2}, \quad \theta(x) = \arctan(-1/x).
\]

Then

\[
(M(s)f)(1) = \int_{-\infty}^{\infty} (1 + x^2)^{-s} f(k_{\theta(x)}) dx
\]

which convergences for $s > 1/2$, that is $\text{Re}(s_1 - s_2) > 0$.

To show $M(s)f \in H(s_2, s_1, \varepsilon)$, we check

\[
(M(s)f)(\begin{bmatrix}
y_1 \\
y_2
\end{bmatrix} g) = (M(s)f)(g), \quad (M(s)f)(\begin{bmatrix}
y_1 \\
y_2
\end{bmatrix} g) = \text{sgn}(y_1)^{\varepsilon}|y_1|^{s_2 + \frac{1}{2}}|y_2|^{s_1 - \frac{1}{2}}(M(s)f)(g).
\]
The first one is an easy consequence of change of variable, for the second,

\[
(M(s)f)([y_1 \\ y_2]) = \int f([y_1 \\ y_2]) dx
\]

\[
= \int f([y_1 \\ y_2]) dx
\]

\[
= \frac{y_1}{y_2} \int f([y_1 \\ y_2]) dx
\]

\[
= \frac{y_1}{y_2} \int f([y_1 \\ y_2]) dx
\]

\[
= \frac{y_1}{y_2} \text{sgn}(y_1)^{y_1/2} |y_2|^{s_1 - 1/2} \left( 1 - |y_2|^{s_1 - 1/2} (M(s)f)(g) \right)
\]

To check \( M(s)f \) is smooth, notice that the restriction of \( M(s)f \) to \( K \) equals

\[
(M(s)f)(k_t) = \int_{-\infty}^{\infty} (1 + x^2)^{-s} f(k_{\theta(x)+t}) dx.
\]

The convergence is uniform in \( t \), thus is smooth in \( t \).

The commutativity of \( M(s) \) with \( G \)-action is immediate, because left and right action commutes.

\( \square \)

**Prop. (15.6.4.19).** Let \( f_{k,s} \) be the function \( f_k \) in \( H(s_1, s_2, \varepsilon) (15.6.3.29) \) where \( \text{Re}(s_1 - s_2) > 0 \) and \( s = \frac{1}{2}(s_1 - s_2 + 1) \), then

\[
M(s)f_{k,s} = (-i)^k \sqrt{\pi} \frac{\Gamma(s) \Gamma(s - \frac{1}{2})}{\Gamma(s + \frac{k}{2}) \Gamma(s - \frac{k}{2})} f_{k,1-s}
\]

**Proof:** Because \( M(s) \) commutes with \( G \)-action, \( M(s)f_{k,s} \) is a multiple of \( f_{k,1-s} \), thus it suffices to calculate \( (M(s)f_{k,s})(1) \), which is

\[
(M(s)f)(1) = \int_{-\infty}^{\infty} (1 + x^2)^{-s} e^{ik\theta(x)} dx, \quad \theta(x) = \arctan(-1/x)
\]

by (15.6.4.18).

This integral then is calculated to be the expression above, by (10.4.8.1). \( \square \)

**Lemma (15.6.4.20) [Complementary Series].** For \( \mu \) purely imaginary and \( 0 < \lambda < 1/4 \) and \( \varepsilon = 0 \), there exists an irreducible unitary representation in this class of the \((g, K)\)-module \( P_\mu(\lambda, 0) \).

**Proof:** Let \( s_1, s_2 \) be complex numbers, we construct first a Hermitian pairing

\[
H(s_1, s_2, \varepsilon)_{\text{fin}} \times H(-s_1, -s_2, \varepsilon)_{\text{fin}} \to \mathbb{C} : (f, g') \mapsto \int_K f(k)\overline{g'(k)} dk
\]

which is invariant under action of \( G \) by (10.9.1.45). Now let \( s_2 = -s_1 \), then \( s = \frac{1}{2}(s_1 - s_2 + 1) \) is real and \( \mu = s_1 + s_2 \) is purely imaginary. Then composing this pairing with \( i^\varepsilon M(s) : H(s_1, s_2, \varepsilon)_{\text{fin}} \to H(s_2, s_1, \varepsilon)_{\text{fin}} = H(-s_1, -s_2, \varepsilon)_{\text{fin}} \), then

\[
(f, f') = \int_K f(k)i^\varepsilon M(s)f'(k) dk.
\]
is $G$-invariant. We will show that it is positive definite if $\epsilon = 0$ and $1/2 < s < 1$.

It can be seen from (15.6.4.19) that an orthogonal basis for $H(s_1, s_2, 0)_{fin}$ under this pairing is $f_{k,s}$ for $k$ even. And by (15.6.4.19),

$$(f_{k,s}, f_{k,s}) = (-1)^{k/2} \sqrt{\pi} \frac{\Gamma(s)\Gamma(s - \frac{1}{2})}{\Gamma(s + \frac{k}{2})\Gamma(s - \frac{k}{2})}$$

which is positive for $1/2 < s < 1$. Now we obtain a unitary representation of $G$ on the Hilbert completion of this space (10.9.2.8).

Now we have constructed a unitary representation in the infinitesimal equivalence class $P_\mu(\lambda, 0)$ with $\lambda = s(1 - s)$, $s = \frac{1}{2}(s_1 - s_1 + 1)$, so any $0 < \lambda < 1/4$ is possible. \hfill $\Box$

Lemma (15.6.4.21). For any integer $k$, there is a bijection between holomorphic functions $\varphi$ on $H$ and smooth functions $\Phi$ on $GL(2, \mathbb{R})^+$ that is invariant under $Z(R)^+$ and

$$\Phi(gk_0) = e^{ik\theta} \Phi(g), \quad L \Phi = 0.$$  

**Proof:** The bijection is given by

$$\varphi(z) = y^{-k/2} \Phi \left( \begin{bmatrix} y & 1 \\ x & 1 \end{bmatrix} \right), \quad \Phi(g) = ((y^{k/2} \varphi)[g]_k)i.$$  

and the proof is a combination of formal calculation in (15.7.3.9) and (15.7.1.24) forgetting $\Gamma$:

$$L_k(y^{k/2} f(z)) = -(z - \bar{z}) \frac{\partial}{\partial z} - \frac{k}{2} (y^{k/2} f(z)) = -2iy^{(k+2)/2} \frac{\partial}{\partial z} f(z).$$  

\hfill $\Box$

Lemma (15.6.4.22) [Discrete Series]. If $k > 1$, then there exists a unitary representation in the infinitesimal equivalence class $D^+(k)$, more precisely,

- Let $L^2(H, \mu_k)$ be the $L^2$-space of holomorphic functions $f$ on the upper plane $H$ w.r.t the measure $\mu_k = y^k \frac{dx dy}{y^2}$. Then the left action

$$\pi_k(g)f = f[g^{-1}]_k.$$  

of $G$ is unitary and this representation $\pi_k$ is in the infinitesimal equivalence class $D^-(k)$.

- Consider the automorphic of $GL(2, \mathbb{R})^+$:

$$\iota \left( \begin{bmatrix} a & b \\ c & d \end{bmatrix} \right) = \begin{bmatrix} a & -b \\ -c & d \end{bmatrix}.$$  

then the representation $\pi_k \circ \iota$ is in the infinitesimal equivalence class $D^+(k)$.

**Proof:** The second one follows from the first one, as $\iota$ interchanges the action of $K$ thus the $K$-types.

For the first one, firstly it is a unitary representation: for $z' = g(z) = x' + iy'$, we have

$$y' = \frac{ad - bc}{cz + d} y.$$
and $\mu_z = \mu_{z'}$, thus
\[
||\pi(g^{-1})f||^2 = \int_{\mathcal{H}} |f(z')|^2 \frac{(ad-bc)^k}{|cz+d|^{2k}} \mu_z = \int_{\mathcal{H}} |f(z')|^2 (y')^k \mu_{z'} = ||f||^2.
\]

For the infinitesimal equivalence class, we consider the orthogonal basis $\varphi_n = \left(\frac{z-i}{z+i}\right)^n \left(\frac{2i}{z+i}\right)^k$ and prove
\[
\pi(k^{-1}) \varphi_n = e^{2\pi i (k+2n)\theta} \varphi_n.
\]

Then this will determine the $K$-type of $\pi_k$. This can be proven by direct calculation, Cf.[Ngo, P39].

**Cor. (15.6.4.23)** By (15.6.4.21) and the measure $\mu_k$ we choose, it is clear that there is an isometry between $L^2(\mathcal{H}, \mu_k)$ and a subspace of $L^2(G/Z)$ that is compatible with the left $G$ action on $L^2(G)$, but the left and right action on $L^2(G/Z)$ is isomorphic, as $f(t) \mapsto f(t^{-1})$ intertwine them, because $G/Z$ is unimodular. So this representation is **square integrable**, i.e. it can be embedded in $L^2(G/Z)$.

**Lemma (15.6.4.24) [Limits of Discrete Series]**. There exists a unitary representation in the infinitesimal equivalence class $D^\pm(1)$.

**Proof:** These two classes already appear in the unitary representation $H(0,0,1)$, by (15.6.3.32). \hfill \Box

**Prop. (15.6.4.25) [List of Irreducible Unitary Representations of $GL(2, \mathbb{R})^+$]**. Let $\mu$ be purely imaginary,

- The 1-dimensional representation $g \mapsto |\deg(g)|^\mu$.
- The unitary principal series $P_\mu(\lambda, \varepsilon)$, where $\varepsilon = 0, 1$ and $\lambda \geq 1/4$.
- The complementary series representations $P_\mu(\lambda, 0)$ where $0 < \lambda < 1/4$.
- The holomorphic discrete series $D_\mu^0(k)(k \geq 2)$ and limits of discrete series ($k = 1$) $D_\mu^1(k)$.

Notice each of these infinitesimal equivalence classes of irreducible representations has a unique representative that is a unitary representation by (15.6.3.10).

**Proof:** By (15.6.3.25) and (15.6.3.10), the conclusion follows from the classification of $(\mathfrak{g}, K)$-modules (15.6.3.33) and determining which infinitesimal class has a unitary representative, which follows from (15.6.4.13) (15.6.4.16), (15.6.4.15) (15.6.4.17), (15.6.4.20) (15.6.4.22), (15.6.4.24). \hfill \Box

**Cor. (15.6.4.26)**. Similar as in (15.6.3.34), by (15.6.3.25), we can classify all irreducible unitary representations of $GL(2, \mathbb{R})$. 

15.7 Automorphic Representations of GL($n$) over Archimedean Local Fields

Main References are [Bum98], [Bor97], [Automorphic Forms and L-Functions for the Group $GL(n, \mathbb{R})$] and [A Course given by Liang Xiao]. Notice that [?] has many gaps, and these gaps can be filled by [Bor97].

1 Setsups

Def.(15.7.1.1) [General Notations]. Let $F = \mathbb{R}$ or $\mathbb{C}$,

$\mathcal{H}$ is the Poincaré’s upper plane with measure $y^{-2}dxdy$, which is left-$GL(2, \mathbb{R})^+$-invariant.

$G = GL(n, F)^+, G_1 = SL(n, F), K = SO(n, F)$, $B$ the upper triangular matrices, $N(F)$ the group of unipotent upper triangular matrices in $G$, $T$ the group of diagonal matrices, $Z(F)$ the group of scalar matrices.

Then $G$ acts on $\mathcal{H}$ through linear fractional transformation and fixes the measure. We will denote $a, b, c, d$ the linear functionals on $M(2, \mathbb{R})$ for $\gamma \in M(2, \mathbb{R})$,

$\gamma = \begin{bmatrix} a(\gamma) & b(\gamma) \\ c(\gamma) & d(\gamma) \end{bmatrix}$.

We will consider right regular action $\rho$ of $G$ on $C^\infty(G)$, and also the left regular action $\lambda$. We will write $dX$ for $X \in \mathfrak{g}$ as the representation of Lie algebra of $G$ via $\rho$, then it commutes with $\lambda$. So it induces a map of $U(\mathfrak{g})$ to the ring of left $G$-invariant differential operators on $G$.

Also we will use the Lie algebra notations (2.5.2.11):

$H = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$, $R = \frac{1}{2} \begin{bmatrix} 1 & i \\ i & -1 \end{bmatrix}$, $L = \frac{1}{2} \begin{bmatrix} 1 & -i \\ -i & -1 \end{bmatrix}$, $W = \begin{bmatrix} 0 & 1 \\ -1 & 0 \end{bmatrix} = iH$.

and the Casimir element in $Z = Z(U(\mathfrak{g}))$:

$\Delta = -\frac{1}{4}(H^2 + 2RL + 2LR)$.

Fix a character $\psi$ of $F$, we define a character $\psi_N$ on $N(F)$ by

$\varphi_N(u) = \psi(\sum_{i=1}^{n-1} u_{i,i+1})$.

Prop.(15.7.1.2) [Classification of Transformations]. Let $\alpha \in SL(2, \mathbb{R})$ and $\alpha \neq I$, then by Jordan decomposition, $\alpha$ is conjugate to one of the matrix of the two following types:

$\begin{bmatrix} \lambda & 1 \\ \lambda & \lambda \end{bmatrix}$, $\begin{bmatrix} \lambda \\ \mu \end{bmatrix}$, $\lambda \neq \mu$

according as it has repeated eigenvalues or distinct eigenvalues. In the first case, $\alpha$ is called parabolic, and in the second case, if $|\lambda/\mu| = 1$, it is called elliptic. If $\lambda/\mu$ is real and positive, it is called parabolic, and called loxodromic otherwise.

- If $\alpha \in SL_2(\mathbb{R})$ is parabolic, then it has a unique real eigenvector, which means it has a unique fixed point in $\mathbb{R} \cup \infty$.
• If $\alpha \in SL_2(\mathbb{R})$ is elliptic, then $\alpha$ has two conjugate eigenvectors, which means it has exactly one fixed point $z$ in $\mathcal{H}$, and a second fixed point, namely $\overline{z}$, in the lower half plane.

• If $\alpha \in SL_2(\mathbb{R})$ is hyperbolic, then it has two real eigenvectors, which means it has two distinct fixed points in $\mathbb{R} \cup \infty$.

**Prop. (15.7.1.3) [Iwasawa-Decomposition].** Every element of $G$ has a unique representation of the form (11.6.6.4):

$$g = \begin{bmatrix} u & y \end{bmatrix} \begin{bmatrix} y^{1/2} & x y^{-1/2} \\ y^{-1/2} & 1 \end{bmatrix} k_\theta$$

where $k_\theta = \begin{bmatrix} \cos \theta & \sin \theta \\ -\sin \theta & \cos \theta \end{bmatrix}$. So by (10.9.1.39) and (10.9.1.19) the Haar measure is calculated to be $dg = \frac{1}{2\pi} \frac{du}{u} \frac{dy}{y^2} d\theta$, and it is unimodular by (10.9.1.22). (Notice the upper triangular matrix group $B \subset GL(2, \mathbb{R})^+$ is not unimodular).

**Proof:** For the calculation of Haar measure, notice that it suffices to calculate for $u, x, y$ and it is

$$
\frac{d(uy^{1/2})d(uy^{-1/2})d(uxy^{-1/2})}{(uy^{1/2})^2 y^{-1/2}} = \frac{dx d(uy^{1/2})d(uy^{-1/2})}{x^2 y} = \frac{dxdydu}{uy^2}.
$$

**Cor. (15.7.1.4).** Every element of $G_1$ has a unique representation of the form

$$g = \begin{bmatrix} e^\frac{2i\theta}{2} & 0 \\ 0 & e^{-\frac{2i\theta}{2}} \end{bmatrix} \begin{bmatrix} 1 \\ x \end{bmatrix} k_\theta.$$

And the Haar measure is given by $dg = \frac{1}{2\pi} du dx d\theta$ by similar calculation, which is unimodular.

**Prop. (15.7.1.5).** In the coordinate (15.7.1.3), we have the following equation:

$$dR = e^{2i\theta} (iy \frac{\partial}{\partial x} + y \frac{\partial}{\partial y} + \frac{1}{2i} \frac{\partial}{\partial \theta}), \quad dL = e^{-2i\theta} (-iy \frac{\partial}{\partial x} + y \frac{\partial}{\partial y} - \frac{1}{2i} \frac{\partial}{\partial \theta}), \quad dH = -i \frac{\partial}{\partial \theta}.$$

So in particular

$$\Delta = d\Delta = -y^2 (\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2}) + y \frac{\partial^2}{\partial x \partial \theta}.$$

**Proof:** $H = -iW$, and $\exp(tW) = k_t = \begin{bmatrix} \cos t & \sin t \\ -\sin t & \cos t \end{bmatrix},$ so $dW = \partial / \partial \theta$ is clear.

For $dR$, first notice that

$$k_\theta \exp(tR) = \exp(e^{2i\theta} R)k_\theta,$$

as

$$k_\theta \exp(tR)k_{-\theta} = C^{-1} \begin{bmatrix} e^{i\theta} & e^{-i\theta} \\ e^{i\theta} & e^{-i\theta} \end{bmatrix} \exp(te^{-i\theta} e^{i\theta}) C = C^{-1} \begin{bmatrix} e^{i\theta} & e^{-i\theta} \\ e^{i\theta} & e^{-i\theta} \end{bmatrix} \begin{bmatrix} 1 & t \\ 1 & 1 \end{bmatrix} C = C^{-1} \begin{bmatrix} 1 & e^{2i\theta} t \\ 1 & 1 \end{bmatrix} C.$$
where \( C \) is the Cayley transformation, notation as in (2.5.2.11).

Now
\[
(dRf)(g) = \frac{d}{dt} f(bk_\theta \exp(tR)) = \frac{d}{dt} f(b \exp(e^{2i\theta} tR)k_\theta) = e^{2i\theta} \frac{d}{dt} f(b \exp(tR)k_\theta)
\]

Then notice
\[
R = 1/2H + \begin{bmatrix} 0 & i \\ 0 & 0 \end{bmatrix} + 1/2 \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \exp(tR) \sim k_{t/2} + \begin{bmatrix} 1 & it \\ i & 1 \end{bmatrix} + \begin{bmatrix} e^{t/2} & 0 \\ 0 & e^{-t/2} \end{bmatrix}
\]

so we get the desired result.

For \( dL \) the calculation is similar to that of \( dR \).

**Def. (15.7.1.6) [\( \Gamma \) Setting].** Let \( \Gamma \) be a discrete subgroup of \( G \) that the volume of \( \Gamma \backslash \mathcal{H} \) is finite, we may also assume that \(-1 \in \Gamma \subset SL(2, \mathbb{R})\).

Let \( \chi \) be a character of \( \Gamma, \omega \) be a character of the center \( Z(\mathbb{R}) \subset G \) (the scalar matrices). Assume that \( \omega(-1) = \chi(-1) \).

**Def. (15.7.1.7) [Cusps].** A cusp of \( \Gamma \) is a point in \( \mathbb{P}^1(\mathbb{R}) \) whose stabilizer in \( \Gamma \) contains a non-trivial parabolic element (15.7.1.2).

Let \( \infty \) be a cusp, then \( \{ \pm 1 \} \Gamma_\infty = \{ \pm 1 \} \langle \begin{bmatrix} 1 & r \\ 0 & 1 \end{bmatrix} \rangle \) for some \( r > 1 \). Then if \( \Gamma_\infty = \langle - \begin{bmatrix} 1 & r \\ 0 & 1 \end{bmatrix} \rangle \), then it is called an irreducible cusp, otherwise it is called a regular cusp. Similarly, for any other cusp \( a = \xi(\infty) \), where \( \xi \in SL(2, \mathbb{R}) \), we called \( a \) is regular/irregular cusp if \( \infty \) is regular/irregular cusp w.r.t. \( \Gamma' = \xi^{-1}\Gamma \xi \).

**Def. (15.7.1.8) [Form Spaces].** Let \( C^\infty(\Gamma \backslash G, \chi, \omega) \) be the space of smooth functions \( F : G \rightarrow \mathbb{C} \) that
\[
F(\gamma g) = \chi(\gamma) F(g), \quad \gamma \in \Gamma, g \in G,
\]
\[
F(zg) = \omega(z) F(g), \quad z \in Z(\mathbb{R}), g \in G.
\]

Let the subspace \( C^c_\infty(\Gamma \backslash G, \chi, \omega) \) be those functions \( f \) that \( |f| \) is compactly supported in \( G \). Similarly we define \( C(\Gamma \backslash G, \chi, \omega) \) and \( C_c(\Gamma \backslash G, \chi, \omega) \).

Define \( C(\Gamma \backslash G, \chi, k) \) or \( C_c(\Gamma \backslash G, \chi, k) \) to be the subspace of \( C(\Gamma \backslash G, \chi) \) or \( C_c(\Gamma \backslash G, \chi) \) consisting of functions \( F \) s.t. \( \rho(k_\theta)F = e^{ik_\theta} F \).

When \( \omega \) is the character of \( Z(\mathbb{R}) \) that \( \omega(Z(\mathbb{R}^+)) = 1 \), then we denote \( C^\infty(\Gamma \backslash G, \chi) = C^\infty(\Gamma \backslash G, \chi, \omega) \).

**Def. (15.7.1.9) [Archimedean Automorphic Forms].** Let the space of automorphic forms \( \mathcal{A}(\Gamma \backslash G, \chi, \omega) \) be the subspace of \( C^\infty(\Gamma \backslash G, \chi, \omega) \) consisting of \( K \)-finite and \( \mathcal{Z} \)-finite functions satisfies the condition of moderate growth:
\[
|F(g)| < C ||g||^N
\]
for some \( C, N > 0 \), where the height on \( G \) is induced from the inclusion
\[
G \rightarrow M(n, \mathbb{R}) \times M(n, \mathbb{R}) : g \mapsto (g, g^{-1}).
\]

When \( \omega \) is trivial on \( Z^+(\mathbb{R}) \), let \( \mathcal{A}(\Gamma \backslash G, \chi, k) \) be the subspace of \( \mathcal{A}(\Gamma \backslash G, \chi) \) consisting of functions \( f \) that \( \rho(k_\theta)(f) = e^{ik_\theta} f \).

Automorphic forms are real analytic, by (15.7.2.10).
Def. (15.7.1.10) [Cuspidal Forms]. If $\infty$ is a cusp of $\Gamma$, then $\{\pm 1\} \Gamma_\infty = \{\pm 1\} \left\langle \begin{bmatrix} 1 & r \\ 1 & 1 \end{bmatrix} \right\rangle$, so a $F \in \mathcal{A}(\Gamma \setminus G, \chi, \omega)$ is called cuspidal at $\infty$ iff $\chi(\tau_r) \neq 1$ or

$$\int_0^T F \left[ \begin{array}{c} 1 \\ x \\ 1 \end{array} \right] g dx = 0.$$ 

for any $g \in G$. Notice this is independent of $r$ chosen.

More generally, if $a$ is a cusp of $\Gamma$, then choose $\xi \in SL(2, \mathbb{R})$ that $\xi(\infty) = a$, then for $F \in \mathcal{A}(\Gamma \setminus G, \chi, \omega)$, $F'(g) = F(\xi g) \in \mathcal{A}(\Gamma' \setminus G, \chi', \omega)$, where $\Gamma' = \xi^{-1} \Gamma \xi$, $\chi'(\gamma') = \chi(\xi' \xi^{-1})$(Because left and right actions commute). Then $F$ is called cuspidal at $a$ iff $F'$ is cuspidal at $\infty$.

The subspace of cuspidal forms is denoted by $\mathcal{A}_0(\Gamma \setminus G, \chi, \omega) \subset \mathcal{A}(\Gamma \setminus G, \chi, \omega)$.

Prop. (15.7.1.11) [Hecke Operators]. Similar as in (15.11.3.6), we can define the action of $\mathcal{R}_N$ on $C^\infty(\Gamma_0(N) \setminus G, \chi_d)$:

$$T_\alpha(f)(g) = \sum_i \chi_d(\alpha_i)^{-1} f(\alpha_i g), \quad \text{if} \quad \Gamma_0(N) \alpha \Gamma_0(N) = \prod_i \Gamma_0(N)\alpha_i.$$ 

and preserves automorphic or cuspidal forms.

Proof: This is an action because if $\Gamma_0(N) \alpha \Gamma_0(N) = \prod_i \Gamma_0(N)\alpha_i \Gamma_0(N) \rho \Gamma_0(N) = \prod_j \Gamma_0(N)\beta_j$, then $[\alpha][\beta] = \prod_i \Gamma_0(N)\alpha_i \beta_j$.

Also $f(\gamma x) = \chi(\gamma) f(x)$ for $\gamma \in \Gamma_0(N)$ because $\Gamma_0(N) \setminus \Gamma \setminus \Gamma_0(N)$ is right $\Gamma_0(N)$-invariant.

□

$\Gamma \setminus \mathcal{H}$

Def. (15.7.1.12) [Right Weight Action]. There are right actions of $GL(2, \mathbb{R})^+$ on $C^\infty(\mathcal{H})$ defined to by

$$(f|_k g)(z) = \left( \frac{cz + d}{|cz + d|} \right)^k f(\frac{az + b}{cz + d})$$

Proof: It is an action because □

Def. (15.7.1.13) [Holomorphic Right Weight Action]. Besides the right weight action (15.7.1.12), there is another family of actions:

$$f[\gamma]_k(z) = \deg(\gamma)^{k/2} (cz + d)^{-k} f(\frac{az + b}{cz + d}).$$

Proof: This is an action because □

Remark (15.7.1.14). This action is related to that of (15.7.1.12) via (15.7.3.9).

Lemma (15.7.1.15). If $f$ is a holomorphic function on $\mathcal{H}$ and $\gamma \in SL_2(\mathbb{R})$ satisfies $\gamma^n = 1$ for any $n \neq 0$ and $f[\gamma]_k = f$, then $f = 0$.

Proof: Use a Cayley transformation $\mathcal{H} \rightarrow \mathbb{D}$ to map the fixed point to origin, then $\gamma$ corresponds to $\text{diag}(\alpha, \alpha^{-1})$, where $\alpha$ is not a root of unity. Then if $f(z) = \sum a_n z^n$, the formula $f[\gamma]_k = f$ says $a_n \alpha^{2n+k} = a_n$. Because $\alpha^{2n+k} \neq 1$ for any $n$, $a_n = 0$ for any $n$, thus $f = 0$. □
Def. (15.7.1.16) [Form Spaces]. If $\Gamma$ is a discrete subgroup of $G_1$, let $C^\infty(\Gamma \backslash \mathcal{H}, \chi, k)$ be the space of smooth functions on $\mathcal{H}$ that
\[ f|_k \gamma = \chi(\gamma) f, \quad \gamma \in \Gamma. \]
And elements in $C^\infty(\Gamma \backslash \mathcal{H}, 1, 0)$ are called automorphic functions.

Let the subspace $C_c^\infty(\Gamma \backslash \mathcal{H}, \chi, k)$ be those functions $f$ that $|f|$ is compactly supported in $\Gamma \backslash \mathcal{H}$.

Def. (15.7.1.17) [Behavior at Cusps]. If $\infty$ is a cusp of $\Gamma$, then $\Gamma$ contains some $\tau_\infty = \begin{bmatrix} 1 & \tau \\ 0 & 1 \end{bmatrix}$ for $\tau > 0$, then a continuous function $f(x + iy)$ on $\mathcal{H}$ is called
- at most linear exponential growth at $\infty$ iff $|f(x + iy)| = O(e^{Ny})$ for $y \to \infty$
- of decay moderate at $\infty$ iff $|f(x + iy)| = O(y^N)$ for $y \to \infty$.
- decay rapidly at $\infty$ iff $|f(x + iy)| \leq y^{-N}$ for some $N > 0$.
- cuspidal at $\infty$ iff either $\chi(\tau_\infty) \neq 1$ or $\int_0^\tau f(z + u)du = 0$ for any $z \in \mathcal{H}$.

If $f$ is meromorphic on $\mathcal{H}$ then we have a Fourier expansion
\[ f(z) = \sum_{n=-\infty}^{\infty} a_n e^{2\pi intz/r} = \sum_{n=-\infty}^{\infty} a_n q^n = T(q). \]
Then $f$ is called meromorphic/holomorphic/vanishes at the cusp $\infty$ iff $T(q)$ does at 0.

The general cusp case is reduced to the $\infty$ case the same way as in (15.7.1.10). Notice this is independent of possible $r$ chosen.

Prop. (15.7.1.18) [Hecke Operators]. Similar as in (15.11.3.6), we can define the action of $\mathcal{R}_N$ on $C^\infty(\Gamma_0(N) \backslash \mathcal{H}, \chi_d, k)$:
\[ T_\alpha(f) = \sum_i \chi_d(\alpha_i)^{-1} f|_k \alpha_i(15.7.1.12), \quad \text{if } \Gamma_0(N) \alpha \Gamma_0(N) = \prod_i \Gamma_0(N) \alpha_i. \]
and preserves automorphic or cuspidal automorphic forms.

Proof: This is an action because if $\Gamma_0(N) \alpha \Gamma_0(N) = \prod_i \Gamma_0(N) \alpha_i, \Gamma_0(N) \beta \Gamma_0(N) = \prod_j \Gamma_0(N) \beta_j$, then $[\alpha][\beta] = \prod_{i,j} \Gamma_0(N) \alpha_i \beta_j$.
Also $T_\alpha(f)|_k \gamma = T_\alpha(f)$ for $\gamma \in \Gamma_0(N)$ because $\Gamma_0(N) \backslash \Gamma_0(N) \alpha \Gamma_0(N)$ is right $\Gamma_0(N)$-invariant.  

$L^2$-Spaces

Def. (15.7.1.19) [Inner Product on Form Spaces]. Notice that if $f, g \in C^\infty(\Gamma \backslash \mathcal{H}, \chi, k)(15.7.1.16)$, then $f \overline{g}$ is invariant under action of $\Gamma$, so we define the Hilbert space $L^2(\Gamma \backslash \mathcal{H}, \chi, k)$ as the square-integrable functions in the inner product (15.7.1.1):
\[ (f, g) = \int_{\Gamma \backslash \mathcal{H}} f(z) \overline{g(z)} \frac{dxdy}{y^2}. \]

Def. (15.7.1.20) $L^2$-Spaces. $L^2(\Gamma \backslash G, \chi)$ is defined to be the space of functions on $G$ that is $\chi$-invariant and that is square integrable on $\Gamma \backslash G_1$ (because it can descend) with the quotient Haar measure (15.7.1.3)(notice that the absolute value descents to $\Gamma \backslash G_1$) that satisfies conditions in (15.7.1.8).

$L^2_0(\Gamma \backslash G, \chi)$ is the subspace of $L^2(\Gamma \backslash G, \chi)$ of cuspidal elements, where cuspidality is defined the same way as in (15.7.1.10) but in the sense that holds for a.e. $g$.

$L^2(\Gamma \backslash G, \chi, k)$ be the subspace of $L^2(\Gamma \backslash G, \chi)$ consisting of functions $F$ that $\rho(k_\theta)F = e^{ik\theta} F$.  

Prop.(15.7.1.21). The space \( C_c(\Gamma \backslash G, \chi) \) is dense in \( L^2(\Gamma \backslash G, \chi) \).

Proof: Firstly we show \( C_c(\Gamma \backslash G, \chi) \) is dense in \( L^2(\Gamma \backslash G, \chi) \). Let \( \mathcal{F} \) be a Poincaré fundamental domain for \( \Gamma \) in \( SL_2(\mathbb{R})(15.7.2.5) \), then elements in \( C_c(\mathcal{F}) \) can be extended to elements of \( C_c(\Gamma \backslash G, \chi) \), and in this way, \( L^2(\Gamma \backslash G, \chi) \) is identified with \( L^2(\mathcal{F}) \), so the claim follows from (10.4.6.6). \( \square \)

Cor.(15.7.1.22). The right regular action of \( G \) extends to a continuous unitary representation of \( G \) on \( L^2(\Gamma \backslash G, \chi) \). \( L^2_0(\Gamma \backslash G, \chi) \) is invariant under this representation.

Proof: We must verify continuity, and this is clear using the proposition because we can choose a compact supported function \( f \) to approximate, then the right action is uniformly continuous. The unitaricity is clear. The invariance of \( L^2_0(\Gamma \backslash G, \chi) \) is clear. \( \square \)

Remark(15.7.1.23). Can this be extended to arbitrary locally compact group \( G \)?, compare with (10.9.2.9).

Prop.(15.7.1.24)[Two Form Spaces Equal]. There is an isomorphism of Hilbert spaces
\[
\sigma_k : C^\infty(\mathcal{H}, \chi, k) \cong C^\infty(\Gamma \backslash G, \chi, k) : (\sigma_k f)(g) = (f|k g)(i).
\]
that preserves the inner products thus induces an isomorphism
\[
\sigma_k : L^2(\mathcal{H}, \chi, k) \cong L^2(\Gamma \backslash G, \chi, k)
\]
And we have (15.7.3.1):
\[
\sigma_{k+2} R_k = dR \sigma_k, \quad \sigma_{k-2} L_k = dL \sigma_k, \quad \sigma_k \Delta_k = \Delta \sigma_k.
\]
Also cuspidality and the behaviors at the cusps are compatible.

Also if \( \Gamma = \Gamma_0(N) \), this isomorphic is compatible with the Hecke operator actions (15.7.1.18) and (15.7.1.11).

Proof: It can be verified that the inverse of \( \sigma_k \) is given by
\[
f(z) = F\left(\begin{bmatrix} y \\ x \\ 1 \end{bmatrix}\right)
\]
More precisely, if coordinates (15.7.1.3),
\[
F(u, x, y, \theta) = f(x + iy)e^{ik\theta}, \quad f(z) = F(0, x, y, 0).
\]
Check the left action of \( \Gamma \) and \( Z^+(\mathbb{R}) \): For \( \Gamma \) actions (15.7.1.16) and (15.7.1.8), this is because \( \sigma_k(f)(\gamma g) = f|k(\gamma g)(i) = \sigma_k(f|k \gamma) \). Finally check that \( \sigma_k \) preserves inner product, which is immediate from (15.7.1.19)(15.7.1.20) and (15.7.1.3).

The equations between \( R_k, L_k \) and \( R, L \) are easily verified from (15.7.1.5).

Th action of Hecke operators are compatible by the form \( (\sigma_k f)(g) = (f|k g)(i) \) as above.

Compatibility of behaviors at cusps: It suffices to check growth conditions, and this follows from ??.
2 Technicalities

Prop.(15.7.2.1). \[ k_\theta \begin{bmatrix} y_1 \\ y_2 \end{bmatrix} = \begin{bmatrix} y_1 y_2 D(\theta)^{-1} & \xi D(\theta)^{-1} \\ D(\theta) \end{bmatrix} k_{\theta'} \]

where \[ \theta' = \arctan(\frac{y_1}{y_2} \tan \theta), \quad D(\theta) = \sqrt{y_1^2 \sin^2 \theta + y_2^2 \cos^2 \theta}, \quad \xi = (y_2^2 - y_1^2) \sin \theta \cos \theta. \]

Proof: Hint: find \( \theta' \) first.

Prop.(15.7.2.2)[Gelfand]. Let \( G = GL(n, \mathbb{R})^+, K = SO(n) \), denote \( C_c^\infty(K \backslash G/K) \) to be the smooth functions \( \varphi \in C^\infty(G) \) that \( \varphi(k_1 g k_2) = \varphi(g) \), then \( C_c^\infty(K \backslash G/K) \) is commutative.

Proof: Consider the map \( \varphi \mapsto \hat{\varphi} : \hat{\varphi}(g) = \varphi(g') \), then it is an anti-involution of \( C_c^\infty(K \backslash G/K) \):

\[ (\widehat{\varphi_1} \ast \widehat{\varphi_2})(g) = \int_G \varphi_1(g'h) \varphi_2(h^{-1}) dh = \int_G \widehat{\varphi_2}(h^{-1}) \widehat{\varphi_1}(h') dh = \int_G \widehat{\varphi_2}(h) \widehat{\varphi_1}(h^{-1} g) dh = (\hat{\varphi_2} \ast \hat{\varphi_1})(g) \]

But we find \( \hat{\varphi} = \varphi \), because we can use(11.6.6.1), \( \varphi(g) = \varphi(d) = \hat{\varphi}(d) = \hat{\varphi}(g) \).

Prop.(15.7.2.3). Let \( G = GL(2, \mathbb{R})^+, K = SO(2) \), let \( \sigma \) be a character of \( K \), then \( C_c^\infty(K \backslash G/K, \sigma) \) is commutative.

Proof: The proof is the same as that of(15.7.2.2), but modified as

\[ \hat{\varphi}(g) = \varphi\left( \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} g' \begin{bmatrix} -1 & 0 \\ 0 & 1 \end{bmatrix} \right). \]

Siegel Sets

Def.(15.7.2.4)[Siegel Sets].

Prop.(15.7.2.5)[Poincaré Fundamental Domain]. Fundamental domain for \( \Gamma \subset GL(2, \mathbb{R}) \) acting on \( \mathcal{H} \) is defined in(10.9.1.35). There is a well-shaped open subset \( F \) with a set \( F \subset F' \subset \overline{F} \) that \( F' \) is a fundamental domain for \( \Gamma \) acting on \( \mathcal{H} \).

Notice that if \( \mathcal{F} \) is a fundamental domain for \( \Gamma \) in \( \mathcal{H} \equiv SL_2(\mathbb{R})/SO(2, \mathbb{R}) \), then the inverse image of \( \mathcal{F} \) is a fundamental domain for \( \Gamma \) in \( SL_2(\mathbb{R}) \), because a.e. \( z \in \mathcal{H} \) is not fixed by any \( \gamma \in \Gamma \).

Proof: Choose a \( z \in \mathcal{H} \) which is not fixed by any \( \gamma \in \Gamma \), then for any \( \gamma \in \Gamma \), draw the circle of points that have the same distance to \( z \) and \( \gamma(z) \), then the intersection of all the part containing \( z \) is a fundamental domain.

Prop.(15.7.2.6)[Siegel]. If a Poincare fundamental domain \( \Omega \) has finite area, then \( \partial \Omega \) is a union of f.m. geodesics, and \( \partial \Omega \cap X \) is finite, and \( \Gamma(\partial \Omega \cap X) \) is the set of cusps for \( \Gamma \).
Proof: The volume of $\Omega$ has a relation with the angles of geodesics of $\Omega$, so it can only have f.m. vertices with interior angle $< 0.9\pi$. And the $\Gamma$-orbits of these angles intersect $\Omega$ at f.m. vertices, which is because they consists of $\Gamma$-conjugates with the same distance with $z_0$, and a compact set meets f.m. geodesics of $\Omega$, because $\Gamma z_0$ is discrete in $\mathcal{H}$. In particular, $\Gamma$ has f.m. vertices in the boundary.

Now if $\Gamma$ has infinitely many vertices, there is a vertex $b$ that all its $\Gamma$-conjugates have angles $> 0.9\pi$, then consider the $\Gamma$-conjugates of $\Omega$ with a vertex $b$, then all their angle at $b > 0.9\pi$, but this cannot be possible geometrically.

For any cusp $x$ of $\Gamma$, suppose the Poincare fundamental domain is defined using $z$, notice there is a $\gamma \in \Gamma$ that $d(\gamma x, z)$ attains minimum, then $\gamma x$ must by in the boundary of $\Gamma$, as $d(\gamma_0 z, \gamma x) = d(z, \gamma x)$, and no other $z$ are closer to $\gamma x$.

Prop. (15.7.2.7) [Siegel Set and Fundamental Set]. Siegel set is a nicely shaped substitutes for a fundamental domain:

1. Let $a_1, \ldots, a_n \in \mathbb{R} \cup \{\infty\}$ be a representation of the $\Gamma$-orbits of cusps of $\Gamma$(15.7.2.6), let $\xi \in SL(2, \mathbb{R})$ be chosen that $\xi_i(a_i) = \infty$. If $c > 0, d > 0$ be chosen suitably, then the set $\cup \xi_i^{-1}F_{c,d}$ contains a fundamental domain of $\Gamma$.
2. Suppose $\infty$ is a cusp of $\Gamma$, then if $d$ is large enough, then $F_d^\infty$ contains a fundamental domain for $\Gamma$.

Proof: 1: $\xi_i\Gamma\xi_i^{-1}$ contains a unipotent subgroup generated by $\begin{bmatrix} 1 & \delta_i \\ 0 & 1 \end{bmatrix}$, so if $d \geq \delta_i$, then $\xi_i^{-1}F_{c,d}$ contains a nbhd of the cusp $a_i$ in the fundamental domain $F$ of $\Gamma$, so $F - \cup \xi_i^{-1}F_{c,d}$ is precompact in $\mathcal{H}$, by(15.7.2.6). Now if $c = 0, d = \infty$, then $F - \cup \xi_i^{-1}F_{c,d} = \emptyset$, then this is true for some $c, d$.

For 2: because $\infty$ is a cusp, we may assume $F \in \mathcal{H} \cap \{x > 0\}$. If $d$ is large, then $d$ will contain each of the pieces $\xi_i^{-1}F_{c,d} \cap F$ in item1.

Prop. (15.7.2.8) [Compatibility of Growth Conditions]. Let $G/R$ be semisimple, $f$ be a function on $\Gamma \backslash G(\mathbb{R})$, then the following are equivalent:

1. $f$ is of moderate growth/rapidly decreasing.
2. $f$ is of moderate growth/rapidly decreasing on each cusp of $\Gamma$.
3. $f$ is of moderate growth/rapidly decreasing on each Siegel set $S_{i,c,d}$.

Proof: Cf.[Bor97]P5.11. We only prove for $SL(2, \mathbb{R})$.

Harish-Chandra Theorem

Thm. (15.7.2.9) [Harish-Chandra]. If $G$ is semisimple and $f \in C^\infty(G)$ be both $K$-finite and $Z$-finite, then

1. $f$ is real analytic.
2. $U(g)f$ is an admissible $(g, K)$-module.
3. There exists $\alpha \in C^\infty_c(G)$ that
   \[ \alpha(kgk^{-1}) = \alpha(g), \forall k \in K, \quad f * \alpha = f. \]
4. If $|f(g)| < C||g||^N$, then all $U(g)f$ satisfies similar inequalities with the same $N$, i.e. $f$ is uniformly of moderate growth.
15.7. AUTOMORPHIC REPRESENTATIONS OF $GL(N)$ OVER ARCHIMEDEAN LOCAL FIELDS

\textbf{Proof:} We prove only for $G = SL(2)$. See \cite{Harish-Chandra, Discrete series for semisimple Lie groups, II. Explicit determination of the characters. Acta. Math. 116 (1966)} or \cite{Gan’s notes, P24} for the general case.

Because $W$ lies in the Lie algebra of $K$ and $W = iH$, the hypothesis implies $\mathcal{R}f$ is f.d., where $\mathcal{R} = \mathbb{C}[\Delta, H]$. Let $V$ be the smallest closed $G$-invariant subspace of $C^\infty(G)$ containing $f$ and let $V_0 = U(\mathfrak{g})f$.

We first prove that

$$V_0 = \bigoplus_{-\infty}^{\infty} (V_0 \cap V(n)).$$

Notice there is a continuous projection of $V$ onto $V(n)$:

$$E_n\varphi(g) = \frac{1}{2\pi} \int_0^{2\pi} e^{-in\theta} \varphi(gk\theta)d\theta,$$

because $f$ is $K$-finite, there is an $N$ s.t. $f = \sum_{n=-N}^N E_n f$. Then notice any $Df$ is also $K$-finite because $D$ is combination of polynomials in $R, L, H$ and $R, L, H$ shift the weights, so the LHS is contained in the RHS. It’s left to show now $E_n Df \in V_0$ for any $n$: $E_n Df$ can be extracted using Lagrange polynomial in $H$, so it is clearly in $V_0$.

Next we show $V_0 \cap V(n)$ is of f.d.: Let $f_1, \ldots, f_k$ be a basis of $\mathcal{R}f$, because each $f_k$ is $K$-finite, so if we use the decomposition of $U(\mathfrak{sl}_2(\mathbb{C}))$ (2.5.8.24), only the $R, L$ shifting of the $E_n f$ will be considered, and clearly each $V_0 \cap V(n)$ is of f.d.

Now we show $f$ is analytic: because $f$ is $Z$-finite, there is an equation $P(\Delta)f = 0$ where $P$ is a monic function, and because $\Delta$ commutes with $E_k$ and $f$ is $K$-finite, $P(\Delta)E_k f = 0$. Note the $P(\Delta)E_k f = P(\Delta_k)E_k f$ by (15.7.1.5) and (15.7.3.1), and $P(\Delta_k)$ is an elliptic operator, so $E_k f$ is analytic by (10.11.8.5).

Now we show $V$ is the closure of $V_0$: Suppose not, then by Hahn-Banach there is a non-zero continuous linear functional $\Lambda$ on $V$ that $\Lambda(V_0) = 0$. If $F \in C^\infty(G)$, let $\varphi_F(g) = \Lambda(\rho(g)F)$, and let $\varphi = \varphi_F$. Clearly $dX \varphi_F = \varphi_{dX F}$, so $D\varphi_F = \varphi_{DF}$, which implies $\varphi$ is $Z$-finite and smooth, and also $K$-finite because $f$ does. So by what we have proved, $\varphi$ is analytic. But now $\varphi$ is analytic and $D\varphi(1) = \varphi_{DF}(1) = 0$ because $Df \in V_0$, so $\varphi = 0$ by Taylor expansion. So $\Lambda(\rho(g)F) = 0$ for any $g$, contradiction because $\rho(g)F$ is dense in $V$.

So actually $V(n) \subset V_0$, because $E_n V_0 = V_0 \cap V(n) \subset V(n)$ is dense, and $V_0 \cap V(n)$ is of f.d., so $V(n) \subset V_0 = V_0(10.7.1.8)$ and $V_0 = \oplus V(n)$ is an admissible $(\mathfrak{g}, K)$-module.

Let $J$ be the convolution algebra (because $G$ is unimodular) of functions $\alpha$ that $\alpha(kgk^{-1}) = \alpha(g)$, then it can be checked that convolution $- * \alpha$ commutes with action of $K$, so $f * J$ is in the same $K$-type space as $f$, thus $K$-finite and in a f.d. space.

Now we can approximate $f$ by $f \ast J$: choose a Dirac sequence $\{\alpha_n\} \subset C_c^\infty(G_1)$, we may replace $\{\alpha_n\}$ by the function $\beta_n(g) = \int_K \alpha_n(k^{-1}gk)dk$ to obtain a Dirac sequence in $J$. Then $f \ast \alpha_n \rightarrow f$ uniformly on compact sets. But $f \ast J$ is f.d., so there are some $f \ast \alpha = f$.

Finally for the growth estimate, it suffices to check for $D \in G$. Then $dX(f) = dX(f \ast \alpha) = f \ast (dX \alpha)$, from which the estimate is clear. \qed

**Cor. (15.7.2.10) [Automorphic Forms Generate Admissible $(\mathfrak{g}, K)$-Modules].** The space $\mathcal{A}(\Gamma \setminus G, \chi, \omega)$ and $\mathcal{A}_0(\Gamma \setminus G, \chi, \omega)$ are stable under the action of $U(\mathfrak{g})$, and for $f \in \mathcal{A}(\Gamma \setminus G, \chi, \omega)$, $f$ is analytic and $U(\mathfrak{g})f$ is an admissible $(\mathfrak{g}, K)$-module.

Moreover, if $f$ satisfies condition of moderate growth (15.7.1.9) and $D \in U(\mathfrak{g})$, then $Df$ satisfies similar conditions with the constant $N$. 

Proof: It suffices to prove for $\mathcal{A}(\Gamma \backslash G, \chi, \omega)$ because the cuspidality condition is clearly preserved by right action.

We want to use Harish-Chandra theorem (15.7.2.9) on $G(K)/Z(K)$. Now $|f|$ is constant on each fiber of $G(K) \to G(K)/Z(K)$, it suffices to compare the norm on $G(K)$ and $G(K)/Z(K)$.

We do this only for $\text{GL}(2, \mathbb{R})$?

The condition of moderate growth is compatible because the minimal $\|g\|$ in a $Z(\mathbb{R})$-orbit is achieved when $\deg g = 1$(15.7.1.9). So all the assertion follows from that of(15.7.2.9) and its proof. □

3 Maass Forms

Maass Forms

Def. (15.7.3.1) [Maass Operator]. A Maass differential operators on $C^\infty(\mathcal{H})$ is defined to be

$$R_k = (z - \overline{z})\frac{\partial}{\partial z} + \frac{k}{2} = iy\frac{\partial}{\partial x} + y\frac{\partial}{\partial y} + \frac{k}{2}, \quad L_k = -(z - \overline{z})\frac{\partial}{\partial \overline{z}} - \frac{k}{2} = -iy\frac{\partial}{\partial x} + y\frac{\partial}{\partial y} - \frac{k}{2}$$

and

$$\Delta_k = -y^2\left(\frac{\partial^2}{\partial x^2} + \frac{\partial^2}{\partial y^2}\right) + iky\frac{\partial}{\partial x} = -L_{k+2}R_k - \frac{k}{2}(1 + \frac{k}{2}) = -R_{k-2}L_k + \frac{k}{2}(1 - \frac{k}{2})$$

$\Delta_k$ is a symmetric (unbounded) operator on $L^2(\mathcal{H})$ with domain $C_c^\infty(\mathcal{H})$.

Proof: For the formula:?

For the symmetry: composed with the measure, the order 2 part is just the ordinary Laplacian, and the order 1 part becomes $iy^{-1}\frac{\partial}{\partial x}$, then notice

$$\int_{\mathcal{H}} iy^{-1}\left(\frac{\partial f}{\partial x} + f \frac{\partial y}{\partial x}\right) dxdy = i \int_{\mathcal{H}} d(y^{-1}f\overline{g}dy) = 0$$

as $f, g$ are compactly supported. □

Prop. (15.7.3.2) [Maass Operator and Weight Action]. For $f \in C^\infty(\mathcal{H}), g \in G$,

$$(R_k f)|_{k+2g} = R_k(f|k g), \quad (L_k f)|_{k-2g} = L_k(f|k g), \quad (\Delta_k f)|_{k g} = \Delta_k(f|k g)$$

Proof: For $R_k$, because scalar doesn’t matter, we may assume $g \in SL_2(\mathbb{R})$, and let $w = \frac{az + b}{cz + d}$, then

$$\frac{\partial}{\partial z} = \frac{\partial w}{\partial z} \frac{\partial}{\partial w} = \frac{(cz + d)^2}{|cz + d|^2}(w - \overline{w}) = \frac{z - \overline{z}}{|cz + d|^2}.$$ 

So

$$(w - \overline{w})\frac{\partial}{\partial w} = \frac{(cz + d)^2}{|cz + d|^2}(z - \overline{z})\frac{\partial}{\partial z}.$$ 

And for any smooth function $\varphi \in C^\infty(\mathcal{H})$,

$$(z - \overline{z})\frac{\partial}{\partial z}(\frac{cz + d}{|cz + d|})^k \varphi = (z - \overline{z})(\frac{cz + d}{|cz + d|})^k \frac{\partial \varphi}{\partial z} + \frac{k}{2}
\left(\frac{cz + d}{|cz + d|}\right)^{k+2} - \left(\frac{cz + d}{|cz + d|}\right)^k \varphi.$$ 

This is because

$$\frac{\partial}{\partial z}|cz + d| = \frac{c}{2}\frac{cz + d}{|cz + d|}, \quad \frac{\partial}{\partial z}(\frac{cz + d}{|cz + d|})^k = -\frac{k}{2}\frac{c(z - \overline{z})}{|cz + d|^2}(\frac{cz + d}{|cz + d|})^k = \frac{k}{2}
\left(\frac{cz + d}{|cz + d|}\right)^{k+2} - \left(\frac{cz + d}{|cz + d|}\right)^k.$$
Thus,
\[ R_k(f|g) = [(z - \overline{z}) \frac{\partial}{\partial z} + k \frac{cz + d}{|cz + d|})^k f(w) = [(z - \overline{z}) \frac{cz + d}{|cz + d|})^k \frac{\partial}{\partial z} + k \frac{cz + d}{|cz + d|})^{k+2} f(w) = (\frac{cz + d}{|cz + d|})^{k+2} [(w - \overline{w}) \frac{\partial}{\partial w} + \frac{k}{2} f(w) = ((R_k f)|_{k+2} g)(z). \]

The case of \( L_k \) is similar, and \( \Delta_k \) follows.

\[ \square \]

\textbf{Cor. (15.7.3.3)} The operator \( R_k, L_k, \Delta_k \) maps functions between \( C^\infty(\Gamma \setminus \mathcal{H}, \chi, \kappa) \) and arises and decreases weights respectively.

\textbf{Prop. (15.7.3.4)} For \( f \in C^\infty(\Gamma \backslash \mathcal{H}, \chi, \kappa), g \in C^\infty(\Gamma \backslash \mathcal{H}, \chi, \kappa + 2) \), if one of them decays rapidly at all cusps, then (15.7.1.19)

\[ (R_k f, g) = (f, -L_{k+2} g). \]

In particular, \( \Delta_k = -L_{k+2} R_k = \frac{k}{2} (1 + \frac{k}{2}) \) is symmetric on the subspace of \( L^2(\Gamma \backslash \mathcal{H}, \chi, \kappa) \) consisting of rapidly decaying functions, \( \Delta \) is unbounded and defined only on \( C^\infty(\Gamma \backslash \mathcal{H}, \chi, \kappa) \) now, but will be extended to \( L^2(\Gamma \backslash \mathcal{H}, \chi, \kappa) \) in (15.7.5.5) when \( \Gamma \backslash \mathcal{H} \) is compact.

\textit{Proof:} Let \( \omega = y^{-1} f(z) \overline{g(z)} d\overline{z} \). It can be shown by definition and using (10.5.1.8) that \( \omega(\gamma z) = \omega(z) \), so \( \omega \) descends to a differential form on \( \Gamma \backslash \mathcal{H} \), and because one of \( f, g \) decays rapidly at all cusps,

\[ 0 = \int_{\Gamma \backslash \mathcal{H}} d(y^{-1} f(z) \overline{g(z)} d\overline{z}) = \int_{\Gamma \backslash \mathcal{H}} \left[ \frac{\partial}{\partial y} (y^{-1} f \overline{g}) + i \frac{\partial}{\partial x} (y^{-1} f \overline{g}) \right] dx \wedge dy = \int_{\Gamma \backslash \mathcal{H}} \left[ (iy \frac{\partial f}{\partial x} + y \frac{\partial f}{\partial y}) \overline{g} - (iy \frac{\partial g}{\partial x} - y \frac{\partial g}{\partial y}) f - f \overline{g} \right] \frac{dx dy}{y^2} = \int_{\Gamma \backslash \mathcal{H}} \left[ (R_k f) \overline{g} + f(L_k + 2g) \right] \frac{dx dy}{y^2}. \]

so the conclusion follows.

\[ \square \]

\textbf{Cor. (15.7.3.5)} If \( \lambda \) is an eigenvector of \( \Delta_k \) on \( C^\infty(\Gamma \backslash \mathcal{H}, \chi, \kappa) \), then either \( \lambda = \frac{l}{2} (1 - \frac{1}{2}) \), where \( 1 \leq l \leq k \) and \( l \equiv k \mod 2 \), or \( \lambda \geq \frac{5}{4} (1 - \frac{1}{2}) \), where \( \varepsilon = 0 \) or \( 1 \) and \( k \equiv \varepsilon \mod 2 \). In particular, eigenvalues of \( \Delta_0 \) are \( \geq 0 \) and eigenvalues of \( \Delta_1 \) are \( \geq 1/4 \).

\textit{Proof:} This can be done by repeatedly using \( \Delta_{k-2} L_k = L_k \Delta_k \) to reduce \( \Delta_\varepsilon \), or can be deduced from (15.7.5.11).

\[ \square \]

\textbf{Def. (15.7.3.6) [Maass Forms]. A twisted Maass Form of weight \( k \) and parameter \( s \) for \( \Gamma \) is an element in \( C^\infty(\Gamma \backslash \mathcal{H}, \chi, \kappa) \) (15.7.1.16) that is an eigenform for \( \Delta_k \) of eigenvalue \( \lambda = \frac{1}{4} - s^2 \) and is of moderate growth at cusps of \( \Gamma \mathcal{H} \). The space of Maass forms are denoted by \( \mathcal{A}_{\text{Maass}}(\Gamma \backslash \mathcal{H}, \chi, k) \).

A Maass form of weight \( 0 \) and \( \chi = 1 \) is sometimes just a Maass form. The space of Maass form is denoted by \( \mathcal{A}_{\text{Maass}}(\Gamma \backslash \mathcal{H}) \).

\textbf{Def. (15.7.3.7) [Weak Maass Forms]. A weak Maass form of weight \( k \) and parameter \( s \) for \( \Gamma \) is an element in \( C^\infty(\Gamma \backslash \mathcal{H}, \chi, k) \) (15.7.1.16) that is an eigenform for \( \Delta_k \) of eigenvalue \( \lambda = \frac{1}{4} - s^2 \) and is of at most linear exponential growth at cusps of \( \Gamma \mathcal{H} \). A harmonic Maass form is a Maass form of eigenvalue \( \lambda = \frac{1}{4} - s^2 \) where \( s \) is an integer.
Prop. (15.7.3.8)[Hecke Operators on Maass Forms]. If $\Gamma = \Gamma_0(N)$, the space of Maass forms is stable under the action of the Hecke algebra on $C^\infty(\Gamma_0(N) \backslash \mathcal{H}, \chi, k)$ (15.7.1.18), by (15.7.3.2).

Def. (15.7.3.9)[Holomorphic Modular Forms as Maass Forms]. There is a bijection

$$ M_k(\Gamma, \chi) \cong A_{Maass}(\Gamma \backslash \mathcal{H}, \chi, k)^{L=0} : f \mapsto y^{k/2}f $$

that induces a bijection

$$ S_k(\Gamma, \chi) \cong A_{CuspMaass}(\Gamma \backslash \mathcal{H}, \chi, k)^{L=0}. $$

Proof: Direct calculation shows $L_k(y^{k/2}f(z)) = 2iy^{(k+2)/2} \frac{\partial}{\partial y} f(z)$, and by (10.5.1.8),

$$ (\text{Im}(z)^{k/2}f(z))|_k \gamma = (\frac{cz+d}{cz+d})^k \text{Im}(\gamma z)^{k/2}f(\gamma z) = (\frac{cz+d}{cz+d})^k \text{Im}(z)^{k/2}f(\gamma z) $$

so their invariant properties are compatible. Also, if $f$ is a holomorphic modular form, then each $y^{k/2}f[\gamma]_k$ is bounded by a polynomial of $y$ at $\infty$, and conversely, if $f(q)$ is bounded by a polynomial of $\log(1/|q|)$, then ?? shows $f$ is holomorphic at each cusp. And the cuspidal condition

$$ \int_0^\infty \text{Im}(z)^{k/2}f(z+u)du = \text{Im}(z)^{k/2} \int_0^\infty f(z+u)du = 0 $$

just means $f$ is a cuspidal form. □

Prop. (15.7.3.10)[Non-holomorphic Eisenstein series is a Maass Form]. The non-holomorphic Eisenstein series $E(s, \nu + 1/2)$ is a Maass form of parameter $\nu$ for $\Gamma(1)$.

Proof: $E(s, \nu + 1/2)$ is automorphic and of moderate growth by (16.2.5.6) and (16.2.5.4).

To show $E(s, \nu + 1/2)$ is an eigenfunction of $\Delta$, if $\text{Re}(\nu) > 1/2$, notice $\Delta(y^{\nu+1/2}) = (\frac{1}{4} - \nu^2)y^{\nu+1/2}$, and $\Delta$ is invariant under action of $SL(2, \mathbb{Z})$, thus each $\text{Im}(\gamma(y^{\nu+1/2}))$ is an eigenfunction for $\Delta$ of eigenvalue $\frac{1}{4} - \nu^2$, so the same is true for $E(s, \nu + 1/2)$.

For general $\nu$, this can be seen from the Fourier coefficients of $E(s, \nu + 1/2)$ (16.2.5.5): □

Prop. (15.7.3.11)[Maass Forms as Automorphic Forms]. If $f \in A_{Maass}(\Gamma \backslash \mathcal{H}, \chi, k)$, then $\sigma_k(f) \in C^\infty(\Gamma \backslash G, \chi, k)$ (15.7.1.24), and is an eigenform of $\Delta$. In particular it is $K$-finite, $\omega$-finite, of moderate growth by (15.7.1.24), and it is cuspidal iff $\sigma_k(f)$ is cuspidal, so $\sigma_k(f) \in A(\Gamma \backslash G, \chi, k)$. And $f$ is cuspidal iff $\sigma_k(f)$ is cuspidal.

In fact, there are bijections

$$ A_{Maass}(\Gamma \backslash H, \chi, k, \lambda) \cong A(\Gamma \backslash G, \chi, k, \lambda), \quad A_{Maass}(\Gamma \backslash H, \chi, k) \cong A(\Gamma \backslash G, \chi, k)^{\Delta-ss} $$

$$ A_{CuspMaass}(\Gamma \backslash H, \chi, k) \cong A_0(\Gamma \backslash G, \chi, k), \quad A_{CuspMaass}(\Gamma \backslash H, \chi) \cong A_0(\Gamma \backslash G, \chi) = L^2_0(\Gamma \backslash G, \chi)^{K-fin}. $$

This is because when $f$ is cuspidal, $\Delta$ is semisimple on the finite dimensional subspace $Zf$ because of the spectral decomposition of $L^2_0(\Gamma \backslash G, \chi, k)$ (15.7.5.8).

Cor. (15.7.3.12)[Modular Forms as Automorphic Forms]. Combine this and (15.7.3.9), we get a bijection

$$ M_k(\Gamma, \chi) \cong A(\Gamma \backslash G, \chi, k)^{L=0} $$

that induces a bijection

$$ S_k(\Gamma, \chi) \cong A_0(\Gamma \backslash G, \chi, k)^{L=0}. $$
Cor. (15.7.3.13) [Finitely Many Maass Forms of Given Type]. \( \dim \mathcal{A}_{\text{Maass}}(\Gamma_0(N) \backslash \mathcal{H}, \chi, k, \lambda) < \infty. \)

**Proof:** This follows from (15.7.2.10).

Conj. (15.7.3.14) [Selberg Conjecture]. Let \( \Gamma \) be a congruence subgroup, for any cuspidal Maass form \( f \), the eigenvalue \( \lambda \) of \( \Delta_0 \) satisfies \( \lambda \geq 1/4 \), or equivalently, the parameter \( s \) is purely imaginary. In this case, the cuspidal representation generated by \( f \) is tempered.

This conjecture is true for \( \Gamma = \Gamma(1) \) but wrong for some other congruence subgroups.

**Harmonic Maass Forms**

References are [Harmonic Maass Forms, Mock Modular Forms, And Quantum Modular Forms, Ken Ono], [Harmonic Maass Forms and Mock Modular Forms Theory and Applications].

Def. (15.7.3.15) [Harmonic Maass Forms]. A **harmonic Maass form** is a weak Maass form (15.7.3.7) of eigenvalue \( k^2 (1 - k^2) \), where \( k \) is an integer. Any modular form corresponds to a harmonic Maass form, by (15.7.3.9).

Def. (15.7.3.16) [Mock Modular Forms]. A **Mock modular form** is the holomorphic part of a harmonic Maass form.

4 Whittaker Models

Def. (15.7.4.1) [Whittaker Function Space]. For \( \psi \in \hat{R} \), denote \( W_\psi = \) the space of smooth functions \( f \) on \( GL(n, \mathbb{R})^+ \) that satisfies

\[
f(ug) = \psi_{\text{Unip}(n)}(u)f(g), \quad u \in \text{Unip}(n)
\]

A function \( f \in W \) is called:

- **of moderate growth** if for any compact set \( \Omega \subset G \), \( |f(y)g)| < C|y|^k \) for some \( C, k > 0 \) for any \( g \in \Omega \) when \( |y| \to \infty \).

- **rapidly decreasing** if for any compact set \( \Omega \subset G \) and \( k \in \mathbb{R} \), \( |f(y)g)| < C|y|^k \) for some \( C \) for any \( g \in \Omega \) when \( |y| \to \infty \).

**Lemma (15.7.4.2) [Whittaker Function].** Let \( \mu, \lambda \in \mathbb{C} \) and \( k \in \mathbb{Z} \). Let \( W(\lambda, \mu, k) \) be the space of functions \( f \in W(15.7.4.1) \) on \( G \) s.t. \( \Delta f = \lambda f, \, I f = \mu f, \, f \in (C^\infty(G))^k \) and \( f \) is of moderate growth, then \( W(\lambda, \mu, k) \) is 1-dimensional, and functions in this space are actually rapidly decreasing and analytic.

Moreover, the operators \( R, L \) map \( W(\lambda, \mu, k) \) into \( W(\lambda, \mu, k + 2), \, W(\lambda, \mu, k - 2) \) respectively. Also, for \( |y| \to 0 \) and \( \mu \) imaginary, \( W(\lambda, \mu, k) \) is bounded by \( |y|^{-1/2} \) for some \( \varepsilon > 0 \).

**Proof:** For \( f \in W(\lambda, \mu, k) \), in coordinate (15.7.1.3), we have

\[
f(y) = u^\mu \psi(x)e^{ik\theta}w(y), \quad w(y) = f(y^{1/2}, y^{-1/2})
\]
Thus it suffices to study the behavior of \( w(y) \). By the expression of \( \Delta(15.7.1.5) \), if \( \psi(x) = e^{iax} \), then

\[
\frac{d^2 w}{dy^2} + (-a^2 + \frac{k}{2y} + \frac{\lambda}{y^2})w = 0
\]

And this is the Whittaker’s equation, and the only moderate growth function is rapidly decreasing and analytic. This is by direct calculation in [A course of Modern Analysis, Whittaker/Watson(1927)].

For the action of \( R, L \), they preserve \( W \) because they are right actions. And \( Rf, Lf \) have the same eigenvalue of \( \Delta, I \) because \( \Delta, I \) are in the center of \( U(g) \). They shift the weight by \((15.7.1.24)\) and \((15.7.3.2)\).

\[\square\]

Prop.(15.7.4.3)[Uniqueness of Whittaker Models for \( GL(2, \mathbb{R}) \)]. For \( (\pi, V) \in \text{Irr}^{\text{adm}}((g, K)) \), there exists at most one space \( W(\pi, \psi) \in W \) consisting of \( K \)-finite functions \( f \in W \) that is of moderate growth, and is invariant under the action of \( U(g) \) and \( K \), and is infinitesimal equivalent to \( (\pi, V) \).

Moreover, functions in \( W(\pi, \psi) \) are actually rapidly decreasing and analytic. The space \( W(\pi, \psi) \) is called the Whittaker model of \( \pi \), if it exists.

\[\text{Proof:}\] By \((15.6.3.9)\), \( \Delta, I \) acts by scalars \( \lambda, \mu \) on \( V \). By \((15.6.3.26)\) or \((15.6.3.34)\) if \( V^k \neq 0 \), then \( \dim V^k = 1 \). If \( V^k \neq 0 \), then the image of \( V^k \) under the isomorphism with \( W(\pi, \psi) \) is in the space \( W(\lambda, \mu, k) \). Thus \( W(\pi, \psi) \) is the direct sum of the \( W(\lambda, \mu, k) \) for all \( k \) that \( V^k \neq 0 \), so uniquely determined by \((15.7.4.2)\). And the rapid decreasing and analytic properties are also consequences of \((15.7.4.2)\).

\[\square\]

Prop.(15.7.4.4). If \( (\pi, V) \in \text{Irr}^{\text{adm}}((g, K)) \) has a Whittaker model, then there exists some \( \xi \in V \) that \( W_{\xi}(1) \neq 0 \).

\[\text{Proof:}\] Because \( K \) intersect each connected component of \( G \), we can assume some \( W_{\xi} \) is non-zero on \( K^0 \), thus by analyticity \((15.7.4.3)\), its derivatives at 1 are not identically 0, thus there exists some \( D \in U(g) \) that \( DW_{\xi}(1) = WD_{\xi}(1) \neq 0 \).

\[\square\]

Prop.(15.7.4.5)[Whittaker Models for \( GL(n, \mathbb{C}) \)]. This result is true if \( \mathbb{R} \) is replaced by \( \mathbb{C} \).

\[\text{Proof:}\] Cf.[Automorphic Forms on \( GL(2) \), Jacquet/Langlands (1970) Thm5.3. P232]?

Prop.(15.7.4.6)[Fourier-Maass Expansion].

\[\text{Proof:}\]

\[\square\]

Cor.(15.7.4.7)[Rapidly Decreasing]. Cuspidal automorphic Forms are rapidly decreasing at any Siegel set.

\[\text{Proof:}\] Cf.[Gan's Notes, P26].?

Prop.(15.7.4.8)[Existence of Whittaker Models]. The Whittaker model exists for the

Prop.(15.7.4.9)[Shalika’s Local Multiplicity One Theorem]. Given a unitary irreducible representation \( V \) of \( GL(n, F) \), a Whittaker functional on \( V^\infty \) is a \( \mathcal{N}(F) \)-map \( \lambda : V^\infty \to \psi_N \).

Then the space of Whittaker functionals on \( V^\infty \) is at most 1-dimensional.

\[\text{Proof:}\]
5 The Spectral Problem

The Spectral Problems for $\Gamma \backslash \mathcal{H}$ Compact

**Def. (15.7.5.1).** In this subsection we assume $\Gamma \backslash G_1$ is compact, or equivalently $\Gamma \backslash \mathcal{H}$ is compact, because $K$ is compact. This condition makes $C^\infty(\Gamma \backslash \mathcal{H}, \chi) = L^2(\Gamma \backslash \mathcal{H}, \chi)$, and will make the decomposition having only discrete parts (15.7.5.2).

**Prop. (15.7.5.2)** [$L^2(\Gamma \backslash G, \chi)$ Totally Decomposable]. The space $L^2(\Gamma \backslash G, \chi)$ decomposes into a Hilbert space direct sum of subspaces that are invariant and irreducible under the right regular action $\rho$.

*Proof:* This follows from (15.16.2.3). \hfill $\square$

**Lemma (15.7.5.3).** Let $\sigma$ be the character on $K$ that $\sigma(k) = e^{-ik\theta}$, $C_c^\infty(K \backslash G/K, \sigma)$ is commutative by (15.7.2.3), let $\xi$ be a character of it. Let $H(\xi)$ be the subspace of $f \in L^2(\Gamma \backslash G, \chi, k)$ that $\pi(\xi) = \xi(f)$ for $f \in C_c^\infty(K \backslash G/K, \sigma)$.

Then $H(\xi)$ is of f.d. and different $H(\xi), H(\eta)$ are orthogonal that $\otimes H(\xi) = L^2(\Gamma \backslash G, \chi, k)$.

*Proof:* Suppose $0 \in f \in H(\xi)$, then by (15.6.4.1), we can find a $\varphi \in C_c^\infty(K \backslash G/K, \sigma)$ s.t. $\rho(\varphi)f \neq 0$. And by hypothesis $\rho(\varphi)f = \xi(\varphi)f$, thus $\xi(\varphi) \neq 0$, and $f$ is an eigenvalue of $\rho(\varphi)$ which is compact and self-adjoint, so the $\xi(\varphi)$-eigenspace of $\rho(\varphi)$ is f.d. and $H(\varphi)$ is contained in this space, thus f.d.

To show the orthogonality, choose $\varphi \in C_c^\infty(K \backslash G/K, \sigma)$ that $\xi(\varphi) \neq \eta(\varphi)$. Considering $\varphi = \varphi_1 + i \varphi_2$, where $\rho(\varphi_1), \rho(\varphi_2)$ are both self-adjoint, then we may assume $\varphi$ is self-adjoint. Then $H(\xi), H(\eta)$ are contained in different eigenspaces of $\rho(\varphi)$, so they are orthogonal.

Finally for the direct sum, it suffices to show that if $f$ is orthogonal to all $H(\xi)$, then $f = 0$. Given $f$, let $\varphi_0 \in C_c^\infty(K \backslash G/K, \sigma)$ be chosen that $\rho(\varphi_0)f$ is near $f$ that $\rho(\varphi_0)f, f$ are not orthogonal (15.6.4.1).

Consider the eigenspace decomposition of $\rho(\varphi_0)$ on $L^2(\Gamma \backslash G, \chi, k)$, then $f = f_0 + f_1 + f_2 + \ldots$, then $\rho(\varphi_0)f = \lambda_1 f + \lambda_2 f + \ldots$. Because $f$ is not orthogonal to $\rho(\varphi_0)f$, thus $f_i$ is not orthogonal to $f$ for some $i \geq 1$. Let $V$ be the $\lambda_i$-eigenvalue of $\rho(\varphi_0)$, then $V$ is f.d. and invariant under $\rho(\varphi)$ for all $\varphi \in C_c^\infty(K \backslash G/K, \sigma)$ because $C_c^\infty(K \backslash G/K, \sigma)$ is commutative (15.7.2.3). So $V$ is a direct sum of elements of the spaces $H(\xi)$, so $V$ is orthogonal to $f$, contradiction. \hfill $\square$

**Prop. (15.7.5.4).** The space $L^2(\Gamma \backslash \mathcal{H}, \chi, k)$ decomposes into a Hilbert space direct sum of eigenspaces for $\Delta_k$.

*Proof:* By (15.7.1.24), it suffices to prove for $L^2(\Gamma \backslash G, \chi, k)$ and $\Delta$. Because $\Delta$ are in the center of $U(\gamma)$, $H(\xi)$ are all $\Delta$-invariant. So we finish by the lemma (15.7.5.3), as each $H(\xi)$ is f.d. so $\Delta$ is a self-adjoint operator on $H(\xi)$, because $C_c^\infty(\Gamma \backslash G, \chi)$ is dense (15.7.1.21). So it is a direct sum of $\Delta$-eigenspaces. \hfill $\square$

**Prop. (15.7.5.5).**
- The eigenvalues $\lambda_i$ of $\Delta_k$ on $L^2(\Gamma \backslash \mathcal{H}, \chi, k)$ tends to $\infty$, and satisfies $\sum \lambda_i^{-2} < \infty$.
- The laplacian $\Delta_k$ has an extension to a self-adjoint operator on the Hilbert space $L^2(\Gamma \backslash \mathcal{H}, \chi, k)$.

*Proof:* Cf. [Bump P185]. \hfill $\square$
The Spectral Problems for General Case

Prop. (15.7.5.6) [Gelfand, Graev and Piatetski-Shapiro]. Let \( \varphi \in C_c^\infty(G) \), then
- There exists a constant \( C(\varphi) \) that for all \( f \in L_0^2(\Gamma \backslash G, \chi, \omega) \), we have \( \| \rho(\varphi)f \|_{C(G)} \leq C(\varphi)\|f\|_2 \).
- \( \rho(\varphi) \) is a compact operator on \( L_0^2(\Gamma \backslash G, \chi, \omega) \).

Notice this generalizes (15.16.2.1).

Proof: We may assume \( \Gamma \) has cusps, otherwise this is proved in (15.16.2.1). Conjugating \( \Gamma \) by an element of \( SL(2, \mathbb{R}) \), we may assume that \( \infty \) is a cusp for \( \Gamma \), and \( \Gamma_\infty \) is generated by \( \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix} \). Then it suffices to prove that
\[
\sup_{g \in G_\infty} |\rho(\varphi)f(g)| \leq C_0\|f\|_2,
\]
because we can do the same for other cusps of \( \Gamma \), and use (15.7.2.7) to show that \( \sup_{g \in F} |\rho(\varphi)f(g)| \leq C_0\|f\|_2 \), hence for all \( g \in \mathcal{F} \).

Now let \( \varphi_\omega(g) = \int_{R^+} \varphi(zg)\omega(z)dz \), then
\[
\rho(\varphi)f(g) = \int_{Z(\mathbb{R}) \backslash G} f(gh)\varphi_\omega(h)dh
= \int_{Z(\mathbb{R}) \backslash G} f(h)\varphi_\omega(g^{-1}h)dh
= \int_{\Gamma_\infty Z(\mathbb{R}) \backslash G} \sum_{\gamma \in \Gamma_\infty} f(\gamma h)\varphi_\omega(g^{-1}\gamma h)dh
= \int_{\Gamma_\infty Z(\mathbb{R}) \backslash G} K(g,h)f(h)dh,
\]
where \( K(g,h) = \sum_{\gamma \in \Gamma_\infty} \chi(\gamma)\varphi_\omega(g^{-1}\gamma h) \). Then we can estimate the kernel \( K(g,h) \) and show it decays rapidly for \( h \) when \( g \) is fixed, and this will give the desired result. Cf. [Bump, P286]?

2: Let \( X(\Gamma) \) be the space obtained by compactifying \( \Gamma \backslash G_1 \) by adjoining cusps, and let \( \Sigma \) be the image of the unit ball in \( L_0^2(\Gamma \backslash G, \chi, \omega) \) under \( \rho(\varphi) \), then we can extend each \( |\rho(\varphi)f| \) to \( X(\Gamma) \) that it vanish at the cusps, by the corollary to item 1 below (15.7.5.7), then \( \Sigma \) is bounded in the \( L^\infty \)-norm by item 1, and it is also equicontinuous, because its derivatives can be bounded uniformly for \( f \):
\[
(X\rho(\varphi)f)(g) = \rho(\varphi X)f(g), \quad \varphi X(g) = \frac{d}{dt}\varphi(\exp(-tX)g)
\]
so the conclusion of item 1 applied to \( \varphi X \)'s shows the uniformly boundedness. Now Arzela-Ascoli shows that \( \Sigma \) is precompact in \( C(X(\Gamma)) \), thus also in \( L^2(X(\Gamma)) \). \( \square \)

Cor. (15.7.5.7). If \( \varphi \in C_c^\infty(G) \), \( f \in L_0^2(\Gamma \backslash G, \chi, \omega) \), then \( \rho(\varphi)f \) is smooth and rapidly decreasing at cusps.

Proof: This is contained in the proof of (15.7.5.6) above, Cf. [Bump, P286]?

\( \square \)

Prop. (15.7.5.8) \([L_0^2(\Gamma \backslash G, \chi, \omega) \text{ Totally Decomposable}] \). The space \( L_0^2(\Gamma \backslash G, \chi, \omega) \) decomposes into a Hilbert space direct sum of irreducible subrepresentations of \( G \), and if \( H \) is such a subrepresentation, then the \( H^{K-\text{fin}} \subset H \) is dense, and \( H^{K-\text{fin}} \in \text{Irr}_{\text{adm}}((g, K)) \) is contained in \( A_0(\Gamma \backslash G, \chi, \omega) \).

Moreover, \( A_0(\Gamma \backslash G, \chi, \omega) \) is just the smooth part of \( L_0^2(\Gamma \backslash G, \chi, \omega) \).
Proof: The proof is exactly the same as that of (15.7.5.2), but where we use (15.7.5.6) in place of (15.16.2.1). Lemma (15.6.4.1) is indispensable.

$H^{K-\text{fin}} \in \text{Irr}^{\text{adm}}((\mathfrak{g}, K))$ by (15.6.4.4). To show it is contained in $A_0(\Gamma \backslash G, \chi, \omega)$, it suffices to show that $H^k \subset A_0(\Gamma \backslash G, \chi, \omega)$ for any $k$. For this, if $0 \neq f \in H_k$, choose by (15.6.4.1) a function $\varphi \in C^\infty_c(G)$ that $\rho(\varphi)f \neq 0$, thus we can assume $\rho(\varphi)(f) = f$ by (15.6.4.1) and (15.16.2.1), as $\dim H^k < \infty$ by (15.6.4.3). Then by (15.7.5.7) $f$ is smooth and decay rapidly, and it is clearly $K$-finite and $Z$-finite, thus $f \in A_0(\Gamma \backslash G, \chi, \omega)$.

The last assertion follows as any cuspidal form decays rapidly thus is contained in $L^2_0(\Gamma \backslash G, \chi, \omega)(15.7.4.7).$

□

Cor. (15.7.5.9)[Finite Multiplicity].

- $L^2_0(\Gamma \backslash G, \chi, \omega) = \bigoplus_\pi \pi^{m(\pi)}$, where for each $\pi$, $m(\pi)$ is finite.
- Let $A(\Gamma \backslash G, \chi, \omega, \lambda)$ be the $\lambda$-eigenspace of $\Delta$ on $A(\Gamma, \chi, \omega)$, and $A(\Gamma \backslash G, \chi, \omega, \lambda, k)$ be the $k$-part in $K$-decomposition of $A(\Gamma \backslash G, \chi, \omega, \lambda)$, and $A_0(\Gamma \backslash G, \chi, \omega, \lambda, k)$ the cuspidal part, then $A_0(\Gamma \backslash G, \chi, \omega, \lambda, k)$ is of f.d.

Proof: 1: Let $(\pi, V)$ be an irreducible unitary representation of $G$, let $k$ be chosen that $V^k \neq 0$, let $0 \neq \xi \in V^k$, then by (15.6.4.1) there is a $\varphi \in C^\infty_c(G)$ that $\pi(\varphi)\xi = \xi$ and $\pi(\varphi)$ is self-adjoint by (15.6.4.1) and (15.16.2.1), as $\dim H^k < \infty$ by (15.6.4.3). Now consider for any continuous linear map $\mathcal{T} : V \to L^2_0(\Gamma \backslash G, \chi, \omega)$, $\mathcal{T}\xi$ lies in the 1-eigenspace of the compact self-adjoint operator $\rho(\varphi)$, which is of $f.d.$ as $\rho(\varphi)$ is compact by (15.7.5.6). Of course, $T$ is determined by $\mathcal{T}\xi$ because $V$ is irreducible, so these $T$ form a f.d. vector space, so the multiplicity is finite.

2: This follows from the first, because by (15.7.5.8) the $K$-finite parts of an irreducible subrepresentation of $L^2_0(\Gamma \backslash G, \chi, \omega)$ are just the space of cuspidal forms contained in it, and $\lambda, k$ determined the action of $\Delta, I$, so there are at most one representation of $G$ that satisfies these, by classification in (15.6.3.34) and (15.6.3.10), and they appear for finite multiplicity by item1, and for each of them, the $k$-part is of $f.d.$, because they are admissible (15.6.4.4). So the conclusion follows. □

Remark (15.7.5.10) [Fundamental Theorem of Harish-Chandra]. In fact, Harish-Chandra showed that for any finite codimensional ideal $J \subset Z$, The subspace $A(\Gamma, \chi, \omega, J)$ of automorphic forms annihilated by $J$ is an admissible $(\mathfrak{g}, K)$-module.

In particular, any irreducible admissible $(\mathfrak{g}, K)$-module $\pi$ appears in $A(\Gamma, \chi, \omega)$ with finite multiplicity.

Thm. (15.7.5.11)[Main Theorem]. Let $\chi(-1) = (-1)^\varepsilon, \varepsilon = 0, 1$, (15.7.5.2) shows the representation $\mathcal{H} = L^2_0(\Gamma \backslash G, \chi)$ decomposes into Hilbert space direct sums of irreducible representations, and $\Delta$ acts as real scalars $\lambda$ on each irreducible subspace (15.6.3.33), and $\mu$ acts by $0$. So comparing the classification of representations of $GL(2, \mathbb{R})(15.6.4.25)$, we can list what representation can appear in it by looking at eigenvalues $\lambda$ of $\Delta$:

- There is only one $f.d.$ irreducible unitary subrepresentation of $G$ occurring in $\mathcal{H}$, the trivial representation.
- If $\lambda \neq \frac{k}{2}(1 - \frac{k}{2})$ for any $k \geq 1 \in \mathbb{Z}$ and $k \equiv \varepsilon \mod 2$, then $\lambda \geq \frac{\varepsilon}{2}(1 - \frac{\varepsilon}{2})$, and this subrepresentation is isomorphic to $P(\lambda, \varepsilon)$. And let $k' \equiv \varepsilon \mod 2$ be any integer, then the multiplicity of $P(\lambda, \varepsilon)$ is equal to the multiplicity of the eigenvalue $\lambda$ of $\Delta_{k'}$ on $L^2(\Gamma \backslash \mathcal{H}, \chi, k')$ because $L^2(\Gamma \backslash \mathcal{H}, \chi, k') \cong L^2(\Gamma \backslash G, \chi, k')$ by (15.7.1.24).
- If $\lambda = \frac{k}{2}(1 - \frac{k}{2})$ for some $k \geq 1 \in \mathbb{Z}$ and $k \equiv \varepsilon \mod 2$, then this subrepresentation is isomorphic to either $D^+(k)$ or $D^-(k)$, and $D^\pm(k)$ have the same multiplicity in $\mathcal{H}$, equal to the dimension $\dim(M_k(\Gamma, \chi))(15.11.1.10)$ of holomorphic modular forms of weight $k$ for $\Gamma$. 

Also if \( k' \equiv \varepsilon \mod 2 \) is any integer \( \geq k \) (resp. \( \leq -k \)), then the multiplicity of \( D^+(k) \) (resp. \( D^-(k) \)) is equal to the multiplicity of the eigenvalue \( \lambda \) of \( \Delta_{k'} \) on \( L^2(\Gamma \backslash \mathcal{H}, \chi, k') \) because \( L^2(\Gamma \backslash \mathcal{H}, \chi, k') \cong L^2(\Gamma \backslash G, \chi, k') \) by (15.7.1.24).

**Proof:** These follow from classification of irreducible representations of \( GL(2, \mathbb{R}) \) (15.6.4.26).

Relation with modular forms: by (15.6.3.28), the multiplicity of \( D^+(k) \) equals the dimension of the \( \frac{k}{2}(1 - \frac{k}{2}) \)-eigenspace of \( \Delta_k \) on \( L^2(\Gamma \backslash \mathcal{H}, \chi, k) \), and any \( f \) in this eigenspace is annihilated by \( L_k \) by (15.7.3.1)(15.7.3.3). But (15.7.3.9) shows the dimension of space of functions annihilated by \( L_k \) equals the dimension of modular forms of weight \( k \). Finally notice that complex conjugation interchanges \( L^2(\Gamma \backslash \mathcal{H}, \chi, k) \) and \( L^2(\Gamma \backslash \mathcal{H}, \chi, -k) \) and \( \overline{\Delta_k} = \Delta_{-k} \) (15.7.3.1), so the multiplicity of \( D^+(k) \) and \( D^-(k) \) equal.

**Eisenstein Series**

**Prop. (15.7.5.12).** Let \( \mathcal{A}^2(\Gamma \backslash G, \chi, \omega) = \mathcal{A}(\Gamma \backslash G, \chi, \omega) \cap L^2(\Gamma \backslash G, \chi, \omega) \), then this is exactly the space of smooth \( K \)-finite \( \mathcal{Z} \)-finite vectors in the discrete spectrum \( L^2_{\text{disc}}(\Gamma \backslash G, \chi, \omega) \).

**Proof:**
15.8 Admissible Representations of $\text{GL}(n)$ over $p$-Adic Number Fields

Main references are [Bum98], [Representation theory of $\text{GL}(n)$ over non-Archimedean local fields, Prasad], [B-Z76], [C.J. Bushnell and P.C. Kutzko, The admissible dual of $\text{GL}(N)$ via compact open subgroups, Princeton university press, Princeton, (1993)].

Notations (15.8.0.1).

- Use notations defined in Classical Representation Theory.
- Let $K$ be a $p$-adic local field or a finite field.
- Use group-theoretic notations as in (15.10.0.2).
- Fix a non-trivial character $\psi$ of $K$ with conductor $p^{-n(\psi)}$.
- Choose the Haar measure $dx$ on $K$ that is self-dual w.r.t. $\psi$ as in (10.9.3.33).
- For $\alpha \in A^{n-1}(K)$, let $\psi_{N,\alpha}$ be a character of $N(K)$ given by $\psi_N(g) = \sum_i \psi(\alpha_i g_{i,i+1})$.

Def. (15.8.0.2) [p-adic Local Fields]. If $K$ is a $p$-adic local field, let $O_K$ the ring of integers in $K$, $p$ the maximal ideal in $O_K$, and $\varpi$ a fixed uniformizer of $p$.

Denote $\mathcal{K} = GL(n,O_K)$, $G_n^0 = \text{det}^{-1}(O^*) \subset GL(n,K)$.

Define subgroups $\text{Unip}_k(n,K)$ of $\text{Unip}(n,K)$ as $\text{Unip}_k(n,K)$ is the group of unipotent matrices that $v(e_{ij}) \geq k(i-j)$. Then $\cup_{k>0} \text{Unip}_k(n,K) = \text{Unip}(n,K)$. In particular, $\text{Unip}(n,K)$ is exhausted by compact open subgroups.

For any character $\chi$ of $O_K^*$, by continuity, there is a minimum $v$ that $c(1+p^v) = 1$, and $p^v$ is called the conductor of $\chi$.

1 Basics


Geometry

Prop. (15.8.1.1). $GL(n,K)$ is unimodular, and the modular function of $B(K)$ is $\Delta_B\begin{bmatrix} x & y \\ z & z \end{bmatrix} = \frac{z}{x}$ by (10.9.1.20). Also denote $\delta = \Delta_B^{-1}$.

Def. (15.8.1.2) [Unramified Quasi-Characters]. A unramified quasi-character on $F$ is a quasi-character $\chi$ that $\chi(O_K^*) = 0$.

Define $\alpha(\chi) = \chi(\varpi)$ if $\chi$ is unramified and 0 otherwise, called the Satake parameter of $\chi$.

Prop. (15.8.1.3) [Diagonal Quasi-Characters]. Let $\chi_1, \ldots, \chi_n$ be quasi-characters of $K^*$, then define two quasi-characters $\chi, \chi'$ on $T(K)$:

$\chi(\text{diag}(y_1, \ldots, y_n)) = \chi_1(y_1) \cdots \chi_n(y_n)$, $\chi'(\text{diag}(y_1, \ldots, y_n)) = \chi_n(y_1) \cdots \chi_1(y_n)$.

When $n = 2$, the quasi-character $\chi$ on $T(K)$ is called regular if $\chi_1 \neq \chi_2$, and dominant if $|\chi_1(\varpi)| < |\chi_2(\varpi)|$. 
**Prop. (15.8.1.5) [Iwasawa Decomposition]**. $GL(n, K) = B(K)\mathcal{K}$, in particular, $B(K)\setminus G$ is compact.

**Proof:** Prove by induction on $n$. $n = 1$ is clear. Given a $g \in GL(n, K)$, we consider its bottom row, and let $x_{nk}$ be the term of minimal multiplicative valuation, then we can right multiply by a permutation matrix $w \in K$ that $x_{nn}$ is of minimal valuation. Now right multiply by a matrix $k$, which is 1 on the diagonal and $k_{ni} = -x_{ni}^{-1}$ on the bottom row, then $k \in K$, and $gk$ has bottom row $e_n$. Thus we can induct and find a $k_0 \in \mathcal{K}$ that $gk_0 \in B(K)$. □

**Prop. (15.8.1.6) [p-adic Cartan Decomposition]**. A complete set of double coset representatives for $\mathcal{K}\setminus GL(n, K)/\mathcal{K}$ consists of diagonal matrices $\begin{bmatrix} a & 0 \\ 0 & b \end{bmatrix}$, $a \leq b \in \mathbb{Z}$.

**Proof:** This follows directly from Smith normal form (11.6.6.7). □

**Cor. (15.8.1.7) [Principal Congruence Subgroups]**. There is a map $\pi : \mathcal{K} \to GL(n, \mathcal{O}_K/(\varpi^n))$, the kernel of which is called the **principal congruence subgroup** of level $m$, denoted by $\mathcal{K}_m$.

**Def. (15.8.1.8) [Partition and Groups]**. Let $\alpha = (n_1, \ldots, n_k)$ be a partition of $n$, define $GL_{\alpha} = GL(n_1) \times \ldots \times GL(n_k)$, $\mathcal{K}_{\alpha} = \mathcal{K} \cap GL_{\alpha}(F)$, $B_{\alpha} = B \cap GL_{\alpha}$, $D_{\alpha} = D \cap GL_{\alpha}$

And for a principal congruence subgroup $\mathcal{K}_m$ of $GL(n, K)$, $\mathcal{K}_m \cap GL_{\alpha}(F)$ is called a principal congruence subgroup of $GL_{\alpha}(F)$.

Denote $U_{\alpha}$ the subgroup of $U_n$ that $a_{ij} = 0$ for $i, j$ in the same segment of $\alpha$ and $i \neq j$. Let $P_{\alpha} = GL_{\alpha} \ltimes U_{\alpha}$ be the parabolic subgroup corresponding to $\alpha$.

For $\beta \ltimes \alpha$, denote $U_\beta(\alpha) = U_\beta \cap GL_{\alpha}$, $P_\beta(\alpha) = P_\beta \cap GL_{\alpha} = GL_\beta \ltimes U_\beta(\alpha)$.

Let $N = \mathcal{K}_m \cap G_{\alpha}$ be a principal congruence subgroup, denote $N_\beta(\alpha) = N \cap U_\beta(\alpha)$, $N_\beta(\alpha) = N \cap U_\beta(\alpha)$, $N_0(\alpha) = N \cap GL_\beta(F)$.

Moreover, define $K_0(\alpha) = \pi^{-1}(B(\mathcal{O}_F/\mathcal{A})), K_1(\alpha) = \pi^{-1}(N(\mathcal{O}_F/\mathcal{A}))$. In particular, $K_0(\mathcal{O})$ are called the **Iwahori subgroup**, a vector is called **Iwahori fixed** if it is $K_0(\mathcal{O})$-fixed.

**Prop. (15.8.1.9) [Iwahori Factorizations]**. If $\mathcal{O} \neq \mathcal{O}$, there are **Iwahori factorizations**

$$K_0(\alpha) = N_-(\alpha)T(\mathcal{O})N(\mathcal{O}), \quad K_1(\alpha) = N_-(\alpha)T(\alpha)N(\mathcal{O})$$

$$N = N_\beta(\alpha)N_0(\alpha)N_\beta(\alpha) = N_\beta(\alpha)N_0(\alpha)N_\beta(\alpha)$$

**Proof:** This is by column and row reduction. Cf. [Bernstein-Zelevinsky 1, P32]. □

**Cor. (15.8.1.10)**. Denote $K_0 = K_0(\alpha)$ or $K_1(\alpha)$, and $T_0 = T(\mathcal{O})$ or $T(\alpha)$ respectively, then we can decompose the Haar measure on $K_0$ as

$$\int_{K_0} \varphi(k)dk = \int_{N_-(\alpha)} \int_{T_0} \int_{N(\mathcal{O})} \varphi(n_{-1}t_0m)dn_0dt_0dm_ = \int_{N_-(\alpha)} \int_{T_0} \int_{N(\mathcal{O})} \varphi(nt_0m_0)dn_0dt_0dm_.$$
Proof: Use \(10.9.1.39\), noticing all groups here are compact. \(\square\)

Cor. (15.8.1.11) [Iwahori-Bruhat Decomposition].

\[
GL(2, K) = B(K)K_0(p) \prod B(K)w_0K_0(p).
\]

? How about the general case?

Proof: By pulling back the Bruhat decomposition of \(GL(2, \mathcal{O}/p)\) to \(\mathcal{K} = GL(2, \mathcal{O})\), we have

\[
\mathcal{K} = K_0(p) \cup K_0(p)w_0K_0(p).
\]

The Iwahori factorization shows \(K_0(p) = (K_0(p) \cap B(K))N_-(p)\). Then this implies

\[
\mathcal{K} = K_0(p) \cup (K_0(p) \cap B(K))w_0K_0(p),
\]

because \(w_0^{-1}N_-(p)w_0 \in K_0(p)\). Then Iwasawa decomposition \(G = BK\) gives the desired result. Notice this decomposition is clearly disjoint. \(\square\)

Prop. (15.8.1.12).

- Any open normal subgroup of \(GL(2, K)\) must contain \(SL(2, K)\).
- If a subgroup of \(GL(2, K)\) contains \(N_\mathbb{K}(K)\) and an open subgroup, then it must contain \(SL(2, K)\).

Proof: 1: this normal subgroup contains \(
\begin{bmatrix}
1 & a \\
1 & 1
\end{bmatrix}
\) for \(|a|\) small enough, and it is also a group, but

\[
\begin{bmatrix}
t \\
t^{-1}
\end{bmatrix}^{-1} \begin{bmatrix}
1 & a \\
1 & 1
\end{bmatrix} \begin{bmatrix}
t \\
t^{-1}
\end{bmatrix} = \begin{bmatrix}
1 & at^{-1} \\
1 & 1
\end{bmatrix},
\]

thus it contains all \(N_\mathbb{K}(K)\). and then by item2 it contains \(SL(2, K)\). Now for any f.d. irreducible smooth representation of \(GL(2, K)\), choose a basis \(v_1, \ldots, v_n\), then there is an open normal subgroup fixing all \(v_i\), thus \(SL(n, F)\) acts trivially on \(V\), and then it factors through \(det : GL(2, K) \to K^\times\), and any irreducible representation of \(K^\times\) is of 1-dimensional by Schur’s lemma, so \(V\) must be 1-dimensional.

2: It contains some matrix that is not upper-triangular, so it contains \(SL(2, K)\) by \((2.1.6.9)\). \(\square\)

Hecke Algebras

Prop. (15.8.1.13) [Spherical Idempotents]. The Hecke algebra \(H_{GL(n, K)}(15.1.4.19)\) has a spherical idempotent \((2.4.4.10)\) \(e_\mathcal{K}\), where the anti-involution is given by transposition.

Then via the correspondence \((15.1.4.23)\), \((\pi, V) \in \text{Ir}_\text{adm}(GL(n, K))\) is called a spherical representation if its corresponding \(H_{GL(n, K)}\)-module is spherical \((2.4.4.11)\). Equivalently, it contains a \(\mathcal{K}\)-fixed vector. And the dimension of spherical vectors is \(\leq 1\) by \((2.4.4.11)\).

Proof: For the invariance of \(H[e_\mathcal{K}]\), notice that \(H[e_\mathcal{K}] = H_\mathcal{K}\) is the subspace of \(\mathcal{K}\)-bi-invariant functions on \(G\), but we have the \(p\)-adic Cartan decomposition \((15.8.1.5)\), so the value of \(\varphi \in H[e_\mathcal{K}]\) are determined by restriction on the diagonal matrices, but they are invariant under transposition. This shows \(e_\mathcal{K}\) is spherical. \(\square\)

Prop. (15.8.1.14) [Transpose Invariant Distribution]. If \(D\) is a distribution on \(GL(n, K)\) that is invariant under conjugation, then it is also invariant under transpose.
**Proposition (15.8.1.15) [Gelfand-Kazhdan]**: If \((\pi, V) \in \text{Irr}^\text{adm}(\text{GL}(n, K))\), then:

- If \(\pi_1\) is defined by \(\pi_1(g) = \pi(g^{-1})\), then \(\pi^\vee \cong \pi_1\).
- Suppose \(n = 2\) and \(\omega\) is the central character of \(\pi\), then if \(\pi_2 = \pi \otimes (\omega^{-1} \circ \text{deg})\), then \(\pi^\vee \cong \pi_2\).

**Proof**: 1: It is clear that the character (15.1.4.34) of a representation is conjugation invariant, thus by (15.8.1.14) it is transpose invariant.

Now the character of \(\pi_1\) is \(\chi_1(\varphi) = \chi(\varphi'')\), where \(\varphi''(g) = \varphi(g^{-1})\), and this equals \(\chi(\varphi')\) where \(\varphi'(g) = \varphi(g^{-1})\), because the character is transpose invariant. It is also clear that \(\varphi' = \pi(\varphi)t\) on a finite space \(V^K\), then \(\tilde{\chi}(\varphi) = \chi(\varphi') = \chi_1(\varphi)\), so by (15.1.4.39) \(\pi \cong \pi_1\).

2: If \(n = 2\), we use further the property that if \(g = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\), then

\[
g^{-1} = (\text{deg } g)^{-1} \begin{bmatrix} d & -b \\ -c & a \end{bmatrix} = (\text{deg } g)^{-1} \begin{bmatrix} 1 \\ -1 \end{bmatrix} g^t \begin{bmatrix} 1 \\ -1 \end{bmatrix}^{-1}
\]

then the assertion is clear using item 1. \(\square\)

**Corollary (15.8.1.16)**: Let \(\pi\) be an admissible representation of \(\text{GL}(n, K)\), then \(\pi\) is irreducible iff \(\pi^\vee\) is irreducible.

**Smooth Representations**

**Definition (15.8.1.17) [Twists]**: Let \((\pi, V) \in \text{Irr}^\text{adm}(\text{GL}(n, K))\), for any quasi-character \(\chi\) of \(K^\times\), denote \(\pi(\chi)\) the representation \(\pi \otimes (\chi \circ \text{det})\). And for \(s \in \mathbb{C}\), denote \(\pi(s)\) the representation of \(\pi\) tensored by the 1-dimensional representation \(g \mapsto |\text{det}(g)|^s\).

**Proposition (15.8.1.18) [Admissible Representation of \(G_m^N(K)\)].** Any non-zero \((\pi, V) \in \text{Rep}^\text{adm}(G_m^N(K))\) contains a 1-dimensional invariant subspace.

**Proof**: Consider the restriction on \(G_m^N(O_K)\), by (15.1.4.32), \(V = \bigoplus_{\chi \in \text{Irr}(O_K)} V_{\chi}\), and \(\dim V_{\chi} < \infty\). As \((1, \ldots, \varpi, \ldots, 1)\) commutes with \(G_m^N(O_F)\), it preserves \(V_{\chi}\) for each \(\chi\). And these elements commute, so they have a common eigenvalue, which means \(V\) has a 1-dimensional invariant subspace. \(\square\)

**Lemma (15.8.1.19)**: Let \((\pi, V) \in \text{Rep}^\text{alg}(\text{GL}(n, K))\), then \(\pi|_{G_m^0}\) splits into a finite direct sum of irreducible representations of \(G_m^0\).

**Proof**: This follows from (15.1.1.24). \(\square\)

**Lemma (15.8.1.20)**: If \((\pi, V) \in \text{Rep}^\text{alg}(\text{GL}(n, K))\) satisfies \(V\) is generated by \(V_{K_m}\), then for any submodule \(V', V'\) is generated by \(V_{N} \cap V'\).

**Proof**: Cf. [B-Z76] P38. \(\square\)

**Proposition (15.8.1.21) [Irreducible Smooth Representation is Admissible]**: For any connected reductive group \(G\) over a \(p\)-adic number field \(F\), \(\text{Irr}^\text{alg}(G(F)) = \text{Irr}^\text{adm}(G(F))\).
Proof: We only prove for $G = \text{GL}(n)$.

By (15.8.2.9)(15.8.2.10) and (15.8.2.8), it suffices to prove for $\pi$ quasi-cuspidal. But then this follows from (15.8.2.12)(15.8.1.19) and (15.1.4.55).

Prop. (15.8.1.22)[Howe]. Let $(\pi, V) \in \text{Rep}^{\text{alg}}(\text{GL}(n, K))$, then $\pi$ is of finite length iff it is admissible and f.g.

Proof: A finite length representation is admissible by (15.8.1.21) and (15.1.4.31). For the converse, as $V$ is f.g., take $N$ compact open s.t. $V$ is generated by $V^N$, and $\dim V^N < \infty$ as $V$ is admissible. Then by (15.8.1.19): $V' \to V' \cap V^N$ is an injection from the set of subrepresentations of $V$ to the set of subspaces of $V^N$, thus $V$ is of finite length.

Finite dimensional Representations

Prop. (15.8.1.23). Any $\pi \in \text{Irr}^{\text{adm}}(\text{GL}(2, K))$ has dimension 1.

Proof: By the no-small-subgroup argument, the kernel of this representation contains an open normal subgroup. But any open normal subgroup of $\text{GL}(2, V)$ contains $\text{SL}(2, V)$ by (15.8.1.12), thus this is a representation of $K^\times$, which must be of 1-dimensional by (15.8.1.18).

Lemma (15.8.1.24)[2-Dimensional Smooth Representation of $K^\times$]. Any $\rho \in \text{Rep}^{\text{adm}, \dim = 2}(K^\times)$ is one of the following form:

- $\rho(t) = \text{diag}(\xi(t), \xi'(t))$, where $\xi, \xi'$ are two quasi-characters of $K^\times$.
- $\rho(t) = \xi(t) \begin{bmatrix} 1 & v(t) \\ 0 & 1 \end{bmatrix}$, where $\xi$ is a quasi-character of $K^\times$.

Proof: There exists a 1-dimensional invariant subspace spanned by $x$ by (15.8.1.18), on which $K^\times$ acts by a quasi-character $\xi$, and consider the quotient space, on which $K^\times$ acts by a quasi-character $\xi'$. Choose $y$ that is linearly-independent of $x$, then $\rho(t)y = \xi'(t)y + \lambda(t)x$, and

$$\lambda(tu) = \xi'(u)\lambda(t) + \lambda(u)\xi(t)$$

which is symmetric in $t, u$.

If $\xi \neq \xi'$,

$$\lambda(t)(\xi(u) - \xi'(u)) = \lambda(u)(\xi(t) - \xi'(t))$$

therefore $\lambda(t) = C(\xi(t) - \xi'(t))$, so $z = y - Cx$ is fixed by $\rho(K^\times)$.

If $\xi = \xi'$, then $\lambda/\xi$ is an additive character of $K^\times$, thus it is trivial on $\mathcal{O}^*$, so $\lambda(t) = cv(t)$.

Zelevinsky Segments

Def. (15.8.1.25) [Zelevinsky Segments]. For $\pi \in \text{Irr}^{\text{adm}}(\text{GL}(n, K))$, a Zelevinsky segment $\Delta(\pi, m)$ is an ordered $m$-tuple $(\pi, \pi(1), \ldots, \pi(m - 1))$ of cuspidal representations of $\text{GL}(n, K)$.

For two segments $\Delta(\pi_1, m)$ and $\Delta(\pi_2, n)$, $\Delta(\pi_1, m)$ precedes $\Delta(\pi_2, n)$ if $\Delta(\pi_1, m) \cap \Delta(\pi_2, n) = \emptyset$ and $(\Delta(\pi_1, m), \Delta(\pi_2, n))$ is another segment. They are called linked segments if one precedes another.

Def. (15.8.1.26) [Dual Segments]. For a segment $\Delta(\pi, m) = (\pi, \pi(1), \ldots, \pi(m - 1))$, its dual segment $\Delta^\vee$ is the segment $(\pi^\vee(1 - m), \pi^\vee(2 - m), \ldots, \pi) = \Delta(\pi^\vee(1 - m), m)$. 

\textbf{Def. (15.8.1.27)} $[\pi(\Delta)]$. Let $\Delta = \Delta(\pi, m)$ be a Zelevinsky segment of length $m$ and degree $mn$, we can define an admissible representation $\pi(\Delta)$ of $GL(mn, K)$ given by

$$\pi(\Delta) = \pi \times \pi(1) \times \ldots \times \pi(m-1) = I_{P(n, n, \ldots, n)}^{GL(mn, K)}(\otimes \pi_i)$$

\textbf{Def. (15.8.1.28)} [Zelevinsky Conditions]. A tuple of Zelevinsky segments $\Delta_1, \ldots, \Delta_r$ is said to satisfy the Zelevinsky condition if for each $i < j$, $\Delta_i$ doesn’t precede $\Delta_j$.

\section{Cuspidal Representations}

\textbf{Jacquet Functors}

\textbf{Def. (15.8.2.1)} [Jacquet Functors]. Let $P = LU$ be a parabolic subgroup of $G$, if $(\pi, V)$ be a representation of $G(F)$, then $V_U = V/(\text{span}\{\rho(u)v - v|u \in U\}) = V/V(U)$ is naturally a $L \cong P/U$ representation, so we can define the \textbf{Jacquet functor}:

$$J^G_P : \text{Rep}^{alg}(G(F)) \rightarrow \text{Rep}^{alg}(L(F)) : V \mapsto V_U.$$ 

Given a character $\psi$ of $U(F)$, similarly $V_{U,\psi} = V/(\text{span}\{\rho(u)v - \psi(u)v|u \in U\}) = V/V(U, \psi)$ is a $Z(K)$-module, we can also define similarly the \textbf{twisted Jacquet functor}

$$J^{G \psi}_P : \text{Rep}^{alg}(G(F)) \rightarrow \text{Rep}^{alg}(Z(K)) : V \mapsto V_{U,\psi}.$$ 

For convenience, define the \textbf{normalized Jacquet functor}: $r^G_P = \sqrt{\frac{\Delta_P}{\Delta_G}} \otimes J^G_P$. $J^G_P, J^{G \psi}_P, r^G_P$ are exact functors, by (15.1.1.17).

\textbf{Prop. (15.8.2.2)}. For the the minimal parabolic subgroup $P = B(K)$, $J_{N, a, N}(V) \cong J_{N, \psi_a, N}(V)$ for $a \in G^{n-1}(F) \times 1$.

\textit{Proof:} This is because $\pi(a)$ maps $V(N, \psi_a, N)$ isomorphically to $V(N, \psi_N, V)$, thus induces an isomorphism $J_{N(K), \psi_a, N}(V) \cong J_{N(K), \psi_N, N}(V)$. 

\textbf{Prop. (15.8.2.3)}. $J^G_P, J^{G \psi}_P, r^G_P$ map smooth representations of finite length to smooth representations of finite length (because it is f.g.).

\textit{Proof:} If $V$ is a f.g. $G$-module, then it is a f.g. $P$-module, because $G = PK$, and $Kv_i$ is of f.d. for any $v \in V$. Thus the quotient $V_U$ of $V$ is also f.g..

For finite length $\lfloor ?, \text{Cf.}[\text{Bernstein-Zelevinsky}2, \text{P}8]$. 

\textbf{Lemma (15.8.2.4)} [Jacquet]. If $(\pi, V)$ is a smooth representation of $GL(n, K)$, then using the notation as in (15.8.1.10), where $\alpha$ is a proper ideal, $V_{K_0}$ and $V_{N^{-\alpha} T_0}$ have the same image in the Jacquet module $J(V)$.

\textit{Proof:} One inclusion is trivial, for the other, if $x \in V_{N^{-\alpha} T_0}$ then $x_1 = \int_{K_0} \pi(k) xdk$ lies in $V_{K_0}$, so it suffices to show $x$ and $x_1$ have the same image in $J(V)$. But by (15.8.1.10)

$$x_1 = \int_{N^{-\alpha}} \int_{T_0} \int_{N(O)} \pi(n t_0 n^-) x dndtn = \int_{N(O)} \pi(n) xdn$$

and notice $p(\pi(n)x) = p(x)$. 

\textit{□}
Prop. (15.8.2.5) [Jacquet Modules are Admissible]. Let \((\pi, V)\) be a smooth representation of \(GL(2, K)\), then

- Using the notation as in (15.8.1.10), if \(\mathfrak{a}\) is a proper ideal, then the projection map \(p : V \rightarrow J(V)\) induces a surjection of \(V^{K_0} \rightarrow J(V)^{T_0}\).

- If \((\pi, V)\) is admissible, then \(J(V)\) is also an admissible representation of \(T(F)\).

Proof: 2 follows from 1 because we can choose \(T_0 = T(\mathfrak{a})\) to be arbitrarily small, then it is of f.d., thus admissible.

For 1, notice that any \(x \in J(V)^{T_0}\) is an image of \(a_1 \in V^{T_0}\), because \(p(\pi(t)x) = \pi(t)p(x) = p(x)\), thus we can choose \(a_1 = \int_{T_0} \pi(t)xdt\).

Thus for any f.d. subspace \(U\) of \(J(V)^{T_0}\), we can find a f.d. \(U \subset V^{T_0}\) that is mapped isomorphically onto \(U\). Now \(U\) is fixed by some \(N_-(p^n)\) for \(n\) large, so \(U\) is fixed by \(N_-(p^n)T_0\). Notice \(\mathfrak{a} = p^m\) for some \(m\), and

\[
\pi(d) N_-(p^n) T_0 \pi(d)^{-1} = N_-(\mathfrak{a}) T_0, \quad d = \begin{bmatrix} \omega^{-m} & \mathbb{1} \\
\frac{1}{\nu} & \frac{1}{\nu}
\end{bmatrix},
\]

so \(\pi(d)U\) is stabilized by \(N_-(\mathfrak{a}) T_0\). Hence by lemma (15.8.2.4), \(\pi(d)p(U) = p(\pi(d)U) \subset p(V^{K_0})\), so the dimension of \(U\) is bounded by dimension of \(V^{K_0}\), so we can choose \(U\) just to be \(J(V)^{T_0}\). Now \(\pi(d)\) commutes with \(T(F)\), so we have \(\pi(d)J(V)^{T_0} = J(V)^{T_0} \subset p(V^{K_0})\). The reverse containment is clear. \(\square\)

**Parabolic Induction**

Def. (15.8.2.6) [Parabolic Induction]. Let \(P = LU\) be a parabolic subgroup of \(G\), let \(pr : P \rightarrow P/U \cong L\), the **parabolic induction** functor \(I_P^G\) is the functor

\[
I_P^G : \text{Rep}^\text{alg}(L) \rightarrow \text{Rep}^\text{alg}(G) : \rho \mapsto \text{Ind}_P^G(\rho \circ pr)(15.1.4.41).
\]

Prop. (15.8.2.7) [Parabolic Induction and Jacquet Functor]. For any parabolic subgroup \(P\), \(I_P^G\) is right adjoint to the normalized Jacquet functor \(r_P^G\).

Proof: For \(\sigma \in \text{Rep}^\text{alg}(L), \rho \in \text{Rep}^\text{alg}(G)\),

\[
\text{Hom}_{P/U}(\sqrt{\Delta_P} \otimes (\text{res}_P^G(\sigma))_U, \rho) \cong \text{Hom}_P(\text{res}_P^G(\sigma), \sqrt{\Delta_P} \otimes (\rho \circ pr)) = \text{Hom}_G(\sigma, \text{Ind}_P^G(\rho \circ pr)).
\]

\(\square\)

Prop. (15.8.2.8). \(I_P^G\) maps admissible representations to admissible representations and maps finite length representations to finite length representations.

Proof: By (15.1.4.51) and Iwasawa decomposition.

For finite length \(\square\).
Cuspidal Representation

Main references are [The Local Langlands Correspondence: The non-Archimedean case, 1994], [Induced Representations of Reductive p-Adic Groups, Berstein Zelevinsky].

Def. (15.8.2.9) [Cuspidal Representations]. $(\pi, V) \in \text{Rep}^{\text{alg}}(G(F))$ is called a quasi-cuspidal representation if for any proper parabolic subgroup $P = LU$ of $G$, $r^P_G(V) = 0$. A cuspidal representation is a representation that is both quasi-cuspidal and admissible. The category of cuspidal representations is denoted by $\text{Rep}^{\text{cusp}}(G(F))$.

Prop. (15.8.2.10) [Cuspidal Dichotomy]. If $\pi \in \text{Irr}^{\text{alg}}(G(F))$, then either $\pi$ is (quasi-)cuspidal, or $\pi$ is a subrepresentation of $I^G_P(\rho)$, where $P = LU$ is a proper parabolic subgroup of $G$, and $\rho \in \text{Irr}^{\text{alg}}(L(F))$ is (quasi-)cuspidal.

Proof: If $\pi$ is not (quasi-)cuspidal, choose a minimal parabolic $P$ that $r^P_G(\pi) \neq 0$. As $r^P_G(\pi)$ is f.g., (15.1.4.50), by (15.1.1.21), it has an irreducible subquotient $\sigma$. Then
\[ 0 \neq \text{Hom}_M(r^P_G\pi, \sigma) = \text{Hom}_G(\pi, I^G_P\sigma). \]
And by minimality, $\sigma$ is (quasi-)cuspidal by (15.8.2.5). □

Prop. (15.8.2.11) [Representation from Finite Case]. Let $(\pi_0, V_0)$ be an irreducible cuspidal representation of $GL(2, F_q)$, then it is representation of $\mathcal{K}$ by the projection $\mathcal{K} \to GL(2, F_q)$, with central character $\omega_0$. Extend $\omega_0$ to a character $\omega$ of $K^\times$, then extend $\pi_0$ to a representation of $\mathcal{K}Z(K)$ with central character $\omega$. Finally let $(\pi, V) = \text{ind}_{\mathcal{K}Z(K)}^{GL(2, K)} \pi_0$. Then $\pi$ is a unitarizable cuspidal irreducible admissible representation of $GL(2, K)$.

Proof: To show it is admissible, we use Mackey’s intertwining formula (15.1.4.50). By (15.1.4.32), it suffices to show for any $\rho \text{Ind}^{\text{adm}}(\mathcal{K})$, $\text{dim} \text{Hom}_\mathcal{K}(\pi_0, \rho) < \infty$. By p-adic Cartan decomposition (15.1.4.50), a representative set for $\mathcal{K}\setminus G/\mathcal{K}Z(K)$ is $\{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \}$, $0 \leq n \in \mathbb{Z}$. Notice $\pi_0$ is of f.d., thus it suffices to show that only f.m. $\text{Hom}_{\mathcal{K}_0(\mathfrak{p}^n)}(\pi_0, \rho^{\omega^n}) \neq 0$. For this, notice that by continuity, for $n$ large, $\rho^{\omega^n}(\begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix}) = \text{id}$ for any $b \in \mathcal{O}$, thus any $\varphi \in \text{Hom}_{\mathcal{K}_0(\mathfrak{p}^n)}(\pi_0, \rho^{\omega^n}) \neq 0$ factors through the Jacquet module of $\pi$, which is 0 as $\pi_0$ is cuspidal.

By (15.1.4.52), $\pi$ is unitarizable. And then by (15.1.4.53), it suffices to show that $\text{dim} \text{End}(\pi) = 1$. By Mackey theory again,
\[ \text{Hom}_G(\pi, \pi) \subset \text{Hom}_G(\pi, \text{Ind}_{\mathcal{K}Z(K)}^{GL(2, K)} \pi_0) = \prod_{n \geq 0} \text{Hom}_{\mathcal{K}_0(\mathfrak{p}^n)}(\pi_0, \rho^{\omega^n}) \]
by the same reason as above, for $n > 0$, this is 0, and for $n = 0$, this has dimension 1 because $\pi_0$ is an irreducible representation of $K$.

It remains to show $\pi$ is cuspidal: Use Mackey theory again. By Iwasawa decomposition, a representative set for $\mathcal{K}\setminus G/\mathcal{K}Z(K)$ is $\{ \begin{bmatrix} 1 & b \\ 0 & 1 \end{bmatrix} \}$, $0 \leq n \in \mathbb{Z}$. Now it suffices to show $\text{Hom}_{\text{Unip}(2, K)}(\pi_0, 1) = 0$. But this is because $\pi_0$ is cuspidal. □

Thm. (15.8.2.12) [Harish-Chandra]. then for $(\pi, V) \in \text{Rep}^{\text{alg}}(GL(n, K))$, the following are equivalent:
• $\pi$ is quasi-cuspidal.
• For any principal congruence subgroup $K_m$, the function $D_{\xi,K} : G \to V : g \mapsto \pi(e_K)\pi(g^{-1})\xi$
  has compact support modulo $Z(K)$.
• Every matrix coefficient of $\pi$ is compactly supported modulo $Z(K)$.
• The restriction of $\pi$ to $G_0$ is compact.

Proof: 2 $\to$ 3 is verbatim as that of (15.1.4.55), 3 $\to$ 4 is easy. 4 $\to$ 2 follows from the definition of compact representations and the fact $GL(n,K)/G_0^0 Z(K)$ is finite.

Cor. (15.8.2.13) [Contragradient of Cuspidal Representations]. For $\pi \in \text{Rep}^{\text{cusp}}(GL(n,K))$, $\hat{\pi} \in \text{Rep}^{\text{cusp}}(GL(n,K))$ too.

3 Whittaker Models

Def. (15.8.3.1) [Whittaker Functionals & Whittaker Models]. For $(\pi,V) \in \text{Irr}^{\text{alg}}(GL(n,K))$,
• a Whittaker functional on $V$ is a $\text{Unip}(n,K)$-map $\lambda : V \to \psi_N$. (Compare with (15.7.4.9).)
• a Whittaker model is a subrepresentation of $\text{Ind}^{GL(n,K)}_{\text{Unip}(n,K)}(\psi_N)$ that is isomorphic to $\pi$ and consists of functions $\varphi$ of moderate growth.

An irreducible smooth representation having a Whittaker functional is called a generic representation.

Remark (15.8.3.2). Generic representations are important because for any global number field $F$ and $\pi \in \text{Irr}^{\text{auto}}(GL(n,F))$, all the local components $\pi_v$ are generic, by (15.10.4.7).

Whittaker models are important because we can use it to attach local Euler factors for such representations.

Prop. (15.8.3.3).
• The definition of generic is independent of $\psi$, by (15.8.2.2).
• $\pi$ is generic iff $\pi^\vee$ is generic.
• For a quasi-character $\chi$ of $K^\times$, $\pi$ is generic iff $\pi(\chi)$ is generic, as $J_{\text{Unip}(n,K),\psi_N}(\pi) = J_{\text{Unip}(n,K),\psi_N}(\pi(\chi))$.

Prop. (15.8.3.4) [Transpose Invariant Distribution]. If $\Delta \in \mathcal{D}(GL(n,K))$ is a distribution that satisfies
$$\lambda(u)\Delta = \psi_N(u)^{-1}\Delta, \quad \rho(u)\Delta = \psi_N(u)\Delta,$$
where $\psi$ is defined in (15.7.4.9), then $\Delta$ is stable under involution $\iota : GL(n,K) \to GL(n,K) : \iota(g) = w^0 g^t w^0$ (15.8.0.1).

Proof: Firstly notice that $\iota$ fixes $N(K)$, and $\psi_N(\iota(g)) = \psi_N(g)$, so $\iota(\Delta)$ also satisfies these equations, so we can replace $\Delta$ by $\Delta - \iota(\Delta)$, then assume $\iota(\Delta) = -\Delta$ and prove $\Delta = 0$.

Consider the group $G$ that is a semi-direct product
$$1 \to N(K) \times N(K) \to G \to F_2$$
and $\iota \in F_2$ acts on $N(K) \times N(K)$ by $(u_1, u_2) \mapsto (\iota(u_2)^{-1}, \iota(u_1)^{-1})$. 

Define a character $\chi$ on $G$ by $\chi((u_1, u_2)) = \psi_N(u_1)^{-1}\psi_N(u_2)$, $\chi(1) = -1$, then $G$ acts on $GL(n, K)$ by

$$\sigma((u_1, u_2)) = \lambda(u_1)\rho(u_2), \quad \sigma(1) = 1$$

then the conditions are summarized into a single condition:

$$\sigma(g)\Delta = \chi(g)\Delta.$$ 

We only prove for $n = 2$.

Consider the action of $N(K) \times N(K)$ on $GL(2, K)$ by left-right action, then we can use (15.1.4.17) and (15.1.4.18), because the action is constructive, by (7.2.1.23), and $i\bar{N(K)}i^{-1} = N(K)$, and $i$ preserves orbits except for diag{$a$, $d$}, $a \neq d$.

But there are no desired distribution on this orbit: this orbit is homeomorphic to $N(K)$ via $u \mapsto u\text{diag}(a, d)$, and the distribution is transferred to a left invariant distribution, thus by (15.1.4.11) it is just the Haar measure

$$\Delta(f) = c_1\int_{N(K)} f\left(\begin{bmatrix} a & b \\ d & c \end{bmatrix}\right)\psi_N(u)du.$$ 

We notice using a right-invariant version of (15.1.4.11) that

$$\Delta(f) = c_2\int_{N(K)} f\left(\begin{bmatrix} a & b \\ d & c \end{bmatrix}\right)\psi_N(u)du = c_2\int_{N(K)} f\left(\begin{bmatrix} a & b \\ d & c \end{bmatrix}\right)\psi_N\left(\begin{bmatrix} a & b \\ d & c \end{bmatrix}^{-1}\right)\left(\begin{bmatrix} a & b \\ d & c \end{bmatrix}\right)du$$

as $N(K)$ is unimodular. Notice now $c_1\psi_N(u) = c_2\psi_N\left(\begin{bmatrix} a & b \\ d & c \end{bmatrix}^{-1}\right)\left(\begin{bmatrix} a & b \\ d & c \end{bmatrix}\right)$ cannot happen for all $u$, as this implies $c_1 = c_2$ by choosing $u = I$, and then $\psi(x) = \psi(ax/d)$, which is impossible by (10.9.3.35). So if some $u$ this is not equal, then we find a function supported at a nbhd of $u$, then this two distributions cannot be equal. \hfill $\Box$

Prop. (15.8.3.5) [Local Multiplicity One Theorem]. For $(\pi, V) \in \text{Irr}^{\text{adm}}(GL(n, K))$, the space of Whittaker functionals has dimension $\leq 1$.

Proof: Define another representation $\pi'(g) = \pi(i(g)^{-1})$, then this representation is isomorphic to $\pi_1$ defined in (15.8.1.15) ($\pi(w^0)$ is an isomorphism), which is isomorphic to the contragradient of $\pi$, so there is a pairing on $V$ that

$$(\pi(g)\xi, \eta) = (\xi, \pi(1)\eta).$$

Now for any smooth functional $\Lambda$, there is an element $[\Lambda]$ that $(\xi, [\Lambda]) = \Lambda(\xi)$.

Now for any linear functional $\Lambda$ on $V$ and $\varphi \in H_G$, we can define another smooth linear function $(\Lambda \ast \varphi)(\xi) = \Lambda(\pi(\varphi)\xi)$. Then clearly $\varphi \ast (\varphi_1 \ast \varphi_2) = (\Lambda \ast \varphi_1) \ast \varphi_2$. We need the following lemma:

Lemma (15.8.3.6).

1. $\pi(g)[\Lambda \ast \varphi] = [\Lambda \ast \rho(1\pi^{-1})\varphi]$.
2. If $L$ is a smooth functional, $[L \ast \varphi] = \pi(\varphi)[L]$.
3. If $L$ is a Whittaker functional, $[\Lambda \ast \lambda(u)\varphi] = \psi_N(u)[\Lambda \ast \varphi]$. 

\hfill $\Box$
Proof: 1:

\[(\xi, \pi(g) [\Lambda * \varphi]) = (\pi(\varsigma(g)) \xi, [\Lambda * \varphi]) = (\Lambda * \varphi)(\pi(\varsigma(g))\xi)\]

\[= \int_G \Lambda(\pi(h)\pi(\varsigma(g))\xi)\varphi(h)dh = \int_G \Lambda(\pi(h)\xi)\varphi(\varsigma(g)^{-1})dh = (\xi, [\Lambda * \rho(\varsigma(g)^{-1})\varphi]).\]

2: \((\xi, [L * \varphi]) = (L * \varphi)(\xi) = L(\pi(\varphi)\xi) = (\pi(\varphi)\xi, [L]) = (\xi, \pi(\varphi)[L]).\)

3:

\[(\xi, [\Lambda * \lambda(u)\varphi]) = (\Lambda * \lambda(u)\varphi)(\xi) = \int_G \Lambda(\pi(g)\xi)\varphi(u^{-1}g)dg\]

\[= \int_G \Lambda(\pi(u)\pi(g)\xi)\varphi(g)dg\]

\[= \psi_N(u)(\Lambda * g)(\xi) = \psi_N(u)(\xi, [\Lambda * \varphi])\]

Now if \(\Lambda_1, \Lambda_2\) are two Whittaker functionals, we will show they are propositional: we define a distribution \(\Delta\) on \(G\) that \(\Delta(\varphi) = \Lambda_1([\Lambda_1 * \varphi])\), then by the lemma above, (15.8.3.4) can be applied to \(\Delta\) so we have \(\Delta = \iota(\Delta)\).

Next we show for any linear functional \(\Lambda, V = \{[\Lambda * \varphi]|\varphi \in H\}\): Notice the RHS is \(G\)-invariant by (15.8.3.6), and it is not empty by smoothness technique. To go further, need another lemma:

Lemma (15.8.3.7). If \(\varphi \in H\) satisfies \(\Lambda_1 * \varphi = 0\), then \(\Lambda_2 * \varphi = 0\).

Proof: Firstly, all \(\Lambda_1 * \pi(g)\varphi = 0\), which follows from (15.8.3.6) item1. Hence,

\[\Lambda_2([\Lambda_1 * \lambda(g)\iota(\varphi)]) = \Delta(\iota(\rho(\iota(g)^{-1})\varphi)) = \Delta(\rho(\iota(g)^{-1})\varphi) = \Lambda_2([\Lambda_1 * \rho(\iota(g)^{-1})\varphi]) = 0.\]

hence by linearity, for any \(\sigma \in H\), \(\Lambda_2([\Lambda_1 * \sigma * \iota(\varphi)]) = 0\), which by (15.8.3.6) item2 is equivalent to \(\Lambda_2(\pi(\varphi)[\Lambda_1 * \varphi]) = 0 = (\Lambda_2 * \varphi)[\Lambda_1 * \varphi]\), because \(\Lambda_1 * \sigma\) is smooth. But we know \([\Lambda * \varphi]\) can be any \(\sigma \in H\), thus \(\Lambda_2 * \varphi = 0\).

By the lemma, we can define a map \(T: V \to V : T([\Lambda_1 * \varphi]) = [\Lambda_2 * \varphi]\), which is a \(G\)-homomorphism by (15.8.3.6), and it is defined on all of \(V\), so \(T\xi = c\xi\) for some \(c\), then we see \(\Lambda_2 = c\Lambda_1\), by a smoothness technique.

Cor. (15.8.3.8) [Local Multiplicity One]. For \((\pi, V) \in \text{Irr}^{\text{alg}}(GL(n, K))\), there exists at most one Whittaker model for \(\pi\).

Proof: A Whittaker model is equivalent to a \(GL(n, K)\)-homomorphism \(V \to \text{Ind}_{\text{Unip}(n, K)}^{GL(n, K)}(C_\psi N)\), which by smooth Frobenius reciprocity (15.1.4.44) is equivalent to a \(N(K)\)-homomorphism \(V \to C_\psi N\), which is just a Whittaker functional. So this proposition is equivalent to (15.8.3.5).

Prop. (15.8.3.9). A Whittaker functional for \((\pi, V)\) is the same as a linear functional on \(J_{\text{Unip}(n, K), \psi N}(V)\).

Cor. (15.8.3.10). For \((\pi, V) \in \text{Irr}^{\text{adm}}(GL(n, K))\), \(\dim J_{\text{Unip}(n, K), \psi N}(V) \leq 1\), by (15.8.3.5).
Existence of Whittaker Models

Def. (15.8.3.11) [Sheaf on $F$ associated to $V$]. As $\text{Unip}(2) \cong \mathbb{A}^1$, any smooth representation $V$ of $\text{Unip}(2, K)$ corresponds to a smooth $H(F)$-module by (15.1.4.23), thus we can view it as a $C^\infty_c(F)$-module by

$$
\varphi(v) = \int_{\text{Unip}(2, K)} \hat{\varphi}(x) \pi(u) v dx.
$$

Then this module is smooth thus non-degenerate by (15.1.4.23), then we can define $S(V)$ the sheaf associated to $V$, as in (15.1.4.7).

Cor. (15.8.3.12). Let $V$ be a smooth $B(K)$-sheaf and let $a \in K$, then the stalk

$$
S(V)_a \cong \begin{cases} 
J(V) & a = 0 \\
J_{\psi_a}(V) \cong J_{\psi}(V) & a \neq 0.
\end{cases}
$$

Proof: By definition (15.1.4.7), the stalk is $V$ modulo the subgroup consisting of elements $v$ that $\chi_U \cdot v = 0$, where $U = a + p^k$ for some large $k$. Back the definition of $S(V)$, consider the Fourier transform

$$
\int_{\text{Unip}(2, K)} \hat{\chi}_{a + p^k}(x) = \int_{\text{Unip}(2, K)} \hat{\psi}(ax) V(p^k) \chi_{p^{n-k}}(x)
$$

where $p^n$ is the conductor of $\psi$. Thus

$$
\int_{\text{Unip}(2, K)} \hat{\chi}_{a + p^k}(x) = C \int_{\text{Unip}(2, K)} \hat{\psi}(ax) \pi \left( \begin{array}{cc} 1 & x \\ 0 & 1 \end{array} \right) v dx = 0
$$

for large $k$, which is equivalent to $v \in V_{N, \psi_a}$ by (15.1.1.19). Finally, $J_{\psi_a}(V) \cong J_{\psi}(V)$ by (15.8.2.2). □

Cor. (15.8.3.13) [Existence of Whittaker Functional]. $(\pi, V) \in \text{Rep}^{\text{adm}}(\text{GL}(2, K))$ has a Whittaker functional unless it factors through the determinant map. In particular, if $\pi$ is irreducible, then dim $J_{\psi}(V) = 1$ iff it is not 1-dimensional, or to say, it is $\infty$-dimensional.

Proof: The existence of a Whittaker functional is equivalent to the fact $J_{\psi}(V) \neq 0$, which is the stalk of the sheaf $S(V)$. If it vanishes, then $S(V)$ is a skyscraper sheaf by (15.8.3.12), and by the correspondence of $S(V)$ and $V$ (15.1.4.7), $V$ equals $\Gamma(F, S(V)) = J(V)$, thus $\text{Unip}(2, K)$ acts trivially on $V$.

So also all the conjugates of $\text{Unip}(2, K)$ acts trivially, so $SL(2, K)$ acts trivially, by 6, thus the representation factors through the quotient $K^\times$, the rest is clear.

Finally, if it is irreducible, then it factors through the determinant map iff $V \cong \mathbb{C}$ and $\pi(g) = \chi(\det(g))$, by (15.8.1.18). So $J_{\psi}(V) = 0$ as $\psi$ is non-trivial. □

Prop. (15.8.3.14) [GL($n$) Case]. In fact, $\pi = Q(\Delta_1, \ldots, \Delta_k) \in \text{Irr}^{\text{adm}}(\text{GL}(n, K))$ is generic iff no two of $\Delta_i$ are linked, in which case

$$
\pi = Q(\Delta_1) \times \ldots \times Q(\Delta_k).
$$

In particular, $\pi$ is generic iff its Gelfand-Kirillov dimension is maximal among those irreducible admissible representations with the same cuspidal supports.

Proof: Cf. [Induced Representations of Reductive $p$-Adic Groups, Zelevinsky (1980)]. □
Kirillov Model

**Def. (15.8.3.15) [Kirillov Model].** For \((\pi, V) \in \text{Irr}^{\text{ad}}(GL(n, K))\), a Kirillov model \(\mathcal{K}(\pi)\) is a subrepresentation of \(\text{Ind}^{\text{Unip}(n, K)}_{N(K)}(\psi)\) that is isomorphic to \(\pi|_{B_1(F)}\), and consist of functions on \(B_1(F)\) that \(\psi\) is compactly supported on \(T_1\) (Notice this condition is automatic by (15.8.3.19)).

When \(n = 2\), it is equivalently a subspace of \(C^\infty(K^\times)\) with an action of \(B_1(F)\) that satisfies
\[
[\pi\left(\begin{bmatrix} a & b \\ 1 & 1 \end{bmatrix}\right)](x) = \psi(bx)\varphi(ax)
\]
and isomorphic to \((\pi, V)\) via the isomorphism \(v \mapsto \varphi_v\).

**Proof:** The last assertion is because \(B_1(F) = \text{Unip}(2, K)T_1(F)\), thus the value of a function in \(\text{Ind}^{B_1(F)}_{N(K)}(\psi)\) is determined by its restriction on \(T_1(F) \cong K^\times\). \(\square\)

**Prop. (15.8.3.16).** The action of \(B_1(F)\) on \(C_c^\infty(K^\times)\) as defined in (15.8.3.15) is irreducible.

**Proof:** Let \(U\) be a non-zero invariant subspace of \(C_c^\infty(K^\times)\), we will show that for any \(a \in K^\times\), \(U\) contains \(\chi_U\) for any sufficiently small nbhd \(U\) of \(a\). Let \(\varphi \in U\) and \(\varphi(b) \neq 0\), then by action of \(\begin{bmatrix} b/a \\ 1 \end{bmatrix}\), we may assume \(\varphi(a) \neq 0\).

If \(f \in C_c^\infty(F)\), \(f\) acts on \(\varphi\) via
\[
\pi(f)\varphi = \int_F f(x)\pi\left(\begin{bmatrix} 1 \\ x \end{bmatrix}\right)\varphi dx,
\]
which in fact a finite sum of elements in \(N(K)\). Then \(\pi(f)\varphi(y) = \int_F f(x)\psi(xy)\varphi(y) dx = \hat{f}(y)\varphi(y)\).
By the isomorphism \(\mathcal{H}_F \cong C_c^\infty(F)\,(15.1.4.26)\), we can choose \(f\) that \(\hat{f} = \varphi(a)^{-1}\chi_U\) for a small nbhd \(U\) of \(a\) that \(\varphi\) is constant on \(U\), then \(\pi(f)\varphi = \chi_U\). \(\square\)

**Lemma (15.8.3.17).** For \((\pi, V) \in \text{Irr}^{\text{ad}}(GL(2, K))\), if \(\dim V = \infty\), then \(V^{\text{Unip}(2, F)} = 0\).

**Proof:** Cf. [Bump, P464]? The stabilizer of \(v\) is open, thus by (15.8.1.12) it is fixed by all \(SL(2, K)\). Also it is fixed by the center \(Z(K)\). Now \(GL(2, K)/SL(2, K)Z(K) \cong K^\times/(K^\times)^2\) which is finite by (12.2.3.5), thus the invariant subspace generated by \(v\) is of f.d., contradiction. \(\square\)

**Lemma (15.8.3.18).** If \((\pi, V) \in \text{Irr}^{\text{ad}}(GL(2, K))\), and \(\Lambda\) is a Whittaker functional on \(V\), then for \(v \neq 0 \in V\), there exists some \(a \in K^\times\) that \(\Lambda(\pi\left(\begin{bmatrix} a \\ 1 \end{bmatrix}\right)v) \neq 0\).

**Proof:** For any \(a \in K^\times\), it is clear that the kernel of the map \(v \mapsto \Lambda(\pi\left(\begin{bmatrix} a \\ 1 \end{bmatrix}\right)v)\) contains \(V_{N, \psi_a}\) but by local multiplicity one (15.8.3.5), \(\dim J_{\psi_a}(V) \leq 1\), and this map is non-trivial because \(\Lambda\) is non-trivial, thus the kernel is exactly \(V_{N, \psi_a}\).

Thus if \(\Lambda(\pi\left(\begin{bmatrix} a \\ 1 \end{bmatrix}\right)v) = 0\), then \(v\) is the section of \(S(V)\) that vanishes at all \(a \neq 0\), thus for any \(x \in F\), \(v' = v - \pi\left(\begin{bmatrix} x \\ 1 \end{bmatrix}\right)v\) vanishes at every \(a \in F\), thus \(v' = 0\). Then \(v = 0\) by (15.8.3.17). \(\square\)
**Prop.(15.8.3.19)** [Kirillov Model and Whittaker Model]. For \((\pi, V) \in \text{Irr}^{\text{adm}}(GL(2, K))\), if it has a Whittaker functional \(\Lambda\), then it has a Whittaker model \(W\) consisting of functions \(W_v(g) = \Lambda(\pi(g)v)\), and we can define functions on \(K^\times\) by

\[
\varphi_v(a) = W_v\left(\begin{bmatrix} a & \cdot \\ 0 & 1 \end{bmatrix}\right).
\]

Then \(G\) acts on \(\mathcal{K}(\pi)\) by acting on the subscript. Then it is a Kirillov model for \(V\), and consists of functions that is compactly supported on \(F\).

Conversely, if \(\{\varphi_v|v \in V\}\) is a Kirillov model for \((\pi, V)\), then we can construct functions on \(GL(2, K)\) by \(W_v(g) = \varphi_{\pi(g)v}(1)\). Then this is a Whittaker model for \(V\).

**Proof:** The equations can be checked by hand. To given an action \(\pi(\varphi_v) = \varphi_{\pi(g)v}\) on \(\{\varphi_v|v \in V\}\), we need to show that \(W_v \mapsto \varphi_v\) is injective, which is true by (15.8.3.18). Then \(v \mapsto \pi_v\) is an isomorphism.

It remains to show that \(\varphi_v \in C_c^\infty(K^\times)\). As \(\pi\) is a smooth representation, for any \(v\), \(W_v\) is stable under \(N(p^k)\) for some \(k\), thus by equation above, \(\varphi_v(a) = \psi_v(n)\varphi_v(a)\) for all \(a\) and \(n \in N(p^k)\). Then if \(|a|\) is sufficiently large, \(\psi_v(n) \neq 0\) for some \(n \in N(p^k)\), implying \(\varphi_v(y) = 0\).

**Prop.(15.8.3.20)** [Kirillov Model and Jacquet Functor]. Let \(V\) be a generic irreducible admissible representation of \(GL(2, K)\), thus having a Kirillov model by (15.8.3.19), thus we can identify \(V\) with a space of functions on \(K^\times\), and there is an exact sequence of vector spaces

\[
0 \to C_c^\infty(K^\times) \to \mathcal{K}(\pi) \to J_{\text{Unip}(2, K)}(\pi) \to 0.
\]

**Proof:** \(V_N\) is generated by elements of the form \(v' = \pi(\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix})v - v\). Notice \(\varphi_{v'}(y) = (\psi(xy) - 1)\varphi_v(y)\), as \(\psi\) is continuous, when \(|y|\) is small, \(\varphi_{v'}(y) = 0\).

To show that if \(C_c^\infty(K^\times) \subset V_N\), notice \(V_N\) is non-zero, because \(\dim V = \infty\) but \(\dim J(V)\) is finite (15.8.4.20). Notice \(V_N\) is stable under \(B(K)\) action, thus it must be \(C_c^\infty(K^\times)\) by (15.8.3.16).

**Prop.(15.8.3.21).** If \((\pi, V)\) is an irreducible generic admissible representation of \(GL(2, K)\) thus having a Kirillov model. If \(\chi\) is a quasi-character of \(T(F)\) that \(\pi(t)\varphi_v = (\delta^{1/2}\chi)(t)\varphi_v \in J(V)\), then for \(|t|\) small, \(\varphi_v(t)\) is a constant multiple of \(|t|^{1/2}\chi_1(t)\).

**Proof:** Let \(t_0 \in p \backslash p^2\), then

\[
\pi(\begin{bmatrix} t_0 \\ 1 \end{bmatrix})\varphi - |t_0|^{1/2}\chi_1(t_0)\varphi \in V_N,
\]

thus by (15.8.3.20), there exists some \(\varepsilon(t_0) > 0\) that

\[
\varphi(tu) - |t|^{1/2}\chi_1(t)\varphi(u) = 0
\]

for \(t = t_0\) and \(|u| \leq \varepsilon(t_0)\). Because both sides are locally constant on \(t\), by the compactness of \(p \backslash p^2\), there exists some \(\varepsilon > 0\) that for the equation is true for all \(t \in p \backslash p^2\) and \(|u| \leq \varepsilon\).

Now any element \(t \in p\) can be factored into product of elements in \(p \backslash p^2\), so by induction this is true for any \(t \in p\). Thus we are done.
15.8. ADMISSION REPRESENTATIONS OF GL(N) OVER P-ADIC NUMBER FIELDS

**Lemma (15.8.3.22) [Gelfand Uniqueness Principle].** Let \((\pi, V) \in \text{Irr}^{\text{adm}}(GL(2, K))\), and let \(\chi\) be a quasi-character of \(K^\times\), then there are at most two essentially different values of \(s\) that there are at least two linear functionals \(L : V \rightarrow \mathbb{C}\) that satisfies

\[
L(\pi(\begin{bmatrix} y & \ast \\ 1 & \ast \end{bmatrix})v) = \chi(y)|y|^sL(v).
\]

**Remark (15.8.3.23).** In fact, for any \(s\), there exists at most one such linear functional \(?\).

**Proof:** If \(\dim V = 1\), this is trivial. Otherwise \(\dim V = \infty\) and \((\pi, V)\) has a Kirillov model. Identify \(V\) with its Kirillov model. Suppose \(L_1, L_2\) are two linear functionals that satisfies the equation, consider their restriction to \(V_N = C_*^\infty(K^\times)\), on which \(B_1(F)\) acts, thus \(L_1, L_2\) are linearly dependent when restricted to \(V_N\) by (15.1.4.12). Thus there exists constants \(c_1, c_2\) that \(c_1L_1 + c_2L_2\) factors through \(J(V)\). \(\dim J(V) \leq 2\) by (15.8.4.20). So by (15.8.1.24) for all but two possible choices of \(s\), \(c_1L_1 + c_2L_2 = 0\), thus there are two linear functionals only for possibly two choices of \(s\). \(\square\)

4 Bernstein-Zelevinsky Classification

**Thm. (15.8.4.1) [Bernstein-Zelevinsky].**
1. For any Zelevinsky segment \(\Delta\) of length \(m\), the representation \(\pi(\Delta)\) has length \(2^{m-1}\).
2. Let \(\Delta\) be a Zelevinsky segment, then \(\pi(\Delta)\) has a unique irreducible subrepresentation \(Z(\Delta)\) and a unique irreducible quotient representation \(Q(\Delta)\).
3. Let \((\Delta_1, \ldots, \Delta_r)\) be a tuple of Zelevinsky segments satisfying the Zelevinsky condition (15.8.1.28), then \(Q(\Delta_1) \times \ldots \times Q(\Delta_r) \in \text{Rep}^{\text{adm}}(GL(\sum n_im_i, F))\) admits a unique irreducible quotient \(Q(\Delta_1, \ldots, \Delta_r)\). Moreover, \(Q(\Delta_1, \ldots, \Delta_r)\) is independent of the order of \(\Delta_1, \ldots, \Delta_r\) (also need to satisfy the Zelevinsky condition).
4. Any irreducible representation \((\pi, V)\) of \(GL(n, K)\) is isomorphic to one of the form \(\pi \cong Q(\Delta_1, \ldots, \Delta_r)\) where \(\Delta_i = \Delta(\pi_i, m_i)\) and \(\sum n_im_i = n\). for a unique tuple of segments \((\Delta_1, \ldots, \Delta_r)\) satisfying Zelevinsky condition up to permutation.
5. Let \((\Delta_1, \ldots, \Delta_r)\) be a tuple of segments satisfying the Zelevinsky condition, then \(Q(\Delta_1, \ldots, \Delta_r)\) is irreducible iff no two elements are linked.
6. \(Q(\Delta_1, \ldots, \Delta_r) = Z(\Delta_1', \ldots, \Delta_r')\).
7. Dual statement of item 3–6 holds for \(Z(\Delta_1) \times \ldots \times Z(\Delta_r)\), which admits a unique irreducible subrepresentation \(Z(\Delta_1, \ldots, \Delta_r)\).

**Proof:**

**Cor. (15.8.4.2) [Principal Series].** \(\mathcal{B}(\chi_1, \chi_2)\) is irreducible except the following two cases:
- If \(\chi_2 = \chi_1(1)\), then \(\mathcal{B}(\chi_1, \chi_2)\) has a 1-dimensional invariant subspace and the quotient representation is irreducible.
- If \(\chi_2 = \chi_1(-1)\), then \(\mathcal{B}(\chi_1, \chi_2)\) has an irreducible invariant subspace of codimension 1.

In these cases, the infinity-dimensional irreducible representations are called the **Steinberg representations** \(\sigma(\chi_1, \chi_2)\), and the one-dimensional representation is denoted by \(Z(\chi_1, \chi_2)\).

**Proof:** Firstly we prove if \(\mathcal{B}(\chi_1, \chi_2)\) has a non-trivial subspace, then it has a non-trivial subspace of dimension 1 or codimension 1: Let \(V'\) be the invariant subspace and \(V''\) the quotient space, by
the exactness of Jacquet functor \((15.8.2.1)\) and \((15.8.3.10)\), at least one of \(J_\psi(V'), J_\psi(V'')\) vanishes. If \(J_\psi(V') = 0\), then by \((15.8.3.13)\) it factors through the determinant map, thus it has a 1-dimensional invariant space. If \(J_\psi(V'') = 0\), then we can use \((15.8.4.9)\) and \((15.1.4.28)\) to dualize.

Next, if \(B(\chi_1, \chi_2)\) has a 1-dimensional subspace \(V = \{f\}\), then \(\pi(g)f = \rho(\det(g))f\) for some quasi-character \(\rho\) of \(K^\times\). Now consider the fact \(f \in B(\chi_1, \chi_2)\), take \(b = \text{diag}(y, y^{-1})\), then \((\delta^{1/2}\chi)(b) = 1\), showing \(\chi_1\chi_2^{-1} = |·|^{-1}\). The codimension 1 case is dual by \((15.1.4.28)\) and \((15.8.4.9)\), so \(B(\chi_1, \chi_2)\) is irreducible except when \(\chi_1\chi_2^{-1} = |·|^{±1}\).

Finally, if \(\chi_1\chi_2^{-1} = |·|^{-1}\), let \(\chi_1 = \chi|·|^{-1/2}\), then \(f(g) = \chi(\det(g))\) is an invariant 1-dimensional subspace, and this is the only 1-dimensional invariant subspace that factors through the determinant map, because if \(f(g) = \chi'(\det(g)) \in B(\chi_1, \chi_2)\), then \(\chi' = \chi_1|·|^{1/2} = \chi_2|·|^{-1/2} = \chi\).

Also the quotient representation is irreducible because the same argument by Jacquet module shows if it is non-irreducible, then it has an invariant subspace of dimension 1 that \(G\) action factors through the determinant map or of codimension 1, which means there are two invariant 1-dimensional subspaces that the \(G\)-action factors through the determinant map, or an invariant subspace of codimension 1 of \(B(\chi_1, \chi_2)\), the latter case contradicting the argument above. For the former case, we get a 2-dimensional subrepresentation of \(B(\chi_1, \chi_2)\) that factors through the determinant map. The argument above shows it is generated by \(\chi(\det())\) and some function \(f\), but \(f\) must satisfy \(f(g) = \chi(\det(g))f(1) + a\), which is possible only if \(a = 0\), so \(f = \chi \circ \det\), contradiction.

The codimension 1 case is dual by \((15.1.4.28)\) and \((15.8.4.9)\).

\begin{proof}
Cor. (15.8.4.3) [Steinberg Representation]. Consider the segment \(\Delta(|·|^{1/n}, n)\) of length \(n\) and degree \(n\), then \((\pi(\Delta), V)\) is the space of functions \(B \setminus G \to \mathbb{C}\). Thus \(Z(\Delta)\) is the trivial representation, and \(Q(\Delta)\) is called the (standard) \textbf{Steinberg representation}, denoted by \(\text{St}_n\). It is self-dual.

If \(n = 2\), then \(\pi(\Delta)\) has length 2, thus there are an exact sequences,

\[0 \to 1 \to |·|^{-1/2} \times |·|^{1/2} \to \text{St}_2 \to 0, \quad 0 \to \text{St}_2 \to |·|^{1/2} \times |·|^{-1/2} \to 1 \to 0\]

\begin{cor}
Cor. (15.8.4.4) [Classification of \(\text{Irr}^{\text{adm}}(GL(2, K))\)]. The \(n = 2\) case is particularly clear: any \(\pi \in \text{Irr}^{\text{adm}}(GL(2, K))\) has the following possibilities:

1. \(\pi\) is cuspidal.
2. \(\pi = Q(\chi)|·|^{-1/2}, \chi|·|^{1/2}\), which equals \(\text{St}_2(\chi)\).
3. \(\pi = \chi_1 \times \chi_2\), where \(\chi_1, \chi_2\) are not linked, which is the principal series.
4. \(\pi = Q(\chi)|·|^{1/2}, \chi|·|^{-1/2}\), which equals \(\text{I}(\chi)\).

\end{cor}

Def. (15.8.4.5) [Cuspidal Supports]. For a \(\pi = Q(\Delta_1, \ldots, \Delta_r) \in \text{Irr}^{\text{adm}}(GL(n, K))\), where \(\Delta_i = (\pi_i, m_i)\), define the \textbf{cuspidal supports} of \(\pi\) as the set

\[\text{Supp}(\pi) = \{\pi_i(j)\}_{1 \leq i \leq r, 1 \leq j \leq m_i - 1}\]

\textbf{Principal Series Representations}

Def. (15.8.4.6) [Principal Series Representations]. Given a diagonal quasi-character \(\chi\) of \(T(F)\), define the \textbf{principal series representation} of \(G\) as

\[B(\chi_1, \ldots, \chi_n) = I_{B(K)}^{G(F)}(\chi)(15.1.4.41) = \{f \in C^\infty(G)|f\left(\begin{array}{cccc}
y_1 \\
\ldots \\
y_n\end{array}\right) = \chi_1(y_1)\cdots\chi_n(y_n)|y_1^{n-1}y_2^{n-3}\cdots y_n^{n+1}|^{1/2}\}\]
It is admissible of finite length by (15.8.2.8). If it is irreducible, its isomorphism class is denoted by \( \pi(\chi_1, \chi_2) \).

**Lemma (15.8.4.7).** By (15.1.4.48), we have a map \( P : C^\infty_c(G(F)) \to B(\chi_1, \ldots, \chi_n) \):

\[
(P\varphi)(g) = \int_{B(K)} \varphi(b^{-1}g)(\delta^{1/2}\chi)(b)db
\]

Then this map is intertwining and surjective. Moreover, we have

\[
P(\lambda(b)^{-1}\varphi) = (\delta^{-1/2}\chi)(b)P(\varphi), \quad b \in B(K)
\]

**Prop. (15.8.4.8).** The representation \( B(\chi_1, \ldots, \chi_n) \) admits at most one Whittaker functional. In other words, \( \dim J_\varphi(B(\chi_1, \ldots, \chi_n)) \leq 1 \). in fact, it is exactly one, as will be shown by (15.8.4.2) and (15.8.3.13).

**Proof:** Let \( \Lambda : V \to \mathbb{C} \) be a Whittaker functional, then we define a distribution \( \Delta \) on \( GL(2, K) \) as \( \Delta(\varphi) = \Lambda(P\varphi) \). Then

\[
\lambda(b)\Delta = (\delta^{-1/2}\chi)(b)\Delta, \quad b \in B(K), \quad \rho(n)\Delta = \psi_N(n)^{-1}\Delta, \quad n \in N(K)
\]

by (15.8.4.7). Because \( P \) is surjective (15.8.4.7), it suffices to show that these \( \Delta \) are unique up to scalar.

Consider the left-right action of \( B(K) \times N(K) \) on \( G(F) \), then there are \( n! \) orbits \( B(K)WN(K) \) by Bruhat decomposition (11.6.6.6). For \( w \neq 1 \), the orbit \( B(K)wN(K) \) is isomorphic to \( B(K) \times N(K) \) via \( (b, n) \mapsto bwn^{-1} \), thus the restriction of \( \Delta \) on \( B(K)wN(K) \) must be of the form

\[
\Delta_1(\varphi) = C \int_{B(K)} \int_{N(K)} \varphi(bwn^{-1})\psi_N(n)(\delta^{1/2}\chi^{-1})(b)dbdn
\]

by (15.1.4.11). This is the unique map that satisfies the condition.

As for the distribution on \( B(K) \), the same reasoning shows the restriction of \( \Delta \) on \( B(K) \) must be of the form

\[
\Delta_2(\varphi) = C \int_{B(K)} \varphi(b)(\delta^{1/2}\chi^{-1})(b)db,
\]

but it satisfies \( \rho(n)\Delta_2 = \Delta_2 \), so there are no distribution on \( B(K) \). Finally, (15.1.4.3) gives us the result. \( \square \)

**Cor. (15.8.4.9).** The contragradient of \( \chi_1 \times \ldots \times \chi_n \) is \( \chi_1^{-1} \times \ldots \times \chi_n^{-1} \).

**Proof:** If \( f \in B(\chi_1, \chi_2) \), \( f' \in B(\chi_1^{-1}, \chi_2^{-1}) \), then the pairing \( \langle f, f' \rangle = \int_K f(k)f'(k)dk \) is \( G \)-invariant by (10.9.1.45), so this defines a smooth functional \( l_f \), and it is non-degenerate, the mapping \( f' \mapsto l_f \) is injective (by letting \( f = 1/f' \) on a \( B(K) \)-orbit that \( f' \) is non-zero) from \( B(\chi_1^{-1}, \chi_2^{-1}) \) to \( B(\chi_1, \chi_2)^\vee \).

Now by symmetry the other side is also injective, and we are done because \( (V_1^\vee)^\vee = \cong V(15.1.4.30). \) \( \square \)

**Cor. (15.8.4.10).** \( \text{Hom}(B(\chi_1, \ldots, \chi_n), B(\mu_1, \ldots, \mu_n)) \neq 0 \) only if \( \{\chi_1, \ldots, \chi_n\} = \{\mu_1, \ldots, \mu_n\} \).

**Proof:** By smooth Frobenius reciprocity (15.1.4.44),

\[
\text{Hom}_G(B(\chi_1, \chi_2), B(\mu_1, \mu_2)) \cong \text{Hom}_{B(K)}(B(\chi_1, \chi_2), \delta^{1/2}\mu).
\]
The proof below is similar to that of (15.8.4.8): For such a map \( \Lambda \), we define a distribution \( \Delta(\varphi) = \Lambda(P(\varphi)) \), then
\[
\lambda(b)\Delta = (\delta^{-1/2}\chi)(b)\Delta, \quad \rho(b)\Delta = (\delta^{-1/2}\mu^{-1})(b)\Delta, \quad b \in B(K).
\]
So by the exact sequence (15.1.4.3), such distribution exists on one of the orbits \( B(K)wN(K) \).
If such a distribution exists on \( B(K)wN(K) \) for \( w \neq 1 \), then noticing \( \rho(n)\Delta = \Delta \) for \( n \in N(K) \), by (15.1.4.11)
\[
\Delta(\varphi) = \int_{B(K)} \int_{N(K)} \varphi(bwn^{-1})(\delta^{1/2}\chi^{-1})(b)dbdn,
\]
then we apply \( \rho(t) \) with \( t \) diagonal, then
\[
(\delta^{-1/2}\mu^{-1})(t)\Delta(\varphi) = (\rho(t)\Delta)(\varphi) = \int_{N(K)} \int_{B(K)} \varphi((bwt^{-1}w^{-1})w(tnt^{-1})^{-1})(\delta^{1/2}\chi^{-1})(b)dbdn
\]
\[
= \delta(t)^{-1}(\delta^{-1/2}\chi^{-1})(wtw^{-1})\Delta(\varphi)
\]
via change of variables (10.9.1.16). Notice that \( \delta(t) = \delta(wtw^{-1})^{-1} \), thus \( \mu(t) = \chi(wtw^{-1}) \), which means \( \chi_i = \mu_{w(i)} \).
Similarly, if such a distribution exists on \( B(K) \), then
\[
\Delta(\varphi) = \int_{B(K)} \varphi(b)(\delta^{1/2}\chi^{-1})(b)db.
\]
Apply \( \rho(b) \), then \( \delta^{-1/2}\chi(b) = (\delta^{-1/2}\mu)(b) \), so \( \chi_i = \mu_i \).

\[\square\]

**Intertwining Integrals and Whittaker Functional**

**Prop. (15.8.4.11)**[Intertwining Integral]. Let \( \xi_i \) be two characters of \( K^\times \), and \( \chi_i = |\cdot|^s_i\xi_i \), \( (\pi, V) = B(\chi_1, \chi_2), (\pi', V') = B(\chi_2, \chi_1) \). Define for \( f \in V \),
\[
Mf : GL(2, K) \to \mathbb{C} : Mf(g) = \int_{N(K)} f(w_0ug)du
\]
then if \( \text{Re}(s_1 - s_2) > 0 \), the integral is absolutely convergent, \( Mf \in V' \), and \( M \) is a nonzero intertwining, so \( V \cong V' \) if they are both irreducible.

**Proof:** Should compare this proof with (15.6.4.18).

For the convergence, it suffices to check for \( \begin{bmatrix} 1 & x \\ -1 & 1 \end{bmatrix} \), \(|x| \) large, but then
\[
f(\begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} g) = f(\begin{bmatrix} x^{-1} & -1 \\ x^{-1} & 1 \end{bmatrix} g) = |x|^{-1}(\chi_1^{-1}\chi_2)(x)f(\begin{bmatrix} 1 & -1 \\ x^{-1} & 1 \end{bmatrix} g)
\]
and because \( f \) is locally constant, when \(|x| \) is large, \( f(\begin{bmatrix} 1 & -1 \\ x^{-1} & 1 \end{bmatrix} g) = f(g) \), thus the convergence on the unbounded region is dominated by
\[
\int_{|x| > q^N} |x|^{-1}|(\chi_1^{-1}\chi_2)(x)|dx = \int_{|x| > q^N} |x|^{-s_1+s_2-1}dx,
\]
which converges for \( \text{Re}(s_1 - s_2) > 0 \).

To show \( Mf \in V' \), we need to check

\[
Mf\left( \begin{bmatrix} 1 & x \\ 1 \\ \end{bmatrix} \right) g = Mf(g), \quad Mf\left( \begin{bmatrix} y_1 \\ y_2 \\ \end{bmatrix} \right) g = |y_1/y_2|^{1/2} \chi_2(y_1) \chi_1(y_2) Mf(g).
\]

The first is trivial and for the second:

\[
Mf\left( \begin{bmatrix} y_1 \\ y_2 \\ \end{bmatrix} \right) g = \int_F f\left( \begin{bmatrix} y_2 \\ y_1 \\ \end{bmatrix} \right) \left[ \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \right] g dx
\]

so it is clear.

Finally \( M \) is clearly intertwining, and it is not trivial by looking at the function \( f \):

\[
f = |y_1/y_2|^{1/2} \chi_1(y_1) \chi_2(y_2) \chi_{O_F}(x), \quad \text{where } g = \left[ \begin{bmatrix} y_1 \\ y_2 \\ \end{bmatrix} \right] \left[ \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \right]
\]

and vanish if \( g \in B(K) \). Notice the representation of \( g \) is unique by Bruhat decomposition. Then \( Mf(1) = 1 \). \( \square \)

**Prop. (15.8.4.12) [Analytic Continuation of Intertwining Integral].** Let \( \xi_i \) be two characters of \( K^* \), \( \chi_i = |\cdot|^{s_i} \xi_i \), \( (\pi_{s_1,s_2}, V_{s_1,s_2}) = B(\chi_1, \chi_2), (\pi'_{s_1,s_1}, V'_{s_2,s_1}) = B(\chi_2, \chi_1) \).

Notice that by Iwasawa decomposition (15.8.1.4), an arbitrary \( f \in B(\chi_1, \chi_2) \) is determined by its restriction on \( K \), and if a function \( f_0 \) on \( K \) satisfies

\[
f_0\left( \begin{bmatrix} y_1 \\ y_2 \\ \end{bmatrix} \right) g = \xi_1(y_1) \xi_2(y_2) f_0(k), \quad y_1, y_2 \in O^*,
\]

then \( f_0 \) can extends uniquely to an element \( f_{s_1,s_2} \in V_{s_1,s_2} \) for any \( s_1, s_2 \), called the flat sections of \( f_0 \).

Then the intertwining integral \( Mf_{s_1,s_2} \) defined in (15.8.4.11) is analytic for the dominant \( \chi \) in the flat family, and has an analytic continuation to all \( s_1, s_2 \) that \( \chi_1 \neq \chi_2 \), and defines a nonzero operator \( V_{s_1,s_2} \rightarrow V'_{s_2,s_1} \).

**Proof:** The proof is parallel to that of (15.8.4.11).

\[
Mf_{s_1,s_2}(g) = \int_{|x| \leq q^N} f_{s_1,s_2}\left( \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix} \right) g dx + \int_{x \geq q^{N_1+1}} |x|^{-s_1+s_2-1} \left( \xi_1^{-1} \xi_2 \right)(x) dx f_{s_1,s_2}(g)
\]

the first term can easily be extended, and the second term vanishes if \( \xi_1^{-1} \xi_2 \) ramifies, and equals something like a multiple of \( \left( \frac{\chi_1^{-1} \chi_2(\omega)}{1-\chi_1^{-1} \chi_2(\omega)} \right)^{N_1+1} \), which extends unless \( \chi_1 = \chi_2 \).

For the intertwining property, it is because equalities maintain along analytic continuation, in particular, it is non-trivial as \( Mf_{s_1,s_2}(1) = 1 \). \( \square \)

**Cor. (15.8.4.13).** \( Z(\chi_1, \chi_2) \cong Z(\chi_2, \chi_1) \), \( \sigma(\chi_1, \chi_2) \cong \sigma(\chi_2, \chi_1) \). If \( B(\chi_1, \chi_2) \) is irreducible, then \( \pi(\chi_1, \chi_2) \cong \pi(\chi_2, \chi_1) \). Moreover, there are no other isomorphisms between these representations.

**Proof:** It suffices to show there are no other isomorphisms, and this is by (15.8.4.10). \( \square \)
Prop. (15.8.4.14) [Whittaker functional of $\mathcal{B}(\chi_1, \chi_2)$]. There is a Whittaker functional on $\mathcal{B}(\chi_1, \chi_2)$ defined by

$$\Lambda(f) = \int_{\mathbb{F}} f(w_0 \begin{bmatrix} 1 & x \\ 1 & \end{bmatrix}) \psi(-x) dx.$$ 

This integral is absolutely convergent if $\chi$ is dominant and is analytic for the flat family of $\chi$, by method the same as in the proof of (15.8.4.11). And this can also be extended to all $\chi$ (as flat section (15.8.4.12)) by defining

$$\Lambda(f) = \lim_{k \to \infty} \int_{\mathbb{P}^{k-1} \backslash \mathbb{P}^{k}} f(w_0 \begin{bmatrix} 1 & x \\ 1 & \end{bmatrix}) \psi(-x) dx.$$ 

Remark (15.8.4.15). Compare with (15.10.4.3).

Proof: This makes sense because it stabilize as $k \to \infty$: when $k$ is large,

$$\int_{\mathbb{P}^{k-1} \backslash \mathbb{P}^{k}} f(w_0 \begin{bmatrix} 1 & x \\ 1 & \end{bmatrix}) \psi(-x) dx = q^{-k-1} f(1) \int_{\mathbb{P}^{k-1} \backslash \mathbb{P}^{k}} \psi(-x)(\chi_1^{-1} \chi_2)(x) dx$$

By continuity (See the proof of (15.8.4.11)). If $\psi(t) \neq 0$, choose $k$ large that $\chi_1^{-1} \chi_2(x) = \chi_1^{-1} \chi_2(x + t)$ for any $x \in \mathbb{P}^{k-1} \backslash \mathbb{P}^{k}$, thus this integral vanishes.


Prop. (15.8.4.17). If $\mathcal{B}(\chi_1, \chi_2)$ is irreducible, with the notations in (15.8.4.11), the intertwining integral $M : \mathcal{B}(\chi_1, \chi_2) \to \mathcal{B}(\chi_2, \chi_1)$ satisfies

$$\Lambda' \circ M = \xi_1 \xi_2^{-1} (1)(1 - s_1 + s_2, \xi_1^{-1} \xi_2, \psi) \Lambda,$$

where $\Lambda$ is the Whittaker functional defined in (15.8.4.14), and $\gamma(s, \chi, \psi)$ is the local constant defined in (16.2.2.8).

Proof: Cf. [Bump, P485].

Cor. (15.8.4.18) [Composition of Intertwining Integrals]. If $\mathcal{B}(\chi_1, \chi_2)$ is irreducible, $M : \mathcal{B}(\chi_1, \chi_2) \to \mathcal{B}(\chi_2, \chi_1), M' : \mathcal{B}(\chi_2, \chi_1) \to \mathcal{B}(\chi_1, \chi_2)$ are intertwining integrals, then $M' \circ M$ is the scalar $\gamma(1 - s_1 + s_2, \xi_1^{-1} \xi_2, \psi) \gamma(1 + s_1 - s_2, \xi_1 \xi_2^{-1}, \psi)$.

If $\mathcal{B}(\chi_1, \chi_2)$ is reducible, $M' \circ M = 0$.

Proof: The irreducible case follows from the proposition. For the reducible case, let $\chi_1 \chi_2^{-1} = | \cdot |$, the intertwining integral $\mathcal{B}(\chi_2, \chi_1) \to \mathcal{B}(\chi_1, \chi_2)$ is non-zero, so the image is either $\mathcal{B}(\chi_1, \chi_2)$ or $\pi(\chi_1, \chi_2)$. In the first case, $\mathcal{B}(\chi_2, \chi_1)$ has a infinite dimensional proper quotient, contradiction. The intertwining integral $\mathcal{B}(\chi_1, \chi_2) \to \mathcal{B}(\chi_2, \chi_1)$ is non-zero, so the image is either $\mathcal{B}(\chi_2, \chi_1)$ or $\pi(\chi_1, \chi_2)$. In the first case, $\mathcal{B}(\chi_1, \chi_2)$ has a 1-dimensional quotient, contradiction.
Jacquet Module

Prop. (15.8.4.19) [Jacquet Module of \( B(\chi_1, \ldots, \chi_n) \)]. Let \( \chi_i \) be quasi-characters of \( K^\times \), then the Jacquet module of \( \chi_1 \times \ldots \times \chi_n \) has dimension \( n! \).

And if \( n = 2 \), the representation of \( T(F) \) on the Jacquet module is isomorphic to the representation

\[
t \mapsto \begin{cases} 
\left[ (\delta^{1/2} \chi)(t) \right], & \chi_1 \neq \chi_2 \\
\left[ \begin{array}{c} (\delta^{1/2} \chi')(t) \\ 1 \\
v(t_1/t_2) \\
1 \end{array} \right], & \chi_1 = \chi_2 = \chi
\end{cases}
\]

Proof: Firstly we show \( \dim J(B(\chi_1, \chi_2)) = 2 \): Let \( \Lambda : V \to C \) be a functional that \( \Lambda(\rho(n)v) = \Lambda(v) \) for \( n \in N(K) \), then we define a distribution \( \Delta \) on \( GL(2, K) \) as \( \Delta(\varphi) = \Lambda(P\varphi) \). Then

\[
\lambda(b)\Delta = (\delta^{-1/2} \chi)(b)\Delta, b \in B(K), \quad \rho(n)\Delta = \Delta, n \in N(K)
\]

by (15.8.4.7). Because \( P \) is surjective (15.8.4.7), it suffices to show that there are exactly two linearly independent such \( \Delta \).

Consider the left-right action of \( B(K) \times N(K) \) on \( GL(2, K) \), then there are \( n! \) orbits \( B(K)wN(K) \) by Bruhat decomposition (11.6.6.6). For \( w \neq 1 \), the orbit \( B(K)wN(K) \) is isomorphic to \( B(K) \times N(K) \) via \( (b, n) \mapsto bwn^{-1} \), thus the restriction of \( \Delta \) on it must be of the form

\[
\Delta_1(\varphi) = C \int_{B(K)} \int_{N(K)} \varphi(bwn^{-1})(\delta^{1/2} \chi^{-1})(b)dbdn
\]

by (15.1.4.11).

As for the distribution on \( B(K) \), the same reasoning shows the restriction of \( \Delta \) on \( B(K) \) must be of the form

\[
\Delta_2(\varphi) = C \int_{B(K)} \varphi(b)(\delta^{1/2} \chi^{-1})(b)db,
\]

and it truly satisfies \( \rho(n)\Delta_2 = \Delta_2 \). Finally, (15.1.4.3) gives us the result.

Next we consider \( J(V) \) as a 2-dimensional \( T(F) \)-representation must be of the two forms in (15.8.1.24), it suffices to distinguish these two cases.

Denote \( V = B(\chi_1, \chi_2) \). Consider for any quasi-character \( \mu \) of \( T(F) \),

\[
\text{Hom}_{T(F)}(J(V), \delta^{1/2}\mu) \cong \text{Hom}_{B(K)}(V, \delta^{1/2}\mu) \cong \text{Hom}_{GL(2, K)}(V, B(\mu_1, \mu_2))
\]

So (15.8.4.10) can be used, so if \( \chi_1 \neq \chi_2 \), there are two \( \mu \) that can make the Hom group non-vanish, so it is the first case. If \( \chi_1 = \chi_2 \), then \( V \) is irreducible, and there is only one \( \mu \) that makes this Hom group non-vanish, and the Hom group is of dimension 1 by Schur’s lemma, so it is the second case. \( \square \)

Prop. (15.8.4.20) [Jacquet Module is Finite Dimensional]. For \( (\pi, V) \in \text{Irr}^{\text{adm}}(GL(n, K)) \), \( \dim J_{\text{Unip}(n, K)}(V) \leq n! \), and if it is nonzero, then \( \pi \) is a subrepresentation of some \( B(\chi_1, \ldots, \chi_n) \).

Proof: By (15.8.2.10), \( \pi \) is isomorphic to a subrepresentation of some \( B(\chi_1, \ldots, \chi_n) \). Then by exactness of Jacquet functor (15.8.2.1), \( J(V) \) is a subspace of \( J(B(\chi_1, \ldots, \chi_n)) \), which has dimension \( n!(15.8.4.19) \). \( \square \)
Prop. (15.8.4.21) [Jacquet Functor of $\sigma(\chi_1, \chi_2)$]. Suppose $\chi_1, \chi_2$ are characters of $K^\times$ that $\chi_1\chi_2^{-1} = |\cdot|^{-1}$, then $\mathcal{B}(\chi_1, \chi_2)$ is reducible, then the Jacquet modules of $\pi(\chi_1, \chi_2)$ and $\sigma(\chi_1, \chi_2)$ are 1-dimensional, and the characters of $T(F)$ they afford are $\delta^{1/2}\chi$ and $\delta^{1/2}\chi'$.

Proof: Clearly the Jacquet module of a representation $\mathbb{1}(\chi)$ is of dimension 1, so by the exactness of Jacquet functor (15.8.2.1) and (15.8.4.19), the Jacquet functor for $\sigma(\chi_1, \chi_2)$ is also of dimension 1.

For the determination of the Jacquet module, notice for any representation $(\pi, V)$ of $GL(2, K)$,

$$\text{Hom}_{T(F)}(J(V), \delta^{1/2}\mu) \cong \text{Hom}_{B(K)}(V, \delta^{1/2}\mu) \cong \text{Hom}_{GL(2, K)}(V, \mathcal{B}(\mu_1, \mu_2)).$$

So for $\pi = \pi(\chi_1, \chi_2)$, $\text{Hom}_{T(F)}(J(V), \delta^{1/2}\mu) = C$ for $\mu = \chi$, so $J(\pi(\chi_1, \chi_2))$ is $\delta^{1/2}\chi$. For $\pi = \sigma(\chi_1, \chi_2)$, then $\text{Hom}_{T(F)}(J(V), \delta^{1/2}\mu) = C$ for $\mu = \chi'$ by (15.8.4.13), so $J(\sigma(\chi_1, \chi_2))$ is $\delta^{1/2}\chi'$.

Kirillov Modules of Principal Series

Prop. (15.8.4.22) [Kirillov Model of Principal Series]. Let $\pi(\chi_1, \chi_2)$ be an irreducible principal series,

- If $\chi_1 \neq \chi_2$, then the Kirillov model of $\pi(\chi_1, \chi_2)$ consists of smooth functions $\varphi$ on $K^\times$ that is compactly supported on $F$ and $\varphi(t)$ is a linear combination of the function $|t|^{1/2}\chi_1(t)$ and $|t|^{1/2}\chi_2(t)$ when $|t|$ is small.

- If $\chi_1 = \chi_2$, then the Kirillov model of $\pi(\chi_1, \chi_1)$ consists of smooth functions $\varphi$ on $K^\times$ that is compactly supported on $F$ and $\varphi(t)$ is a linear combination of the function $|t|^{1/2}\chi_1(t)$ and $|t|^{1/2}\chi_1(t)$ when $|t|$ is small.

Proof: First assume that $\chi_1 = \chi_2$, then by (15.8.4.19), there are two functions $\varphi_1, \varphi_2$ that satisfies

$$\pi(t)\bar{\varphi}_1 = (\delta^{1/2}\chi)(t)\bar{\varphi}_1, \quad \pi(t)\bar{\varphi}_2 = (\delta^{1/2}\chi)(t)\bar{\varphi}_2 + v(t_1/t_2)(\delta^{1/2}\chi)(t)\bar{\varphi}_1.$$

Then by (15.8.3.21), $\varphi_1(u) = C|u|^{1/2}\chi_1(u)$ for $|u|$ small, and because $\varphi_1 \neq 0 \in J(V)$, $C \neq 1$ by (15.8.3.20), and we can assume that $C = 1$. Then for any $t_0 \in \mathfrak{p}\backslash\mathfrak{p}^2$,

$$\pi(t_0)\varphi_2 - |t_0|^{1/2}\chi_1(t_0)[\varphi_1 + \varphi_2] \in V_N.$$

Thus by (15.8.3.20), there exists some constant $\varepsilon(t_0)$ that

$$\varphi_2(tu) = |t|^{1/2}\chi_1(t)\varphi_2(u) + |tu|^{1/2}\chi_1(tu).$$

is true for $t = t_0$ and $|u| \leq \varepsilon(t_0)$. Notice both sides are locally constant on $t$, so this is true for $t$ near $t_0$. Because $\mathfrak{p}\backslash\mathfrak{p}^2$ is compact, there is a $\varepsilon$ that this is true for any $t \in \mathfrak{p}\backslash\mathfrak{p}^2$ and $|u| \leq \varepsilon$.

Now any element $t \in \mathfrak{p}$ can be factored into product of elements in $\mathfrak{p}\ \mathfrak{p}^2$, so by induction

$$\varphi_2(tu) = |t|^{1/2}\chi_1(t)\varphi_2(u) + v(t)|tu|^{1/2}\chi_1(tu).$$

for any $t \in \mathfrak{p}$ and $|u| \leq \varepsilon$. So the theorem is true for $\varphi_1$ and $\varphi_2$, thus true for any other function because they differs from a linear combination of these two by an element in $V_N$, which vanishes for $|t|$ small, by (15.8.3.20).

Case 1 is similar and easier.

Prop. (15.8.4.23) [Kirillov Model of Steinberg Representations]. Let $\sigma(\chi_1, \chi_2)$ be a Steinberg representation of $GL(2, K)$, where $\chi_1\chi_2^{-1} = |\cdot|^{-1}$, then the Kirillov model of $\sigma(\chi_1, \chi_2)$ consists of smooth functions $\varphi$ on $K^\times$ that is compactly supported on $F$ and $\varphi(t)$ is a constant multiple of $|t|^{1/2}\chi_2(t)$ when $|t|$ is small.

Proof: The proof is the same as that of (15.8.4.22), with (15.8.4.21) used instead of (15.8.4.19).
5 Spherical Representations

Def. (15.8.5.1) [Normalized Spherical Vector]. Let $\chi_1, \ldots, \chi_n$ be nonramified quasi-characters of $K^\times$, then $B(\chi_1, \ldots, \chi_n)$ contains a $K$-fixed vector $\varphi_K$ that is defined to be

$$\varphi_K(bk) = (\delta^{1/2}(\chi))(b), b \in B(K), k \in K$$

Notice this is well-defined, because for $u \in B(K) \cap K$, $(\delta^{1/2}(\chi))(u) = 1$. $\varphi_K$ is $K$-spherical, and we refer to it the normalized spherical vector in $V$. Such a $B(\chi_1, \ldots, \chi_n)$ is called an unramified principal series if it is irreducible.

Notice when $n = 2$ and $\chi_2 = \chi_1 \cdot |$, this spherical vector just spans the 1-dimensional invariant subspace in $(15.8.4.2)$.

Prop. (15.8.5.2) [Satake Isomorphism]. There is an isomorphism

$$S : \mathcal{H}_K \cong \mathbb{C}[t_1, t_1^{-1}, \ldots, t_n, t_n^{-1}]^W.$$ s.t. if $\varphi \in \mathcal{H}_K$, for any spherical principal series $\pi(\chi_1, \ldots, \chi_n)$ and a spherical vector $v$, $\pi(\varphi)v = S(\varphi)(\alpha_1, \ldots, \alpha_n)$, where $\alpha_i = \chi(\chi_i)$ are the Satake parameters of $\chi_i$.

Remark (15.8.5.3). For general Satake isomorphism, Cf. (15.13.0.2).

Proof: Cf. [Spherical representations and the Satake isomorphism]?

Cor. (15.8.5.4). When $n = 2$, under the Satake isomorphism, the Hecke operators $T(p) =$ \begin{bmatrix} \varphi \\
1
\end{bmatrix}
and $R_p = \varphi I$ are mapped to

$$q^{1/2}(t_1 + t_2), \quad t_1 t_2,$$

resp.

Proof: For any unramified spherical representation with Satake parameters $\alpha_1, \alpha_2$, using the representative of $\mathcal{H} \begin{bmatrix} \varphi \\
1
\end{bmatrix} \mathcal{H}$ over $\mathcal{H}$ as in (15.11.3.9),

$$(T(p)\varphi_K)(1) = \int_{\mathcal{H}} \begin{bmatrix} \varphi \\
1
\end{bmatrix} \mathcal{H} \varphi_K(g) \, dg = \sum_{\gamma \in K} \begin{bmatrix} \varphi \\
\gamma
\end{bmatrix} K/K \varphi_K(\gamma) = (\Delta^{1/2}(\chi))(\begin{bmatrix} 1 \\
\varphi
\end{bmatrix}) + q(\Delta^{1/2}(\chi))(\begin{bmatrix} \varphi \\
1
\end{bmatrix}) = q^{1/2}(\alpha_1 + \alpha_2)$$

and similarly for $R(p)$.

Cor. (15.8.5.5) [Spherical Representation of $GL(n, K)$]. Every irreducible admissible spherical representation $(\pi, V)$ of $GL(n, K)$ is of the form $Q(\Delta_1, \Delta_2, \ldots, \Delta_n)$ where $\Delta_i = (\chi_i, 1)$, $\chi_i$ are unramified quasi-characters.

Proof: Use the Satake isomorphic to find Satake parameters of unramified quasi-characters $\chi_i$ that makes the representation of $\mathcal{H}_K \cong \mathbb{C}[t_1, t_1^{-1}, \ldots, t_n, t_n^{-1}]^W$ isomorphic to that of $\pi$, then by (2.4.4.3), $\chi_1 \times \chi_2 \times \ldots \times \chi_n$ has a unique irreducible subquotient that has the same spherical character as $\pi$, then by (2.4.4.12), this subquotient is isomorphic to $\pi$. Now use the fact we can change the order of $\chi_i$ s.t. it is just $Q(\Delta_1, \Delta_2, \ldots, \Delta_n)$.
Prop. (15.8.5.6)[Intertwining Operator on Spherical Vector]. For $\chi_1, \chi_2$ unramified with Satake parameter $\alpha_i$, consider $M : B(\chi_1, \chi_2) \to B(\chi_2, \chi_1)$, then

$$M \varphi_{K, \chi} = \frac{1 - q^{-1}\alpha_1\alpha_2^{-1}}{1 - \alpha_1\alpha_2^{-1}} \varphi_{K, \chi'}.$$  

Proof: Clearly this equation is true up to scalar because $M$ is intertwining, so it suffices to calculate $(M \varphi_{K})(1)$. For this, we assume $\chi$ is dominant (15.8.5.2) because we can use analytic continuation. Then

$$(M \varphi_{K})(1) = \int_F \varphi_{K}(w_0 \begin{bmatrix} x & \ 1 \\ 1 & 1 \end{bmatrix}) dx.$$  

The integral is 1 on $O$, and for $m > 0$, on $p^{-m}\backslash p^{-m+1}$, by (15.8.4.11), it equals $q^{-m}\alpha_1^m\alpha_2^{-m}q^m(1 - q^{-1})$, so the total sum is $1 + (1 - q^{-1})\alpha_1\alpha_2^{-1}/(1 - \alpha_1\alpha_2^{-1})$.  

Prop. (15.8.5.7). If $\chi_1, \chi_2$ are nonramified, $V = B(\chi_1, \chi_2)$, $K_0(p)$ is the Iwahori subgroup (15.8.1.8), then the composition

$$V^{K_0(p)} \hookrightarrow V \to J(V)$$  

is an isomorphism. In particular, it is of dimension 2.  

Proof: Firstly notice $V^{K_0(p)}$ has dimension $\leq 2$, because of the decomposition (15.8.1.11) and definition, and $J(V)$ has dimension 2 by (15.8.4.19), so it suffices to show the map is surjective. The image is just $J(V)^{T(O)}$ by (15.8.2.5). But by (15.8.4.19) and the fact $\chi_i$ are nonramified, all of $J(V)$ are $T(O)$-fixed, thus $J(V)^{T(O)} = J(V)$.  

Cor. (15.8.5.8)[Casselman Basis]. When $\chi_1 \neq \chi_2$, we can easily find a basis of $V^{K_0(p)}$, that is

$$L_1(\varphi) = \varphi(1), \quad L_0(\varphi) = (M \varphi)(1)$$  

where $M$ is intertwining integral defined in (15.8.4.12). These are $N(K)$-invariant, thus define functionals on $J(V) \cong V^{K_0(p)}$. They are linearly independent checked on $T(F)$.  

Then the dual basis $\varphi_0, \varphi_1 \in V^{K_0(p)}$ are called the **Casselman basis**.

$\varphi_0$ has a simple form: using Iwahori-Bruhat decomposition (15.8.1.11),

$$\varphi_0(g) = \begin{cases} (\Delta_{1/2}(b)) & g = bw_0k \in B(K)wK_0(p) \\ 0 & \text{otherwise} \end{cases}.$$  

Proof: It is easily verified that this formula is well-defined and defines an Iwahori-fixed vector, so it suffices to valuate it by $L_i$. Clearly $L_1(\varphi_0) = 0$, and for $L_0(\varphi_0)$, notice that

$$w_0 \begin{bmatrix} 1 & x \\ 1 & 1 \end{bmatrix} \in B(K)wK_0(p)$$  

iff $x \in O$, so $L_0(\varphi_0) = 1$.  

Lemma (15.8.5.9). When $\chi_1 \neq \chi_2$ nonramified and $m \geq 0$, the function

$$F_m(g) = \int_F \varphi_K(g \begin{bmatrix} 1 & x \\ 1 & 1 \end{bmatrix} a_m) dx, \quad a_m = \begin{bmatrix} \alpha_1^m \\ 1 \end{bmatrix}$$  

is an Iwahori-fixed vector, and

$$F_m = q^{-m/2}\alpha_2^m M(\varphi_{K})(1)\varphi_0 + q^{-m/2}\alpha_1^m \varphi_1$$
Proof: \[
\int_{K_0(p)} \pi(k a_m) \varphi_K dk = \int_{N_-(p)} \int_{T(O)} \int_{N(O)} \varphi_K(g n t_0 n a_m) dndt_0 dn_-(15.8.1.9)
\]
noticing that \(a_m^{-1} t_0 n a_m \in K\) as \(m \geq 0\), so the integrand is independent of \(t_0, n\) and equals \(F_m\), and it is clearly Iwahori-fixed. And
\[
c_1 = L_1(F_m) = F_m(1) = \varphi_K(a_m) = (\Delta^{1/2} \psi)(a_m) = q^{-m/2} \alpha_1^m.
\]
Similarly, for \(\chi\) dominant,
\[
c_0 = L_0(F_m) = \int_{N(K)} F_m(w_0 n) dn = \int_{N(K)} \int_{N(O)} \varphi_K(w_0 n a_m) dn' dn.
\]
By Fubini, the \(n'\) can be omitted, thus it equals \((M \varphi_K)(a_m) = (\Delta^{1/2} \psi')(a_m)\).

\section*{Spherical Whittaker Function and Spherical Functions}


\textbf{Def. (15.8.5.10) [Spherical Whittaker Function].} The spherical Whittaker function of a generic spherical representation is the spherical vector \(W^0\) in the Whittaker model normalized that \(W_0(1) = 1\).

For \(n = 2\), we can define another normalization \(W_0(g) = \Lambda(\pi(g) \varphi_K)\), where \(\Lambda\) is the Whittaker functional defined in (15.8.4.14) and \(\varphi_K\) is the normalized spherical vector defined in (15.8.5.1).

\textbf{Prop. (15.8.5.11).} We may assume that the conductor of \(\psi\) is \(O\), because any other character is of the form \(x \mapsto \psi(ax)\), thus
\[
W_0(g, \psi_a) = \int_F \varphi_K(w_0 \begin{bmatrix} 1 & x \\ 1 & 1 \end{bmatrix} g) \psi(-ax) dx = |a|^{-1/2} \chi_2(a) W_0 \left( \begin{bmatrix} a \\ 1 \end{bmatrix}, \psi \right),
\]
(and also by analytic continuity). In particular, \(\mu(O) = 1(12.2.6.6)\).

Notice that
\[
W_0 \left( \begin{bmatrix} 1 & x \\ 1 & 1 \end{bmatrix} z \\ z \right) g k = \psi(x) \omega(z) W_0(g), z \in K^\times, k \in K,
\]
where \(\omega = \chi_1 \chi_2\), so to calculate \(W_0\), it suffices to compute \(W_0 \left( \begin{bmatrix} \varphi^m \\ 1 \end{bmatrix} \right) = a_m\).

\textbf{Remark (15.8.5.12).} We want to calculate the spherical Whittaker function \(W_0\) explicitly because it is used to evaluate the local part of the global L-function (16.2.6.3).

\textbf{Lemma (15.8.5.13) [Calculating \(W_0\)].} For \(\mathcal{B}(\chi_1, \chi_2)\) with Satake parameters \(\alpha_1, \alpha_2\), the spherical Whittaker function satisfies
\[
W_0(1) = 1 - q^{-1} \alpha_1 \alpha_2^{-1}, \quad W_0(a_m) = 0
\]
for \(m < 0\).
Proof: As in the proof of (15.8.4.11), because \( \varphi_K \) is \( K \)-invariant, we have
\[
\int_\mathcal{O} \varphi_K(w_0 \begin{bmatrix} 1 & x \\ 1 & 1 \end{bmatrix}) \psi(-x) dx = 1,
\]
\[
\int_{\mathbb{P}^{-1} \setminus \mathcal{O}} \varphi_K(w_0 \begin{bmatrix} 1 & x \\ 1 & 1 \end{bmatrix}) \psi(-x) dx = q^{-1} \alpha_1 \alpha_2^{-1} \int_{\mathbb{P}^{-1} \setminus \mathcal{O}} \psi(-x) dx = -q^{-1} \alpha_1 \alpha_2^{-1},
\]
\[
\int_{\mathbb{P}^{-k-1} \setminus \mathbb{P}^{-k}} \varphi_K(w_0 \begin{bmatrix} 1 & x \\ 1 & 1 \end{bmatrix}) \psi(-x) dx = q^{-k-1} \alpha_1^{-1} \alpha_2^{-k-1} \int_{\mathbb{P}^{-k-1} \setminus \mathbb{P}^{-k}} \psi(-x) dx = 0, \quad k \geq 1
\]
For \( W_0(a_m) \), choose \( x \in \mathcal{O} \) that \( \psi(w^m x) \neq 1 \), then
\[
W_0(a_m) = W_0(a_m \begin{bmatrix} 1 & x \\ 1 & 1 \end{bmatrix}) = W_0(\begin{bmatrix} 1 & w^m \\ 1 & 1 \end{bmatrix} a_m) = \psi(w^m x) W_0(a_m)
\]
so \( W_0(a_m) = 0 \).

Lemma (15.8.5.14) [Functional Equation]. For fixed \( g \), \( W_0(g) \) is an analytic function of \( \alpha_1, \alpha_2 \), and \( (1 - q^{-1} \alpha_1 \alpha_2^{-1})^{-1} W_0(g) \) is symmetric in \( \alpha_1, \alpha_2 \).

Proof: The Whittaker functional is defined by calculated by continuation (15.8.4.14), and for \( \chi \) dominant, \( W_0 \) is analytic (15.8.4.14), thus by calculation in (15.8.5.13), its value at 1 is identically 1, thus so does its analytic continuation. Then to check after switching \( \alpha_1, \alpha_2 \) it is the same meromorphic function, it suffices to show for all irreducible principal series \( B(\chi_1, \chi_2) \). But in this case, \( B(\chi_1, \chi_2) \cong B(\chi_2, \chi_1) \), so their Whittaker model thus spherical Whittaker function differ only by a scalar, thus the same.

Prop. (15.8.5.15) [Calculating \( W_0 \)].

\[
(1 - q^{-1} \alpha_1 \alpha_2^{-1})^{-1} W_0(a_m) = \begin{cases} q^{-m/2} \alpha_1^{-1} \alpha_2^{-1} \alpha_1^{m+1} & m \geq 0 \\ 0 & m < 0 \end{cases}
\]

Proof: By ?? we can assume \( \chi \) is dominant and use analytic continuation.
\[
W_0(a_m) = \int_F F_m(w_0 \begin{bmatrix} 1 & x \\ 1 & 1 \end{bmatrix}) \psi(-x) dx,
\]
by (15.8.4.14)(15.8.5.9) and a change of variable. Then use (15.8.5.9), we see that
\[
W_0(a_m) = C_1 q^{-m/2} \alpha_1^m + C_0 q^{-m/2} \alpha_2^m
\]
where
\[
C_0 = (M \varphi_K)(1) \int_F \varphi_0(w_0 \begin{bmatrix} 1 & x \\ 1 & 1 \end{bmatrix}) \psi(-x) dx
\]
And \( \int_F \varphi_0(w_0 \begin{bmatrix} 1 & x \\ 1 & 1 \end{bmatrix}) \psi(-x) dx = 1 \), by the same consideration as in the proof of (15.8.5.8).

Finally, \((M \varphi_K)(1)\) can be calculated by (15.8.5.6), and the requirement of (15.8.5.14) will determine \( C_1 \).
Prop. (15.8.5.16) [Spherical Function]. For a spherical irreducible admissible representation \((\pi, V)\) of \(GL(2, K)\), its contragradient \(\hat{V}\) is also spherical (2.4.4.11). Then we define the spherical function
\[
\sigma(g) = (\pi(g)v, \hat{v})
\]
where \(v, \hat{v}\) are spherical and normalized that \(\langle v, \hat{v} \rangle = 1\). This is bi-invariant under \(K\)-action by (15.8.5.5).

By (15.8.5.5), \((\pi, V)\) is of the form \(\chi(\det(g))\) or \(\pi(\chi_1, \chi_2)\) for \(\pi\) nonramified. In the former case the spherical function is just \(\chi \circ \det\). Now we only consider the latter interesting case, for which there is a spherical functional \(\hat{v} : \varphi \mapsto \int_K \varphi(k)dk\), and it is 1 on the normalized spherical vector \(v(15.8.5.1)\), and
\[
\sigma(g) = \int_K (\pi(g)\varphi_K)(k)dk = \int_K \varphi_K(kg)dk
\]

Prop. (15.8.5.17) [Macdonald Formula]. The spherical function for unramified principal series behave well under \(Z(K)\)-action and is \(K\)-binvariant, so in order to compute it, it suffices to compute its value on \(a_m\). We have:
\[
\sigma(a_m) = \frac{q^{-m/2}}{1 + q^{-1}}[\alpha_1^m - q^{-1} \alpha_2 \alpha_1^{-1}] + \frac{1}{1 - \alpha_2 \alpha_1^{-1}}
\]

Proof: First notice that
\[
\int_K F_m(k)dk = \int_K \int_O \varphi_K(k)\left[\frac{x}{1}\right] a_m dxdk = \int_K \varphi_K(ka_m)dk
\]

by a change of variable. Then by (15.8.5.9), this equals
\[
\frac{q^{-m/2}}{1 + q^{-1}}[\alpha_1^m - q^{-1} \alpha_2 \alpha_1^{-1}] + \frac{1}{1 - \alpha_2 \alpha_1^{-1}}[\int_K \varphi_1(k)dk]q^{-m/2} \alpha_1^m.
\]

Next we calculate \(\int_K \varphi_0(k)dk\) directly: By (15.8.5.8), this equals the volume of \(K \cap (K_0(p)w_0K_0(p)) = K_0(p)w_0K_0(p)\). \(K/K_0(p) \cong GL(2, \mathbb{F}_q)/B(\mathbb{F}_q)\) has cardinality \(q + 1\), and by pulling back the Bruhat decomposition of \(GL(2, \mathbb{F}_q)\), \(K_0(p)w_0K_0(p)\) consists of \(q\) left cosets of \(K_0(p)\). So
\[
\int_K \varphi_0(k)dk = \frac{q}{1 + q}.
\]

Finally the expression is symmetric in \(\alpha_1, \alpha_2\), because the spherical vectors in \(V, \hat{V}\) are unique (2.4.4.11), and \(B(\chi_1, \chi_2) = B(\chi_2, \chi_1)\). Also, the expression is a combination of \(\alpha_i^m\) and the coefficient is independent of \(m\), so it can be determined as above.

6 Unitarizable, Tempered & \(L^2\) Representations

Def. (15.8.6.1) [\(L^2\)-Representations]. An admissible irreducible representation \((\pi, V)\) of \(G\) is called essentially square-integrable if for any \(v \in V\) and \(\lambda \in V^\ast\), the matrix coefficients \(c_{v, \lambda}\) is \(L^2\) on \(K\).

It is called square-integrable if moreover the central character \(\omega_\pi\) is unitary.

Remark (15.8.6.2) [Casselman]. For any smooth representation of \(GL(n, K)\), there exists a unique real-valued quasi-character \(\chi\) that the central character of \(\pi \otimes (\chi \circ \det)\) is unitary.
Def. (15.8.6.3) [Tempered Representations]. Let $G$ be a reductive group over $F$ and $\pi$ an admissible representation of $G(F)$, then $\pi$ is called an **essentially tempered representation** if the matrix coefficients of $\pi$ are all contained in $L^{2+\varepsilon}(K)$ for any $\varepsilon > 0$.

It is called a **tempered representation** if moreover the central character $\omega_\pi$ is unitary.

Prop. (15.8.6.4) [Jacquet, Zelevinsky].
- $\pi \in \Irr^{\text{adm}}(GL(n, K))$ is essentially square-integrable iff it is of the form $Q(\Delta)$ for a single Zelevinsky segment $\Delta$.
- $\pi \in \Irr^{\text{adm}}(GL(n, K))$ is square-integrable iff it is of the form $Q(\Delta)$ for a single Zelevinsky segment, and the central character of $\sigma(\frac{m-1}{2})$ is unitary, where $\Delta = \Delta(\sigma, m)$.
- $\pi \in \Irr^{\text{adm}}(GL(n, K))$ is tempered iff $\pi = Q(\Delta_1, \ldots, \Delta_r)$, where each $Q(\Delta_i)$ is square-integrable.

**Proof:** Cf. [Generic Representations, Jacquet(1977)].

Cor. (15.8.6.5) [Classification of Irreducible tempered representations of $GL(2)$]. Irreducible tempered representations of $GL(2, K)$ are one of the following form:
- Cuspidal representation with unitary central characters.
- Steinberg representations with unitary central characters.
- Principal representations $B(\chi_1, \chi_2)$ with $\chi_1, \chi_2$ unitary.


Cor. (15.8.6.6) [Tempered Representation is Generic]. Irreducible tempered representations are precisely generic ones $Q(\Delta_1) \times \ldots \times Q(\Delta_r)$ s.t. each $Q(\Delta_i)$ has a unitary central character.

**Proof:** It suffices to show that no two $\Delta_i, \Delta_j$ are linked. But notice if $\Delta_i = (\sigma_i, m_i)$, then $\sigma(i)(\frac{m_i-1}{2})$ is the central character, so there are no chance that they are linked.

**Unitarizable Representations**

Lemma (15.8.6.7) [Possibility of Unitarization of Principal Series]. If $B(\chi_1, \chi_2)$ admits an invariant non-degenerate Hermitian pairing, then either $\chi_1, \chi_2$ are all characters or $\chi_1 = \bar{\chi_2}^{-1}$.

**Proof:** There is an anti-linear $GL(2, K)$-map $B(\chi_1, \chi_2) \rightarrow B(\bar{\chi_1}, \bar{\chi_2})$ which is conjugation, so if there is a $GL(2, K)$-invariant Hermitian pairing on $B(\chi_1, \chi_2)$, $(f_1, f_2) \mapsto (f_1, \bar{f_2})$ will be a non-degenerate $GL(2, K)$-invariant bilinear pairing

$$B(\chi_1, \chi_2) \times B(\bar{\chi_1}, \bar{\chi_2}) \rightarrow \mathbb{C}.$$ 

So $B(\chi_1, \chi_2) \cong B(\bar{\chi_1}^{-1}, \bar{\chi_2}^{-1})$, so $\chi_i$ are characters or $\chi_1 = \bar{\chi_2}^{-1}$ by (15.8.4.10).

Lemma (15.8.6.8). If $\chi_1, \chi_2$ are characters, then $B(\chi_1, \chi_2)$ is unitarizable, by (15.1.4.52).

Lemma (15.8.6.9). Let $\chi_s = |\chi_0|^s$, where $\chi_0$ is a character of $F$. If $s \neq 0, 1/2$ is a real number (so that $B(\chi_s, \chi_{-s})$ is irreducible), then $B(\chi_s, \chi_{-s})$ is unitarizable iff $-1/2 < s < 1/2$. 

15.8. ADMISSIBLE REPRESENTATIONS OF GL(N) OVER P-ADIC NUMBER FIELDS

Proof: Because $\mathcal{B}(\chi_s, \chi_{-s}) = \mathcal{B}(\chi, \cdot \mid s) \otimes \mathcal{B}(\cdot \mid -s)$, we can assume $\chi_0 = 1$. Let $M_s : \mathcal{B}(\chi_s, \chi_{-s}) \to \mathcal{B}(\chi_{-s}, \chi_s)$ be the intertwining integral (15.8.4.12), then we see the sesquilinear pairing

$$
(f_1, f_2) = \int_K (M_s f_1)(k) \overline{f_2(k)} dk
$$

is $G$-invariant and non-degenerate by the proof of (15.8.9). For an irreducible representation, such a pairing must be unique, so we are reduced to checking this representation is positive/negative definite.

Consider the Iwahori-fixed vector $f_0 = \Delta^{s+1/2}(b)$ for $g = bk$ as defined in (15.8.5.8), then as $s$ varies, $f_0$ forms a flat section. We calculate $(f_0, f_0)$ for $s > 0$ and then use continuation:

In this case,

$$
(f_0, f_0) = V(K_0(\mathfrak{p})) \int_F f_0(w_0 \begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix}) dx
$$

and

$$
\begin{bmatrix} 1 & -1 \\ 1 & x \end{bmatrix} \in B(K)K_0(\mathfrak{p})
$$

iff $x \notin \mathcal{O}$, in which case

$$
\begin{bmatrix} 1 & -1 \\ 1 & x \end{bmatrix} = \begin{bmatrix} x^{-1} & -1 \\ 1 & x^{-1} \end{bmatrix} \begin{bmatrix} 1 & 0 \\ 0 & 1 \end{bmatrix}.
$$

So

$$
(f_0, f_0) = \frac{1}{q+1} \int_{|x| > 1} |x|^{-1-2s} dx = \frac{1}{1+q} \frac{q^{-2s}}{1-q^{-2s}}.
$$

We then consider the spherical vector $\varphi_K(15.8.5.1)$, then (15.8.5.6) shows

$$(\varphi_K, \varphi_K) = \frac{1-q^{-1-2s}}{1-q^{-2s}}.$$

which is positive if $|s| > 1/2$. So if $\mathcal{B}(\chi_s, \chi_{-s})$ is unitarizable, $|s| < 1/2$.

Now for $|s| < 1/2$, we show $\mathcal{B}(\chi_s, \chi_{-s})$ is unitary: Modify the intertwining operator $M_s^* = (1-q^{-2s})M_s$, then it is definable for $s = 0$, by calculation in (15.8.4.12), so the modified Hermitian product

$$(\cdot, \cdot)^* = (1-q^{-2s})(-, -)$$

is defined at $s = 0$, and is positive/negative definite, because in this case it is irreducible and unitarizable (15.8.6.8). The eigenvalue of this Hermitian form deforms continuously, and it is never zero because it is non-degenerate as said above (only when $s \neq 1/2$ we need $M_s$ to be isomorphism), so it is always definite and $\mathcal{B}(\chi_s, \chi_{-s})$ is unitarizable. □

Prop. (15.8.6.10)[Unitarizable Principal Series]. An irreducible principal series $\mathcal{B}(\chi_1, \chi_2)$ is unitary iff either $\chi_1, \chi_2$ are all characters, or there is a unitary character $\chi_0$ and $-1/2 < s < 1/2$ that $\chi_1 = \chi_0 \cdot \mid \cdot |^s, \chi_2 = \chi_0 \cdot \mid \cdot |^{-s}$, called complementary series representations.

Proof: Follows immediately from the lemmas above (15.8.6.8)(15.8.6.7)(15.8.6.9). □
15.9 Cuspidal Representations

1 $GL(n)$

References are [Local Langlands Correspondence for $GL(2)$], [Bushnell and P. Kutzko. The admissible dual of $GL(N)$ via compact open subgroups].

Prop. (15.9.1.1)[Bushnell-Kutzko]. All cuspidal representations of $GL(n, F)$ can be constructed by induction from open subgroups.


2 $SL(n)$

[Bushnell and P. Kutzko. The admissible dual of $SL(N)$]
15.10  Adelic Automorphic Representations of GL(n)

Main references are [Bum98], [Gan07], [G-H11], [Borel, Casselman, Automorphic forms, representations and L-function (Corvallis)], [Automorphic Forms on GL(2), Jacquet and Langlands(1970)].

Notations (15.10.0.1).
- Use notations defined in Adele and Idele.
- Use notations defined in Admissible Representations of GL(n) over p-Adic Number Fields.
- Use notations defined in Arithmetic of Algebraic Groups.
- Use notations defined in Automorphic Representations of GL(n) over Archimedean Local Fields.
- Fix a global field $F$, $A = A_F$.
- Fix a linear algebraic group $G \in A_{\text{lg}} R^{\xi} F$ with center $Z$.
- Fix a central character $\omega : Z(A_F) \sim Z(F) \rightarrow \mathbb{C}^\times$. Notice if $G = GL(2)$, $\omega$ is just a Hecke character.

Notations (15.10.0.2) [Group-Theoretic Notations]. If $G = GL(n)$, $B$ is the Borel subgroup of upper triangular matrices, $\text{Unip}(n)$ is the subgroup of upper triangle unipotent matrices. $M_n$ is the mirabolic subgroup of $B$ with $a_{n,n} = 1$, which is isomorphic to $GL(n-1) \ltimes \mathbb{A}^n$. $T$ the group of diagonal matrices. $T_1$ is the subgroup of $T$ that $a_{nn} = 1$.

Denote $w^0$ the matrix $= \sum_{i=1}^n e_{i,n-i}$.

If $n = 2$, denote $w_0 = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$, $w_1 = \begin{bmatrix} -1 & 1 \\ 1 & -1 \end{bmatrix}$,

$t(y) = \begin{bmatrix} y & y^{-1} \\ y & 1 \end{bmatrix}$, $n(z) = \begin{bmatrix} 1 & z \\ 0 & 1 \end{bmatrix}$ $y \in F^\times, z \in F$.

following 6.

Def. (15.10.0.3). For $\alpha \in F_1$, let $\psi_{N,\alpha}$ be a character of $N(F)$ given by $\psi_N(g) = \sum_i \psi(\alpha_i g_{i,i+1})$. For $\alpha = (1, \ldots, 1)$, denote $\psi_{N,\alpha}$ by $\psi_N$.

Def. (15.10.0.4) [Global Norm]. Take an embedding $G \hookrightarrow GL(n)$ over $F$. Define the norm on $G(A_F)$ by

$$||g|| = \prod_v \max(|g_{1,v}|_v, |g_{1,v}^{-1}|_v).$$

Notice in non-Archimedean places $||g||_v = 1$ for $g \in GL(m, \mathcal{O}_v)$, so it is definable.

Def. (15.10.0.5) [Lie Algebra]. Let $g_\infty = \text{Lie}(G(A_F,\infty))$ be the Lie algebra of $G(A)$, $Z = Z(U(g_\infty))$.

1 Introduction

Remark (15.10.1.1). Delete this subsection.?
3: To describe the process of attaching an $L$-function to a classical modular form in terms of representation theory, it is cleanest to use the adelic framework, as demonstrated in Tate’s thesis.

4: The questions about the absolute Galois group $\text{Gal}\mathbb{Q}$, like what finite groups are quotients of $\text{Gal}\mathbb{Q}$, or where there extensions of $\mathbb{Q}$ with given ramification conditions, can be understood via automorphic forms. And automorphic forms can be understood via Langlands dual groups.

2 Automorphic Representations

Def. (15.10.2.1) [$L^2$-Space]. Define $L^2(G/F, \omega)$ the space of all measurable functions $\varphi$ on $G(A)$ that satisfies

$$\varphi(zg) = \omega(z)\varphi(g), \forall z \in Z(A), \quad \varphi(\gamma g) = \varphi(g), \forall \gamma \in G(F)$$

and square integrable module the center:

$$\int_{Z(A)G(F)\backslash G(A)} |\varphi(g)|^2dg < \infty.$$ 

Then the right action of $G(A)$ on $L^2(G(F)\backslash G(A), \omega)$ is continuous, by (10.9.2.9).

Def. (15.10.2.2) [Cuspidality]. A function $\varphi \in L^2(G(F)\backslash G(A), \omega)$ is called cuspidal iff for any proper parabolic subgroup $P = MU$, where $U$ is the unipotent radical,

$$\int_{U(F)\backslash U(A)} \varphi(ng)dn = 0$$

a.e. $g \in G(A)$. The closed space of all cuspidal elements in $L^2(G(F)\backslash G(A), \omega)$ is denoted by $L^2_0(G(F)\backslash G(A), \omega)$. $L^2_0(G(F)\backslash G(A), \omega)$ is stable under the right action of $G(A)$.

Thus a function $\varphi \in L^2(GL(n,F)\backslash GL(n,A), \omega)$ is cuspidal iff

$$\int_{M_{r\times s}(F)\backslash M_{r\times s}(A)} \varphi\left(\begin{bmatrix} X & \chi \\ I_r & I_s \end{bmatrix}
\right) g) dX = 0$$

a.e. $g$ for any $r + s = n, 1 < r < n$, as these are the maximal proper parabolic subgroups of $GL(n)$.

Def. (15.10.2.3) [Smooth Functions on $G(A_F)$].

- The space $C^\infty(G(A_F))$ of smooth functions on $G(A_F)$ is defined to be the restricted tensor product $\otimes C^\infty(G_v)$ w.r.t. $f_{v,0} = \chi_K$.

- The space $C^\infty_c(G(A_F))$ of compactly supported smooth functions on $G(A_F)$ is defined to be the restricted tensor product $\otimes C^\infty_c(G_v)$ w.r.t. $f_{v,0} = \chi_K$. $C^\infty_c(G(A))$ acts on $L^2(G(F)\backslash G(A), \omega)$.

- $G(A_F)$ acts on $C^\infty(G(A_F))$ by right translation, and induces an action of $g_\infty$ thus an action of $U(g_\infty)$ on it. A function $f$ is called $\mathcal{Z}$-finite if it is contained in a f.d. space that is invariant under the action of $\mathcal{Z}$.

- A K-finite function $f \in C^\infty(G(A_F))$ is a vector that is contained in a f.d. space that is right-invariant under $K$. Equivalently, it is $\mathcal{K}_\infty$-finite and is right-invariant under an open compact subgroup of $G(A_F)$.

- A function $f \in C^\infty(G(A_F))$ is said to have moderate growth iff $|f(g)| \leq C||g||^N (15.10.0.1)$ for some constant $C > 0$ and any $g \in G(A_F)$. 

15.10. ADELIC AUTOMORPHIC REPRESENTATIONS OF GL(N)

- A function \( f \in C^\infty(G(A_F)) \) is said to be **rapidly decreasing** if for any \( k \in \mathbb{Z}_+ \), \( |f(g)| \leq C_k ||g||^{-k} \) for any \( g \in G(A_F) \) and some constant \( C_k \).

**Def. (15.10.2.4) [Adelic Automorphic Forms]**. We denote by \( \mathcal{A}(G/F, \omega) \) the space of **adelic automorphic forms** consisting of smooth functions on \( G(A_F) \) (15.10.2.3) that satisfies

- \( \varphi(zg) = \omega(z) \varphi(g), \forall z \in Z(A), \varphi(\gamma g) = \varphi(g), \forall \gamma \in G(F) \).
- \( K \)-finite and \( Z \)-finite (15.10.2.3).
- of moderate growth (15.10.2.3).

And the space \( \mathcal{A}_0(G/F, \omega) \) of **cusp forms** the automorphic forms that is cuspidal in sense of (15.10.2.2). \( \mathcal{A}(G/F, \omega) \) is a \((g_\infty, K_\infty)\)-module, and \( G(A_F) \) acts smoothly on it. The subspace \( \mathcal{A}_0(G/F, \omega) \) is stable under both actions.

**Prop. (15.10.2.5) [Analytic Properties]**. Any automorphic form \( f \) is real analytic when restricted to \( G(A_\infty) \), and is of moderate growth.

Any cusp form \( f \) is rapidly decreasing. In particular, \( f \in L^2_0(G/F) \) if \( G \) is semisimple.

**Proof**: It is real analytic by (15.7.2.10). The growth condition reduces immediately to the Archimedean case (15.7.4.7). \( \square \)

**Admissible Representations**

**Def. (15.10.2.6) [Admissible Representations]**. A smooth representation of \( G(A_F) \) is defined to be a commuting smooth \( G(A_F) \)-action and a \((g_\infty, K_\infty)\)-module structure (13.3.3.5). The category of smooth representations of \( G(A_F) \) is denoted by \( \text{Rep}^{\text{alg}}(G(F)) \).

Any \((\pi, V) \in \text{Rep}^{\text{alg}}(G(A_F)) \) induces a representation of \( K = K_f \times K_\infty \). Then this representation is called an **admissible representation** if every vector is \( K \)-finite, and for any irreducible representation \( \rho \) of \( K \), \( \dim V^\rho < \infty \). By (15.1.4.32), it can be checked that this is equivalent to: for any irreducible representation \( \rho_{\infty} \) of \( K_\infty \) and an open compact subgroup \( U \subset K_f \), \( \dim V^\rho_{\infty} \cap V^U < \infty \). The category of admissible representations of \( G(A_F) \) is denoted by \( \text{Rep}^{\text{adm}}(G/F) \).

**Def. (15.10.2.7) [Automorphic Representations]**. \( \mathcal{A}(G/F, \omega) \) and \( \mathcal{A}_0(G/F, \omega) \) afford smooth representations of \( GL(n, A) \) by definition (15.10.2.4). So we define an **automorphic representation** to be an irreducible smooth representation of \( G(A) \) that can be realized as a quotient of a subrepresentation of \( \mathcal{A}(G/F, \omega) \), and an **automorphic cuspidal representation** to be an irreducible smooth representation of \( G(A_F) \) that can be realized as a subrepresentation of \( \mathcal{A}_0(G(F) \backslash G(A), \omega) \).

The category of automorphic representations of \( G(A_F) \) is denoted by \( \text{Irr}^{\text{auto}}(G/F, \omega) \). The category of cuspidal representations of \( G(A_F) \) is denoted by \( \text{Irr}^{\text{cusp}}(G/F, \omega) \).

**Remark (15.10.2.8)**. There is a general method of constructing subrepresentations of \( \mathcal{A}(G(F) \backslash G(A), \omega) \) using Eisenstein series, but no known methods for constructing subrepresentations of \( \mathcal{A}_0(G(F) \backslash G(A), \omega) \).

**Thm. (15.10.2.9) [Automorphic Representations are Admissible, Harish-Chandra]**.

\[ \text{Irr}^{\text{cusp}}(G/F, \omega) \subset \text{Irr}^{\text{auto}}(G/F, \omega) \subset \text{Irr}^{\text{adm}}(G/F). \]

**Proof**: Let \( V_1 \subset V_2 \subset \mathcal{A}(G(F) \backslash G(A), \omega) \) be submodules s.t \( V_2/V_1 \cong \pi \), then we can assume \( V_2 \) is generated by an element \( f \in V_2 \backslash V_1 \), because otherwise change \( V_2 \) by the submodule \( V_2' \) generated by \( f \) and \( V_1 \) by \( V_1 \cap V_2' \).
\( f \) is killed by an ideal \( J_\infty \) of finite codimension in \( \mathbb{Z}_\infty \), and is invariant under the action of a compact open subset \( U \subset G(A_F) \). Let
\[
G(F)\backslash G(A)/U = \prod_i \Gamma_i \backslash G(A_\infty)
\]
as in \((13.3.13)\), then there is an isomorphism of \((g_\infty, K_\infty)\)-modules
\[
A(G(F)\backslash G(A), \omega, J_\infty)^U \cong \bigoplus_i A(\Gamma_i \backslash G(A_\infty)), 1, \omega_\infty, J_\infty)^{(15.7.5.10)},
\]
which is admissible by the fundamental theorem of Harish-Chandra \((15.7.5.10)\). Thus \( V_2 \subset A(G(F)\backslash G(A), \omega, J)^U \) is also admissible.

Tensor Product Theorem

**Def. (15.10.2.10) [Restricted Tensor Representation]**. Given a set of locally compact groups \( G_v \) and a.e. their compact subgroups \( K_v, (\rho_v, V_v) \in \text{Rep}^{alg}(G_v), \xi_v^0 \in V_v^{K_v} \) are given for a.e. \( v \), then we can define the **restricted tensor representation**
\[
(\rho, V) = \bigotimes_v' (\rho_v, V_v, \xi_v^0)
\]
of \( G(A_F) = \prod_v' (G_v, K_v) \) on \( \bigotimes_v' V_v \) by
\[
\rho(\bigotimes_v g_v)(\bigotimes_v \xi_v) = \bigotimes_v \rho_v(g_v) \xi_v.
\]

**Def. (15.10.2.11) [Global Hecke Algebra]**. For \( v \in \Sigma_F \), let \( \mathcal{H}_{G(F_v)} \) be the Hecke algebras constructed in \((15.1.4.19)\) and \((15.6.4.11)\). As \( \mathcal{H}_{G(F_v)} \) has a spherical idempotent \( e_v^0 = e_{K_v}(15.10.2.6) \), we can define the **global Hecke algebra**
\[
\mathcal{H}_{G(A_F)} = \bigotimes_v (\mathcal{H}_{G(F_v)}, e_v^0).
\]

Then by definition of representations in \((15.10.2.7)\) and \((15.6.4.12)(15.1.4.23)\),
\[
\text{Rep}^{alg}(G(A_F)) = \text{Rep}^{alg}(\mathcal{H}_{G(A_F)}).
\]

**Thm. (15.10.2.12) [Tensor Product Theorem, Flath]**. For \( (\rho, V) \in \text{Irr}^{adm}(G/F) \), there exists uniquely for each \( v \in \Sigma_F^\infty \) a \( (\rho_v, V_v) \in \text{Irr}^{adm}(G_v, K_v) \), and for each \( v \in \Sigma_F^\infty \) a \( (\pi_v, V_v) \in \text{Irr}^{alg}(G(F_v)) \) s.t. for a.e. \( v, V_v \) contains a non-zero \( K_v^{\text{-fixed vector}} \xi_v^0 \), and
\[
(\rho, V) = \bigotimes_v' (\rho_v, V_v, \xi_v^0).
\]

Conversely, any such a restricted tensor product is in \( \text{Irr}^{adm}(G/F) \).

**Proof**: By considering the global Hecke algebra, this follows immediately from \((15.10.2.11)\) and \((15.6.4.12)(15.1.4.23)\).

**Cor. (15.10.2.13) [Contragradient Representations]**. For any \( \rho = \bigotimes_v \rho_v \in \text{Irr}^{adm}(G/F) \), we can define the **contragradient** of \( \rho \) as \( \hat{\rho} = \bigotimes_v \hat{\rho}_v(15.1.1.20) \in \text{Irr}^{adm}(G/F) \).

**Cor. (15.10.2.14) [Irreducible Representations of \( K \)]**.
\[
\text{Irr}(K) = \bigotimes_v \text{Irr}(K_v).
\]

**Proof**: This is similar to the proof of \((15.10.2.12)\).
3 $\text{Irr}^{\text{auto}}(\text{GL}(n)/F)$

Main references are [Bum98]Chap3.

Basics

Prop. (15.10.3.1). $\text{GL}(n, F)$ is unimodular.

Proof: This is because $\text{GL}(n, F_v)$ is unimodular for any $v \in \Sigma_F$ and because we can calculate the restricted product measure by (12.2.5.6).

Def. (15.10.3.2) [Congruence Subgroups]. For $N \in \mathbb{Z}_+$, define the congruence subgroup $\mathcal{K}_0(N) \subset \text{GL}(2, A_F)$ as follows: $\mathcal{K}_0(N) = \prod_{v \in \Sigma_F} \mathcal{K}_0(N)_v$, where

$$\mathcal{K}_0(N)_v = \begin{cases} \text{GL}(2, \mathcal{O}_v) & v \nmid N \\ \mathcal{K}_0(N_v) \subset F_v(15.8.1.8) & v | N \end{cases}$$

Prop. (15.10.3.3). If $F = \mathbb{Q}$, then the inclusion induces homeomorphisms

$$\Gamma_0(N) \backslash \text{GL}(2, \mathbb{R})^+ \cong \text{GL}(2, \mathbb{Q}) \backslash \text{GL}(2, A)/K_0(N).$$

$$\Gamma_0(N) \backslash \text{SL}(2, \mathbb{R}) \cong \text{GL}(2, \mathbb{Q}) Z(A) \backslash \text{GL}(2, A)/K_0(N)$$

Thus the definition of congruence subgroups (15.11.1.1) is compatible with that of (13.3.3.13)

Proof: Because $\text{Cl}(\mathbb{Q}) = 1$ and $\text{det}(\mathcal{K}_0(N)) = \prod_{v \in \Sigma_F} \mathcal{O}_v^\times$, item3 of (13.3.3.12) shows

$$\text{GL}(2, A) = \text{GL}(2, \mathbb{Q}) \text{GL}(2, \mathbb{R}) K_0(N) = \text{GL}(2, \mathbb{Q}) \text{GL}(2, \mathbb{R})^+ K_0(N),$$

so the map

$$\text{GL}(2, \mathbb{R})^+ \rightarrow \text{GL}(2, \mathbb{Q}) \backslash \text{GL}(2, A)/K_0(N)$$

is surjective. Now if $g'_\infty$ and $g_\infty$ has the same image, then $g'_\infty = \gamma g_\infty k_0$, so $g'_\infty = \gamma_\infty g_\infty; \gamma_f = k_0^{-1}$. Then $\gamma_\infty$ belongs to $\Gamma_0(N)$. Thus there is a bijection

$$\Gamma_0(N) \backslash \text{GL}(2, \mathbb{R})^+ \cong \text{GL}(2, \mathbb{Q}) \backslash \text{GL}(2, A)/K_0(N).$$

2 follows from 1 by modulo the center.

Cor. (15.10.3.4). The quotient space $\text{GL}(n, F)Z(A) \backslash \text{GL}(n, A)$ has finite measure.

Proof: For the general case, Cf.[Humphreys, Arithmetic Groups, (1980)].

Because $K_0(N)$ is compact, it suffices to prove that $\text{GL}(n, F)Z(A) \backslash \text{GL}(n, A)/K_0(N)$ has finite measure (because $\text{GL}(n, F)$ and $\text{GL}(n, A)$ are both unimodular, the measure is compatible). But this space is homeomorphic to $\Gamma_0(N) \backslash \text{SL}(2, \mathbb{R})$, which has finite measure because $\Gamma(1) \backslash \text{SL}(2, \mathbb{R})$ does and $\Gamma_0(N)$ is of finite index in $\Gamma(1)$.

Def. (15.10.3.5) [Global Siegel Sets]. For $c, d > 0$, then the global Siegel set $\mathcal{G}_{c,d} = K_f \times \mathcal{G}_{c,d,\infty}$.

And denote $\mathcal{G}_{c,d}$ its image in $Z(A) \backslash \text{GL}(2, A)$.

Prop. (15.10.3.6). For $c, d$ suitable chosen, $\text{GL}(2, A) = \text{GL}(2, F) \mathcal{G}_{c,d}$. 
Proof: We prove only for $F = \mathbb{Q}$: This is true for $c \leq \sqrt{3}/2$ and $d \geq 1$ because of the shape of the fundamental domain of $GL(2, \mathbb{R})$ for $SL(2, \mathbb{Z})$ (15.11.1.6).

Prop. (15.10.3.7) [Contragradient Representations]. For $(\pi, V) \in \text{Irr}^{\text{adm}/\text{cusp}}(GL(n)/F, \omega)$,

- its contragradient $(\hat{\pi}, \hat{V}) \in \text{Irr}^{\text{adm}/\text{cusp}}(GL(n)/F, \omega^{-1})$, and $\hat{V}$ can be chosen to be the space of all functions $g \mapsto \varphi(g^{-t})$.
- if $n = 2$, then $\hat{\pi} \cong \pi \otimes (\omega^{-1} \circ \det)$.

Proof: It suffices to analyze each place. Notice for cuspidal representations, it suffices to show for finite places, because we can use strong multiplicity one (15.10.4.8).

For admissible case we only prove for $n = 2$ and $F$ totally real (the problem is we haven’t studied $\mathbb{C}$)?

Let $\hat{V}$ be the space of functions of the form $\hat{\varphi}(g) = \varphi(g^{-t})$, then the right action of $G$ on $\hat{V}$ corresponds back to the restriction of the right action composed with the automorphism $g \mapsto g^{-t}$. Thus the result follows from (15.8.1.15) and its Archimedean analogy for $(g_{\infty}, K_{\infty})$-modules (15.6.3.35).

Spectral Problem

Prop. (15.10.3.8) [Gelfand, Graev and Piatetski-Shapiro]. Let $\varphi \in C_c^\infty(GL(n, A))$, then

- There exists a constant $C(\varphi)$ that for all $f \in L^2_0(GL(n, F)\backslash GL(n, A), \omega)$, we have $||\rho(\varphi) f||_C(\varphi) \leq C(\varphi)||f||_2$.
- $\rho(\varphi)$ is a compact operator on $L^2_0(GL(n, F)\backslash GL(n, A), \omega)$.

Proof: The proof is the same as that of (15.7.5.6), but use global Siegel sets (15.10.3.5), Cf. [Bump, P297]?

Cor. (15.10.3.9) $[L^2_0(GL(n, F)\backslash GL(n, A), \omega)$ Totally Decomposable]. The space $L^2_0(GL(n, F)\backslash GL(n, A), \omega)$ decomposes into a Hilbert space direct sum of irreducible invariant subspaces over $GL(n, A)$.

Proof: The proof is exactly the same as (15.7.5.2), but where we use (15.10.3.8) in place of (15.16.2.1) and lemma ?? in place of lemma (15.6.4.1).

Prop. (15.10.3.10) [Irreducible Cuspidal Representations Admissible]. If $(\pi, V) \in \text{Irr}^{\text{fin}}(GL(n, A))$ is contained in the decomposition of $\mathcal{H} = L^2_0(GL(n, F)\backslash GL(n, A), \omega)$ in (15.10.3.9), then $V^{K-\text{fin}} \subset V$ is dense, $V^{K-\text{fin}} \subset \mathcal{A}_0(GL(n, F)\backslash GL(n, A), \omega) \in \text{Rep}^{\text{adm}}(GL(n)/F, \omega)$.

In particular,

$$\mathcal{A}_0(GL(n, F)\backslash GL(n, A), \omega) \subset L^2_0(GL(n, F)\backslash GL(n, A), \omega),$$

and

$$\mathcal{A}_0(GL(n, F)\backslash GL(n, A), \omega) = \bigotimes_{\pi \in \text{Irr}^{\text{cusp}}(GL(n)/F, \omega)} m_{\pi} \pi$$

by (15.10.2.5) and (15.10.3.9).

Proof: This is general by (15.6.4.4), and for the containment in $\mathcal{A}_0$ by a similar argument as in (15.7.5.8) using a similar lemma as lemma (15.7.5.7).

The irreducible smooth $GL(n, A)$-representations are admissible by (15.10.2.9).
Proposition (15.10.3.11) [Global Hecke Algebra]. There are isomorphisms

\[
\Gamma_0(N)\backslash G_0(N)/\Gamma_0(N) \cong \prod_{v \in \mathcal{P} \setminus \mathcal{S}_f(N)} K_v \backslash GL(2, Q_v)/K_v.
\]

which induces an isomorphism \( \mathcal{R}_N \cong \prod_{v \in \mathcal{P} \setminus \mathcal{S}_f(N)} \mathcal{H}_{K_v}(15.11.3.2)(15.8.1.13) \).

Proposition (15.10.3.12) [Adelization of Maass Forms]. Let \( \chi \) be a Dirichlet character \( \mod N \) and \( \omega \) be the adelized Hecke character of \( \chi(12.2.5.33) \), then define a character \( \lambda_d \) of \( K_0(N)(15.10.3.2) \) by

\[
\lambda_d\left(\begin{bmatrix} a & b \\ c & d \end{bmatrix}\right) = \prod_{v \in \mathcal{S}_f(N)} \omega_v(d_v).
\]

By (15.10.3.3) there is a homeomorphism

\[
\Gamma_0(N) \backslash GL(2, \mathbb{R})^+ \cong GL(2, \mathbb{Q}) \backslash GL(2, A)/K_0(N),
\]

which induces a map

\[
f \mapsto \varphi_f : C^\infty(\Gamma_0(N) \backslash GL(2, \mathbb{R})^+, \chi_d | \cdot |^\lambda) \to C^\infty(GL(2, \mathbb{Q}) \backslash GL(2, A), \omega | \cdot |^\lambda) : \varphi(\gamma g_\infty k_0) = f(g_\infty) \lambda_d(k_0)
\]

and this map identifies \( K \)-finiteness, \( Z \)-finiteness and moderate growth, thus induces a map

\[
\mathcal{A}(\Gamma_0(N) \backslash GL(2, \mathbb{R})^+, \chi_d) \to \mathcal{A}(GL(2, \mathbb{Q}) \backslash GL(2, A), \omega)
\]

compatible with \( (g_\infty, K_\infty) \)-action, and the image are the automorphic forms satisfying \( \pi(k_0)\varphi = \lambda(k_0)\varphi \) for \( k_0 \in K_0(N) \).

This map also identifies cuspidality, thus it induces a map

\[
\mathcal{A}_0(\Gamma_0(N) \backslash GL(2, \mathbb{R})^+, \chi_d) \to \mathcal{A}_0(GL(2, \mathbb{Q}) \backslash GL(2, A), \omega)
\]

Proof: To show that \( \varphi_f(zg) = \omega(z)\varphi_f(g) \) for \( z \in A^* \), notice by (12.2.5.31), \( Z(A^*) = Z(Q^*)Z(R_+^*)(Z(A) \cap K_0(N)) \), and for these elements \( \varphi_f(zg) = \lambda(z)\varphi_f \), as \( \omega \) is trivial on \( \prod_{v \in \mathcal{S}_f(N)} \mathcal{O}_v^\infty \).

It identifies moderate growth because \( A^* = Q^*R_+^* \prod_{v \in 1^\infty} \mathcal{O}_v^\infty \) again.

To show cuspidality, notice \( x \mapsto \gamma(\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} g) \) is left-invariant under \( a \) if \( g^{-1}\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} g \in K_0(N) \).

but such \( a \) is open in \( A \), thus contains some open compact subgroup \( U_f \subset A_f \). Notice by strong approximation, \( A = Q \times R \times U_f \), thus there is an isomorphism \( R/M \cong A/FU_f \). Now let \( g = \gamma g_\infty k_0 \), then

\[
\int_{A/F} \varphi_f(\begin{bmatrix} 1 & a \\ 0 & 1 \end{bmatrix} g) = C \int_{R/M} \varphi_f(\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} g) dx = C\lambda(k_0) \int_0^M f(\gamma^{-1}(\begin{bmatrix} 1 & x \\ 0 & 1 \end{bmatrix} g_\infty)),
\]

which vanishes for each \( g \) iff \( f \) is cuspidal at every cusp. For similar reason, \( \varphi_f \) is of moderate growth iff \( f \) is of moderate growth at every cusp.
**Remark (15.10.3.13).** Similar isomorphism happens for more general congruence subgroups, for example, we can change $\Gamma_0(N)$ to $\Gamma_1(N)$ and change $K_0(N)$ to

$$U_1(N) = \{ \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{GL}(2, \mathbb{Z}) : c \equiv 0 (\text{mod } N), d \equiv 1 (\text{mod } N) \}.$$ 

**Prop. (15.10.3.14) [Strong Multiplicity One].**

- Let $f$ be a cuspidal eigenfunction in $\mathcal{A}_0(\Gamma_0(N) \backslash GL(2, \mathbb{R})^+, \chi)$ of a.e. Hecke operators $T_p$ for $p \nmid N$, then $\varphi_f$ lies in an irreducible subspace of $L^2_0(\text{GL}(2, F) \backslash \text{GL}(2, A), \omega)$.

- If $f, g$ are cuspidal eigenfunctions for a.e. Hecke operators in $\mathcal{A}_0(\Gamma_0(N) \backslash GL(2, \mathbb{R})^+, \chi)$ of a.e. Hecke operators $T_p$ for $p \nmid N$, then $f = g$.

In particular, any Hecke eigenform generates a cuspidal representation.

**Proof:** 2: By (15.10.3.9), consider the projection of $\varphi_f$ to any irreducible cuspidal representation $\pi$. By (15.10.3.11), $\varphi_f$ is an eigenform of the Hecke operator $T_p$. But it is also eigenvalues of the Hecke operator $R_p$, But $\mathcal{H}_{Q_p}$ is generated by $T_p, R_p, R_p^{-1}$ by (15.11.3.10), so $\pi_p$ is spherical with determined eigenvalues. But then $\pi_v$ is determined by (2.4.4.12). Then $\pi$ is determined by strong multiplicity one (15.10.4.8).

1 follows from 2 because if $\pi$ is a component of $L^2_0(\text{GL}(2, F) \backslash \text{GL}(2, A), \omega)$ that the projection of $\varphi_f$ is non-zero, then it has the same Hecke eigenvalue as $\varphi_f$, so it must be just $\varphi_f$ by item 2.

Cf. [Bump, P344].

**Remark (15.10.3.15).** WARNING: This is in general not true for groups other than $\text{GL}(n)$. This is related to the theory of $L$-packets and $A$-packets.?

**Remark (15.10.3.16) [Adelized Maass Forms].** Notice if $f$ comes from a Maass form, then [G-H11] documented the properties of the adelized Maass form $\varphi_f$ in detail.

**Ramanujan Conjecture**

**Conj. (15.10.3.17) [Ramanujan].** If $\omega$ is unitary and $\rho = \otimes' \rho_v \in \text{Irr}^{\text{cusp}}(\text{GL}(n) / F, \omega)$, then for any $v \in \Sigma_F$, $\rho_v$ is tempered (15.8.6.3).

**Proof:**

**Prop. (15.10.3.18).** The Ramanujan conjecture (15.10.3.17) implies the Ramanujan-Petersson conjecture (16.2.6.16).

**Proof:** The Ramanujan-Petersson conjecture says the eigenvalue $\lambda_p$ of $T_p$ on $f$ satisfies $|\lambda_p| \leq 2p^{1/2}$. Consider the irreducible cuspidal representation $\pi_f$ generated by $\varphi_f$ (15.10.3.14), then $T_p$ is the same as the eigenvalue of the local Hecke algebra $T_p$ on $\varphi_f$. But $\pi_{f, p}$ is unramified, thus by (15.8.6.10) it is unitary principal or complementary. But notice if the Satake parameters of $\pi_{f, p}$ are $\alpha_i$, then $\lambda_p = p^{1/2}(\alpha_1 + \alpha_2)$, Then it suffices to show that $|\alpha_1 + \alpha_2| \leq 2$, which is equivalent to $\pi_p$ being tempered (15.8.6.10).

**Conj. (15.10.3.19) [Generalized Ramanujan Conjecture].** Let $G$ be a reductive group over a global field $F$, and $\pi \in \text{Irr}^{\text{cusp, generic}}(G / F, \omega)$, then $\pi$ is tempered. Notice this implies the Ramanujan conjecture, as any $\rho \in \text{Irr}^{\text{cusp}}(\text{GL}(n) / F, \omega)$ is generic (15.10.4.3).

**Proof:**
Remark (15.10.3.20) [Arthur Conjecture]. In fact, Arthur extends this conjecture further, and explains the extent of failure of the Ramanujan conjecture for irreducible representations in the discrete spectrum of $L^2(G(F)\backslash G(A))$, as well as the multiplicities in the discrete spectrum.

4 Whittaker Models

Def. (15.10.4.1) [Whittaker Models]. The notion of Whittaker model and Whittaker functional, generonicness the same as in the local case (15.8.3.1).

Prop. (15.10.4.2) [Global uniqueness of Whittaker Models]. Let $(\pi, V)$ be an irreducible admissible representation of $GL(2, A)$, then $(\pi, V)$ has a Whittaker model w.r.t $\psi$ iff each $(\pi_v, V_v)$ (15.10.2.12) has a Whittaker model $W(\pi_v, \psi_v)$. If this is the case, then $W(\pi, \psi)$ is unique and

$$W(\pi, \psi) = \bigotimes_v (W_v, W_v^0)$$

where $W_v^0$ are the unique spherical function (15.8.5.15) of $W_v$ normalized s.t. $W_v^0(K_v) = 1$.

Proof: Let $(\pi, V) = \bigotimes_v (\pi_v, V_v)$ w.r.t a.e. spherical vectors $\xi_v^0$ by tensor product theorem (15.10.2.12), and $(\pi_v, V_v)$ are spherical a.e. $v$.

Firstly if every $(\pi_v, V_v)$ has a Whittaker model, the $W$ in the proposition is truly a Whittaker model: functions in $W(\pi, \psi)$ are clearly smooth and $K$-finite, and they have moderate growth because each local part is, and for a.e. $v$, $W_v(\pi, \psi)$ is compactly supported on $|x|_v \leq 1$. And there is a canonical isomorphism of $V$ onto $W(\pi, \psi)$ by letting $(W_\xi)_v = W_v^0$ if $\xi_v = \xi_v^0$ and

$$W_\xi(g) = \prod_v W_{v, \xi_v}(g_v).$$

This is definable because $g_v \in K_v$ for a.e. $v$ thus $W_{v, \xi_v}(g_v) = W_v^0(g_v) = 1$ for a.e. $v$.

Because the local Whittaker models are all rapidly decreasing, and the spherical Whittaker model vanishes for $|\xi_v|_v > 1$, thus $W$ is also rapidly decreasing, and is a Whittaker model for $\pi$.

Secondly if $W$ is a Whittaker model for $(\pi, V)$, denote $\xi \mapsto W_\xi$ the isomorphism of $V$ onto $W$. Notice there exists some $\xi \in V$ that $W_\xi(1) \neq 0$: if $W_\xi(g_\infty g_f) \neq 0$, then $W_\xi(g_f)(g_\infty) \neq 0$, and argue the same way as in (15.7.4.4). We may assume $\xi^0 = \bigotimes_v \xi_v^0$ that $W_{\xi^0}(1) = 1$.

Consider the ”pullback” of $W$ to $GL(n, F_v)$ via $\xi$, then they are clearly Whittaker models for $(\pi_v, V_v)$ thus unique (13.3.1.5) (15.7.4.3), and also $W_{v, \xi_v^0}(1) = 1$. So $W_v^0$ exists a.e. uniquely. Now we prove $W$ is of the form we said above, this will prove uniqueness.

Then we need to prove

$$W_\xi(g) = \prod_v W_{v, \xi_v}(g_v)$$

We only need to prove for one $\xi = \xi^0$, because $W_\xi(\pi_v, \psi_v)$ are both irreducible. And also we can assume $g_v = 1$, a.e., because $(W_\xi)_v(g_v) = W_{v, \xi_v}(g_v) = 1$, a.e. Then we are in the finite case and we can multiply by scalars at f.m. $v$ s.t. this equation is true and nonzero for $g$.

Thm. (15.10.4.3) [Fourier Expansion and Existence of Whittaker Models, Shalika]. Given $(\pi, V) \in \text{Irr}^{cusp}(GL(n)/F, \omega)$, for $\Phi \in V$, define

$$W_\Phi(g) = \int_{\text{Unip}(n, F) \setminus \text{Unip}(n, A)} \Phi(ng) \psi_N(-n) dn,$$
then $GL(n, A_F)$ acts on these functions, and they form a Whittaker model $W(\pi, \psi)$. $W_\Phi(g)$ is called the **Fourier-Whittaker coefficients** for $\Phi$.

And we have a Fourier expansion formula:

$$
\Phi(g) = \sum_{\gamma \in \text{Unip}(n-1,F) \setminus GL(n-1,F)} W_\Phi\left[ \begin{array}{c} \gamma \\ 1 \end{array} \right] (g),
$$

which converges absolutely and uniformly on compact subsets of $GL(n, A_F)$.

**Remark (15.10.4.4).** This is false for some other groups, for the reason that the Fourier inversion may not be true, thus it may happen that all the Fourier coefficients vanish. For example, holomorphic Siegel modular forms on Sp(2n) don’t have Whittaker models.

**Proof:** We only prove for $n = 2$. For general case, see the beautiful paper [Sha74] of Shlikra. For any $g \in GL(n, A)$, consider $F(n) = \varphi(n g)$ on $N(A)$, then it is a continuous function on $N(F) \setminus N(A)$, and $N(F) \setminus N(A)$ is compact (12.2.5.19), so by Fourier inversion formula (10.9.3.17),

$$
F(x) = \sum_{\alpha \in F} C(\alpha) \varphi(\alpha x), \quad C(\alpha) = \int_{\text{Unip}(n,F) \setminus \text{Unip}(n,A)} \varphi\left( \begin{array}{c} \alpha \\ 1 \end{array} \right) g(\psi(-\alpha x)) dx.
$$

Now $C(0) = 0$ because $\varphi$ is cuspidal, and if $\alpha \in F^\times$, as $\varphi$ is automorphic,

$$
C(\alpha) = \int_{\text{Unip}(n,F) \setminus \text{Unip}(n,A)} \varphi\left( \begin{array}{c} \alpha \\ 1 \end{array} \right) g(\psi(-\alpha x)) dx = \int_{A/F} \varphi\left( \begin{array}{c} \alpha \\ 1 \end{array} \right) g(\psi(-\alpha x)) dx = W_\varphi\left( \begin{array}{c} \alpha \\ 1 \end{array} \right) g).
$$

So if we let $x = 0$, we get $\Phi(g) = \sum_{\alpha \in F^\times} W_\Phi\left( \begin{array}{c} \alpha \\ 1 \end{array} \right) g$.

Now we show $\{ W_\Phi \}$ is Whittaker model: they all satisfies $W_\Phi(ng) = \psi(n) W_\Phi(g)$ by construction, and because $W_X \varphi = X W_\varphi$, $\rho(g) W_\varphi = W_{\rho(g) \varphi}$, it is clear that this space is invariant under action of $GL(2, A_F)$ and $(g_\infty, K_\infty)$, and also it is of moderate growth in $y$ because $\varphi$ does (15.10.2.4) and $N(F) \setminus N(A)$ is compact, and it consists of $K$-finite vectors because $V$ is admissible (15.10.3.10). Finally, the Fourier inversion shows that $\varphi \mapsto W_\varphi$ is non-zero, thus injective.

**Cor. (15.10.4.5) [Cuspidal Forms Decay Rapidly].** Any cuspidal form on $GL(2, A_F)$ is rapidly decreasing for $|y| \to \infty$.

Moreover, it also decays rapidly when $|y| \to 0$.

**Remark (15.10.4.6).** This is proved already in (15.10.2.5).

**Proof:** To show it is rapidly decreasing, use the Fourier expansion formula, and the fact the Whittaker model is product of local Whittaker models. Also for $v \in \Sigma_F$, the local Kirillov model is compactly supported (15.8.3.19), and for $v \in \Sigma_F^\infty$, the Whittaker model is rapidly decreasing (15.7.4.3), notice for any $g \in GL(2, A)$, for any $C$, the number of $a \in K^*$ that $\varphi\left( \begin{array}{c} a \\ 1 \end{array} \right) g) \neq 0$ and $|a|_\infty < C$ is bounded by a polynomial of $C$, thus it is rapidly decreasing.
For $|y| \to 0$, as $\varphi$ is automorphic, notice

$$\varphi\left(\begin{bmatrix} y & 1 \\ 1 & 0 \end{bmatrix}\right) = \varphi(w_0 \begin{bmatrix} 1 & y \\ y & 1 \end{bmatrix} w_0) = \omega(y)(\pi(w_0)\varphi)(\begin{bmatrix} y^{-1} \\ 1 \end{bmatrix}).$$

\(\square\)

**Cor. (15.10.4.7).** Every local component of a cuspidal representation of $GL(n, A)$ is generic, by (15.10.4.2).

**Prop. (15.10.4.8) [Strong Multiplicity One for $GL(n)$].** If $(\pi, V), (\pi', V') \in \text{Irr}^{cusp}(GL(n)/F)$ satisfy $\pi_v \cong \pi'_v$ a.e. $v$, then $\pi \cong \pi'$, and $V = V' \subset \mathcal{A}_0(GL(n, F) \backslash GL(n, A_F))$.

**Proof:** We only prove for $n = 2$ and the case $\pi_1, \pi_2$ are isomorphic on Archimedean places. For general $n$, Cf. [Representations of the Group $GL(n, K)$ where $K$ is a local field, Gelfand-Kazhdan], [Euler Subgroups, in Lie Groups and their Representations, Piatetski-Shapiro (1975)]. For the Archimedean places, Cf. [Base Change for $GL(2)$, Langlands (1980) Lemma 3.1]

Firstly if $\pi_v \cong \pi'_v$ for every place $v$, then their corresponding Whittaker model is the same (multiplied by a scalar) by (15.10.4.2). Then by (15.10.4.3) we have a Fourier expansion formula

$$\varphi(g) = \sum_{\alpha \in F^*} W_\varphi\left(\begin{bmatrix} \alpha & 0 \\ 0 & 1 \end{bmatrix} g\right).$$

Thus $V = V'$.

In case that $\pi_v \cong \pi'_v$ only outside a finite set $S$, we choose functions $W_v, W'_v$ in the local Whittaker model for $\pi_v, \pi'_v$ s.t. if $v \not\in S$, $W_v = W'_v$ and $W_v$ is the unique spherical function normalized that $W_v(K_v) = 1$ a.e. $v$, and if $v \in S$, they are chosen that

$$F(y) = W_v\left(\begin{bmatrix} y & 1 \\ 1 & 0 \end{bmatrix}\right) = W'_v\left(\begin{bmatrix} y & 1 \\ 1 & 0 \end{bmatrix}\right) \in C_c^\infty(F^*_v),$$

which is possible by (15.8.3.20). And we define

$$\varphi(g) = \sum_{\alpha \in F^*} W\left(\begin{bmatrix} \alpha & 0 \\ 0 & 1 \end{bmatrix} g\right), \quad \varphi'(g) = \sum_{\alpha \in F^*} W'(\begin{bmatrix} \alpha & 0 \\ 0 & 1 \end{bmatrix} g),$$

$$W(g) = \prod_v W_v(g_v), \quad W'(g) = \prod_v W'_v(g_v).$$

as in (15.10.4.3).

Then we claim $\varphi = \varphi'$ on $GL(2, A)$: $\varphi \in V, \varphi' \in V'$ are automorphic, thus $\varphi = \varphi'$ on $GL(2, F)GL(2, A_F^\circ)$ by continuity, which is just $GL(2, A_F)$ by weak approximation, so we have a $\varphi \in V \cap V'$, meaning $V = V'$.

\(\square\)

5 Eisenstein Series

References are [Bump, Chap3].

**Prop. (15.10.5.1) [Langlands].** For any $\rho \in \text{Irr}^{\text{auto}}(G/F, \omega)$, there exists a parabolic subgroup $P = MN$ and $\sigma \in \text{Irr}^{\text{cusp}}(M/F)$ that $\pi$ is a subquotient of $I_P(\sigma)$.
Proof:

Remark (15.10.5.2). The pair \((M, \sigma)\) may not be unique up to conjugacy. It is unique for \(GL(n)\), by a theorem of Jacquet-Shalika, but in general it is false. For example, Waldspurger showed for \(G = \text{PGSp}(4)\) that there are cuspidal representations \(\pi\) that are abstractly isomorphic to a subquotient of some \(I_P(\sigma)\) with \(\sigma\) cuspidal on \(M = GL(2)\). These are called CAP representations.
15.11 Modular Forms

Main References are [D-S16], [1-2-3 of Modular Forms] and [Mil17c]. This section is a continuation of the discussion of Automorphic Forms in 15.7 and use the same notations.

1 Modular Forms

Def. (15.11.1.1) [Congruence Subgroups]. Let $\Gamma(N)$ be the inverse image of $1 \in SL(2, \mathbb{Z}/N)$ in the mapping $SL(2, \mathbb{Z}) \to SL(2, \mathbb{Z}/N)$, then a subgroup $\Gamma$ of $SL(2, \mathbb{Z})$ is called a congruence subgroup if it contains $\Gamma(N)$ for some $N$.

In particular, a congruence subgroup has finite index in $\Gamma(1)$.

Lemma (15.11.1.2) [Cartan Decomposition]. There is a complete set of coset representatives for $SL(2, \mathbb{Z}) \backslash GL(2, \mathbb{Q})^+ / SL(2, \mathbb{Z})$ consisting of the diagonal matrices $\text{diag}(d_1, d_2)$, where $d_1, d_2 \in \mathbb{Q}^\times$ and $d_1/d_2$ is a positive integer.

More generally, for $N > 0$,

$$GL(2, \mathbb{Q})^+ = \prod_{d_1, d_2 \in \mathbb{Q}^\times, d_1/d_2 \in \mathbb{Z}_+} SL(2, \mathbb{Z}) \begin{bmatrix} d_1 \\ d_2 \end{bmatrix} \Gamma_0(N).$$

Also, let $\Sigma$ be the set of primes dividing $N$, $\mathbb{Z}_\Sigma$ be the localization of $\mathbb{Z}$ at these primes, and $G_0(N)$ be the subgroup of $GL(2, \mathbb{Z}_\Sigma)^+$ consisting of matrices $\begin{bmatrix} a & b \\ c & d \end{bmatrix}$ s.t. $c \in N\mathbb{Z}_\Sigma$. Then

$$G_0(N) = \prod_{d_1, d_2 \in \mathbb{Z}_\Sigma, d_1/d_2 \in \mathbb{Z}_+} \Gamma_0(N) \begin{bmatrix} d_1 \\ d_2 \end{bmatrix} \Gamma_0(N).$$

Proof: The first assertion follows from (11.6.6.7), noticing the sign.

For the second assertion, for any $g \in G_0(N)$, let $g = \gamma_1 \text{diag}(d_1, d_2) \gamma_2$ where $D = d_1/d_2 \in \mathbb{Z}$ and $(D, N) = 1$. Then for any $\begin{bmatrix} a & b \\ Dc & d \end{bmatrix} \in \Gamma_0(N)$, we can change $(\gamma_1, \gamma_2)$ to $(\gamma_1 \begin{bmatrix} a & Db \\ c & d \end{bmatrix}, \begin{bmatrix} a & b \\ Dc & d \end{bmatrix} \gamma_2)$, in this way if $\gamma_2 = \begin{bmatrix} x & y \\ z & w \end{bmatrix}$, we can change $z$ to $Dxc + dz$. Now take $k$ s.t. $(kx + z, N) = 1$, and let $c$ be chosen s.t. $\mathbb{N}|D(kz + x)c + z$, and $d = kDc + 1$, then $(Dc, d) = 1$, and we can find $a, b$ s.t. $ad - Dbc = 1$. Then for this $(a, b, c, d), \begin{bmatrix} a & b \\ Dc & d \end{bmatrix} \gamma_2 \in \Gamma_0(N)$.

Finally, if $g \in G_0(N)$ and $\gamma_2 \in \Gamma_0(N)$, then automatically $\gamma_1 \in \Gamma_0(N)$.

Prop. (15.11.1.3) [Conjugate of Congruence Subgroup]. If $\Gamma$ is a congruence subgroup of level $N$ and $\alpha \in GL(2, \mathbb{Q})^+$, then $\alpha^{-1} \Gamma \alpha$ is a congruence subgroup.

In particular, $\alpha \Gamma \alpha^{-1} \cap \Gamma$ is also a congruence subgroup, and if $\alpha \in SL(2, \mathbb{Z})$ with $\delta(\alpha) = D$, then $\alpha^{-1} \Gamma \alpha$ is a congruence subgroup of level $DN$.

Proof: Let $M_1, M_2$ be positive integers s.t. $M_1 \alpha, M_2 \alpha^{-1} \in M(2, \mathbb{Z}).$ (In the second case we can take $M_1 = 1, M_2 = D$). If $A$ is a matrix that $A \equiv 1 \mod M_1M_2N$, then $\alpha^{-1}(A-1)\alpha \equiv 1 \mod N$. Thus $\alpha^{-1} \Gamma \alpha$ contains $\Gamma(M_1M_2N)$.
Cor.\,(15.11.1.4)[Congruence Topology]. We can define a topology on the group \(GL(2, \mathbb{Q})^+\) given by a basis at the origin given by the open subgroup \(\Gamma(N)\). Then\,(15.11.1.3) can be used to show that this is truly a topology. In fact, it is restriction on \(SL(2, \mathbb{Z})\) is the same as the topology given by the inclusion \(SL(2, \mathbb{Z}) \subset SL(2, \hat{\mathbb{Z}})\).

But unfortunately, \(SL(2, \mathbb{Z})\) is not compact in this topology, because otherwise \(SL(2, \mathbb{Z})\) is closed in \(SL(2, \hat{\mathbb{Z}})\), contradiction.

Lemma\,(15.11.1.5). The action of \(\Gamma(1) = SL(2, \mathbb{Z})\) on \(\mathcal{H}\) is properly discontinuous\,(3.8.1.13).

Proof: Cf.[Bump P18]. \(\Box\)

Prop.\,(15.11.1.6). The subset \(F = \{z \in \mathcal{H}||\text{Re}(z)|| < 1/2, |z| > 1\}\) is a fundamental domain for \(\Gamma(1) = SL_2(\mathbb{Z})\), and moreover, let \(S = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}\) and \(T = \begin{bmatrix} 1 & 1 \\ 0 & 1 \end{bmatrix}\), then \(S^2 = -1, (ST)^3 = (TS)^3 = -1\), and

1. two elements \(z, z'\) of \(\mathcal{F}\) are equivalent under \(\Gamma(1)\) iff
   \[\text{Re}(z) = -1/2\;\text{and}\;z' = z + 1,\;\text{then}\;z' = T(z).\]
   \[|z| = 1\;\text{and}\;z' = -\frac{1}{2},\;\text{then}\;z' = S(z).\]

2. Let \(z \in \mathcal{F}\), if the stabilizer of \(z\) is not \(\pm 1\), then
   \[a = i\;\text{and}\;\text{Stab}(i) = \langle S \rangle.\]
   \[z = \rho = e^{2\pi i/6}\;\text{and}\;\text{Stab}(\rho) = \langle TS \rangle.\]
   \[z = \omega,\;\text{and}\;\text{Stab}(\omega) = \langle ST \rangle.\]

Proof: 1: Let \(\Gamma'\) be the subgroup of \(\Gamma(1)\) generated by \(S\) and \(T\). By\,(10.5.1.8),

\[\text{Im}(\gamma(z)) = \frac{|\text{Im}(z)|}{\sqrt{|cz + d|^2}}.\]

and there is a \(\gamma \in \Gamma'\) that \(|cz + d|\) attains the minimal value, then \(\text{Im}(\gamma(z))\) attains a maximal value. Now there is a \(n\) that \(z' = \text{Re}(T^n\gamma(z)) \in [-1/2, 1/2]\). Now I claim that \(|z'| \geq 1\), because otherwise

\[\text{Im}(SZz') = \text{Im}(-1/z') = \frac{|z'|}{|z'|^2} > \text{Im}(z'),\]

contradiction.

2: Suppose \(z, z' \in \mathcal{F}\) are \(\Gamma\)-conjugate, we can assume \(\text{Im}(z) \leq \text{Im}(z')\). Suppose \(z' = \gamma(z)\) and \(z = x + iy\), then

\[(cx + d)^2 + (cy)^2 \leq 1.\]

Then \(|c| < 2\). If \(c = 0\), then \(d = \pm 1\), and \(\gamma\) is a translation, thus we are in case 1.(a). If \(c = 1\), then \(d = 0\), unless \(z = \rho\) or \(\omega\). If \(d = 0\), then \(\gamma = \begin{bmatrix} a & 1 \\ -1 & 1 \end{bmatrix}\), thus \(\gamma(z) = a - \frac{1}{z}\). If \(a = 0\), then we are in case 1.(b), and if \(a \neq 0\), then \(z = \rho\) or \(\omega\), and the \(c = -1\) case is similar. \(\Box\)

Def.\,(15.11.1.7)[Elliptic Points]. A point \(z \in \mathcal{H}\) is called an elliptic point if it is the fixed point of an elliptic element \(\gamma\) of \(\Gamma(15.7.1.2)\).

Prop.\,(15.11.1.8). Let \(\Gamma\) be a discrete subgroup of \(SL(2, \mathbb{R})\) and \(z\) an elliptic point of \(\Gamma\), then the stabilizer \(\Gamma_z\) of \(z\) in \(\Gamma\) is a finite cyclic subgroup .
**Prop. (15.11.1.9)** [Cusps and Elliptic Points for $\Gamma(1)$].

- The cusps of $\Gamma(1)$ are exactly $\mathbb{P}^1(\mathbb{Q})$, and each of them is $\Gamma(1)$-equivalent to $\infty$.
- The elliptic points of $\Gamma(1)$ are exactly those that are $\Gamma(1)$-conjugate to $i$ or $\rho = (1 + \sqrt{3})/2$, with corresponding stabilizer group cyclic of order 4 and 6.

**Proof:** 1: Clearly $\infty$ is fixed by the parabolic matrix $T = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$. Now for any $m/n$ that $m, n$ is coprime, there exists integers $r, s$ that $rm - sn = 1$. Let $\gamma = \begin{bmatrix} m & s \\ n & r \end{bmatrix}$, then $\gamma(\infty) = m/n$ thus $m/n$ is also a cusp. Conversely, every parabolic matrix is conjugate to $T$, thus its fixed point is conjugate to $\infty$, which means the fixed point is in $\mathbb{Q} \cup \{\infty\}$.

2: For the elliptic points of $\Gamma(1)$, use (15.11.1.6). □

**Def. (15.11.1.10)** [Meromorphic Modular Forms]. Let $\Gamma$ be a discrete subgroup of $SL(2, \mathbb{R})$, $k > 0$ and $\chi$ is a character of $\Gamma$ that $\chi(-1) = (-1)^k$, the space of (twisted) meromorphic modular forms $M_k^\chi(\Gamma)$ is the space of all holomorphic functions $\mathcal{H} \to \mathbb{C}$ that satisfies

- $f$ is meromorphic.
- $f[\gamma]_k = \chi(\gamma)f(15.7.1.13)$.
- $f$ is meromorphic at the cusps (15.7.1.17), equivalently, $f[\gamma]_k$ are all meromorphic at $\infty$ for $\gamma \in GL(2, \mathbb{Q})^+$.

And it is called a holomorphic modular form if it is holomorphic and holomorphic at cusps (15.7.1.17).

A meromorphic modular form of weight 0 is called a modular function.

Denote $M_k^\chi(\Gamma, 1) = M_k^\chi(\Gamma)$, $M_k(\Gamma, 1) = M_k(\Gamma)$, and moreover we denote by $S_k(\Gamma, \chi)$ the set of holomorphic cusp forms consisting of all $f \in M_k(\Gamma, \chi)$ that vanishes at the cusps (15.7.1.17), and denote $S_k(\Gamma, 1) = S_k(\Gamma)$.

Denote by $M^\Gamma(\Gamma) = \bigoplus_{k \geq 0} M_k^\chi(\Gamma)$ the graded ring of meromorphic modular forms, $M(\Gamma) = \bigoplus_{k \geq 0} M_k(\Gamma)$ the graded algebra of holomorphic modular forms for $\Gamma$, $\otimes_{k \geq 0} S_k(\Gamma)$ is a graded ideal of $M(\Gamma)$.

**Def. (15.11.1.11)** [Hauptmodul]. Let $\Gamma$ be a discrete subgroup of $SL(2, \mathbb{R})$ with exactly one cups, $k > 0$, a Hauptmodul for $\Gamma$ is an element in $M^\Gamma(\Gamma)$ s.t. it is holomorphic on $\mathcal{H}$ and has a simple pole at the cusp with residue 1, i.e. its Fourier series at the cusp is of the form

$$f(\tau) = q^{-1} + a_0 + a_1 q + \ldots$$

**Prop. (15.11.1.12)** [Petersson Inner Product]. Let $f \in M_k(\Gamma, \chi)$ and $g \in S_k(\Gamma, \chi)$, then we see $f \overline{g} y^k$ is invariant under the action of $\Gamma$, thus we can define

$$\langle f, g \rangle = \langle f, g \rangle_{\Gamma, k} = \frac{1}{[SL(2, \mathbb{Z}) : \{\pm\} \Gamma]} \int_{\mathcal{H} \setminus \Gamma} f \overline{g} y^k \frac{dxdy}{y^2},$$

which is finite, and restricts to an inner product on $S_k(\Gamma, \chi)$. Moreover, this inner form is invariant of the $\Gamma$ chosen.
Proof: To show it is finite, notice that $\Gamma \backslash \mathcal{H}$ is a finite translations of the fundamental domain of $\Gamma(1)$, and for $\alpha \in SL(2, \mathbb{Z})$,

$$
\int_{\alpha(D)} f \bar{g} y^k \frac{dx dy}{y^2} = \int_D f \circ \alpha g \circ \alpha y(\alpha(z))^k \frac{dx dy}{y^2} = \int_D f[\alpha]_k g[\alpha]_k y^k \frac{dx dy}{y^2},
$$

and $f[\alpha]_k, g[\alpha]_k$ are modular forms for $\Gamma' = \alpha^{-1} \Gamma \alpha, \chi'(\gamma') = \chi(\alpha \gamma \alpha^{-1})$, thus it suffices to prove the integral is finite on the fundamental domain $\mathcal{F}$ for $\Gamma(1)(15.11.1.6)$. For this, notice $g$ is of exponential decay for $y$, thus the integral is bounded by $\int_y e^{-c} y^{k-2} dy < \infty$. 

\begin{prop}(15.11.1.13).
If $\alpha \in GL(2, \mathbb{R})^+, f \in M_k(\Gamma)$ and $g \in S_k(\alpha^{-1} \Gamma \alpha)$, then

$$(f[\alpha]_k, g)_{\alpha^{-1} \Gamma \alpha} = (f, g[\alpha]^{-1}_k)_{\Gamma}. $$

\end{prop}

\begin{proof}
This is because for there is an isomorphism $\alpha : \alpha^{-1} \Gamma \alpha \backslash \mathcal{H} \cong \Gamma \backslash \mathcal{H}$, and for any left $\Gamma$-invariant function $\varphi$,

$$
\int_{\alpha^{-1} \Gamma \alpha \backslash \mathcal{H}} \varphi(\alpha(\tau))d\mu(\tau) = \int_{\Gamma \backslash \mathcal{H}} \varphi(\tau)d\mu(\tau)
$$

and $[f \bar{g}[\alpha^{-1}_k] y^k](\alpha(\tau)) = [f[\alpha]_k \bar{g} y^k](\tau)$. \hfill \Box

\begin{prop}(15.11.1.14)[Twisted Modular Forms].
For each Dirichlet character $\chi \bmod N$, we can define a character of $\Gamma_0(N)$:

$$
\chi d\begin{bmatrix} a & b \\ c & d \end{bmatrix} = \chi(d).
$$

Then we can define $M_k(N, \chi) = M_k(\Gamma_0(N), \chi)(15.11.1.10)$ and $S_k(N, \chi) = S_k(\Gamma_0(1)) \cap M_k(N, \chi)$. Then there are direct sum decompositions:

$$
M_k(\Gamma_1(N)) = \bigoplus_{\chi, \chi(-1)=(-1)^k} M_k(N, \chi), \quad S_k(\Gamma_1(N)) = \bigoplus_{\chi, \chi(-1)=(-1)^k} S_k(N, \chi),
$$

where the summation is over all Dirichlet character $\bmod N$. Moreover, the summands are orthogonal w.r.t. the Petersson inner product(15.11.1.12).

\begin{proof}
Cf.[Diamond, P418]. \hfill \Box

\end{proof}

\begin{cor}(15.11.1.15) [Reduction to $\Gamma_0(N)$].
For any congruence subgroup $\Gamma(N)$, there exists $\alpha \in GL(2, \mathbb{Q})^+$ s.t. 

$$
\begin{bmatrix} 1 & 1 \\ N & 1/N \end{bmatrix} \Gamma_1(N) \begin{bmatrix} 1 & 0 \\ 0 & 1/N \end{bmatrix} \subset \Gamma(N).
$$

Thus if $f \in M_k(\Gamma(N))$, $f[\text{diag}(1, N)]_k \subset M_k(\Gamma_1(N))$, which is a combination of modular forms in $M_k(\Gamma_0(N), \chi)$. Thus the study of congruence modular forms reduces to the study of $M_k(\Gamma_0(N), \chi)$.

\end{cor}

\section{Derivatives}

2 Modular Curves and Jacobians

\begin{prop}(15.11.2.1) [Local Picture].
Let $D$ be the unit disk and $\Delta$ be a finite group acting on $D$ and fixing $0$, then by Schwarz lemma, $\Delta$ is a finite subgroup of $\text{Aut}(D,0) \cong \mathbb{R}/\mathbb{Z}$, so it is a finite cyclic group. If $|\Delta| = m$, then $z^m$ is invariant under $\Delta$ and defines a function on $\Delta \backslash D$. It is a homeomorphism from $\Delta \backslash D$ to $D$, thus defines a complex structure on $\Delta \backslash D$.

\end{prop}
Let \( X = \{ z \in \mathbb{C} \mid \text{Im}(z) > c \} \) and \( h \) an integer. Let \( \mathbb{Z} \) acts on \( X \) by \( nz = z + nh \). This action can extend to \( X^* = X \cup \{ \infty \} \), and we can consider the quotient space \( \mathbb{Z} \setminus X^* \). The function \( q(z) = e^{2\pi i z/h} \) is a homeomorphism from \( \mathbb{Z} \setminus X^* \) onto the open disk of radius \( e^{-2\pi c/h} \) and center \( 0 \), which defines a complex structure on \( \mathbb{Z} \setminus X^* \).

**Lemma (15.11.2.2)** [Modular Curves for \( \Gamma(1) \)]. Let \( \mathcal{H}^* = \mathcal{H} \cup \{ \infty \} \), the Riemann surface \( \Gamma(1) \setminus \mathcal{H}^* \) is compact and of genus 0, so isomorphic to the Riemann surface.

**Proof:** We first define a complex structure on \( \Gamma(1) \setminus \mathcal{H} \): Let \( p : \mathcal{H} \to \Gamma(1) \setminus \mathcal{H} \) be the quotient map, and let \( Q \) be a point of \( \mathcal{H} \) mapping to \( P \). If \( Q \) is not an elliptic point, then we can choose a nbhd of \( Q \) that maps isomorphically to a nbhd of \( P \), so we can define the complex structure near \( P \).

If \( Q = i \), then the map \( z \mapsto \frac{z-i}{z+i} \) maps some open nbhd of \( i \) to an open disk \( D' \) with center 0, and the action of \( S \) is transformed to the action \( z \mapsto -z \). By the local picture, \( f(z) = (\frac{z-i}{z+i})^2 \) is invariant under action of \( S \) and defines a complex structure near \( p(i) \). Similarly, if \( Q = \rho \), then \( g(z) = (\frac{z-\rho}{z+\rho})^3 \) is invariant under the action of \( ST \), and defines a complex structure near \( p(\rho) \).

The space \( \Gamma \setminus \mathcal{H} \) we get is not compact, and it can be compactified by adding a point \( \infty \), the resulting space is compact because it is a quotient space of \( D \cup \{ \infty \} \), which is compact. And we give a complex structure on the resulting space: The function \( q = e^{2\pi i z} \) is a function mapping a nbhd of \( \infty \) in the fundamental domain to an open disk with center 0, and thus giving a complex structure near \( \infty \).

It can be seen directly that \( \Gamma(1) \setminus \mathcal{H}^* \) is homeomorphic to a sphere, and then use the fact any Riemann surface of genus 0 is isomorphic to \( S^1(5.11.8.2) \). \( \square \)

**Prop. (15.11.2.3)** [Modular Curves for \( \Gamma \)]. For a congruence group \( \Gamma \), the quotient space \( \Gamma \setminus \mathcal{H} \) can be compactified to a Riemann surface \( X(\Gamma) \) by adjoining \( n \) points, where \( n \) is the number of cusps of \( \Gamma \).

**Proof:** The quotient space \( \Gamma \setminus \mathcal{H} \) can be given a complex structure exactly the same way as \( \Gamma(1) \setminus \mathcal{H} \), and it can be compactified by adding \( \mathbb{P}^1(Q) \), which has only f.m. orbits under action of \( \Gamma \), by(15.11.1.9) and the fact \( \Gamma \) has finite index in \( \Gamma(1) \). For the complex structure: if \( h \) is the smallest positive integer that \( T^h \in \Gamma \), then \( q = e^{2\pi i z/h} \) is a homeomorphism of a nbhd of \( \infty \) in \( \Gamma \setminus \mathcal{H} \) to some open disk of 0, thus defines a complex structure near \( \infty \). For any other cusps \( \alpha \), let \( \gamma \in \Gamma(1) \) satisfies \( \alpha = \gamma(\infty) \), then \( z \mapsto q(\gamma^{-1}(z)) \) defines a complex structure near \( \alpha \). \( \square \)

**Def. (15.11.2.4)** [Notations]. Let \( \Gamma \) be a congruence subgroup, then we denote

\[ Y(\Gamma) = \Gamma \setminus \mathcal{H}, \quad X(\Gamma) = \Gamma \setminus \mathcal{H}^*. \]

Also abbreviate \( Y(\Gamma(N)) \) to \( Y(N) \), \( X(\Gamma(N)) \) to \( X(N) \), and \( Y(\Gamma_0(N)) \) to \( Y_0(N) \), and \( X(\Gamma_0(N)) \) to \( X_0(N) \).

**Prop. (15.11.2.5)** [Modular Form as Differential Forms]. A holomorphic modular form \( M_k(\Gamma) \) is just a holomorphic form on \( X(\Gamma) \) of degree \( k \), and its dimension can be calculated, see Dimension Formulae.

Similarly, an automorphic function for \( \Gamma \) is the same as a function on \( X(\Gamma)(15.11.2.3) \). In particular, if it is holomorphic and vanishes at cusps, then it is constant.

**Proof:** \( \square \)

**Cor. (15.11.2.6)** [Hauptmodul]. Let \( \Gamma \) be a congruence subgroup with only 1 cusp, a Hauptmodul is the unique meromorphic modular form that has only a simple pole at the cusp with residue 1.
Modular Curves over $\mathbb{Q}$

**Prop. (15.11.2.7)** $[X_0(N)]$. The field $C(X_0(N))$ of modular functions for $\Gamma_0(N)$ is generated by $j(z)$ and $j(Nz)$ over $\mathbb{C}$, and the minimal polynomial $F(j,Y)$ of $j(Nz)$ over $C(j)$ has degree $d = [PSL(2,\mathbb{Z}) : \Gamma_0(N)](15.11.4.1)$, and $F(j,Y) \in \mathbb{Z}[j,Y]$.

When $N > 1$, $F(X,Y)$ is symmetric in $X,Y$, and when $N = p$ is a prime,

$$F(X,Y) \equiv X^{p+1} + Y^{p+1} - X^pY^p - XY \mod p.$$

**Proof:**

**Cor. (15.11.2.8).** The field of functions on $X(1)$ is $\mathbb{C}(j)$.

**Action of Hecke Algebras**

**Prop. (15.11.2.9)**[Double Coset Operators]. There is an action of $\mathcal{R}$ on $X_1(\Gamma)$

**Modular Jacobians**

**Def. (15.11.2.10)**[Modular Jacobians]. Define $J_1(N) = \text{Jac}(X_1(N))$, $J_0(N) = \text{Jac}(X_0(N))$, which is defined over the same field as the defining field of $X_1(N)$ or $X_0(N)$.

3 Hecke Algebra

**Def. (15.11.3.1)**$[G(N)]$. Define $G(N) = \cup_{\alpha \in GL(2,\mathbb{Q}) \alpha \Gamma_0(N)} \Gamma_0(N)\alpha \Gamma_0(N)$.

**Def. (15.11.3.2)**[Hecke Algebra]. Notation as in(15.11.2), if $\alpha \in \Gamma_0(N)\backslash G(N)/\Gamma_0(N)$, then $\Gamma_0(N)\backslash \Gamma_0(N)\alpha \Gamma_0(N)$ is finite, and if $N = 1$, there is a set of representatives $\{\alpha_1, \ldots, \alpha_h\}$ s.t.

$$\Gamma(1)\alpha \Gamma(1) = \coprod_i \Gamma(1)\alpha_i = \coprod_i \alpha_i \Gamma(1) = \Gamma(1)\alpha_i^h.$$

Let $\mathcal{R}'_N$ be the free Abelian group generated by $\Gamma_0(N)\backslash G(N)$ s.t. if $\Gamma_0(N)\alpha \Gamma_0(N) = \sum_i \Gamma_0(N)\alpha_i$, then $[\alpha][\beta] = \sum_i [\alpha_i][\beta]$.

Define the **Hecke algebra** $\mathcal{R}_N$ of $\Gamma_0(N)$ to be the subalgebra of $\mathcal{R}'_N$ consisting by right $\Gamma_0(N)$-invariant elements. Then $\mathcal{R}_N$ is isomorphic to the free Abelian group generated by the double coset $\Gamma_0(N)\backslash G(N)/\Gamma_0(N)$, and is commutative.

**Remark (15.11.3.3).** Compare this definition with that of(15.1.4.19).

**Proof:**

$$\Gamma_0(N)\backslash \Gamma_0(N)\alpha \Gamma_0(N) \cong \Gamma_0(N)\backslash \Gamma_0(N)\alpha \Gamma_0(N)\alpha^{-1}$$

$$\cong \Gamma_0(N) \cap \alpha \Gamma_0(N)\alpha^{-1} \backslash \alpha \Gamma_0(N)\alpha^{-1}$$

$$\cong \alpha^{-1} \Gamma_0(N)\alpha \cap \Gamma_0(N)\backslash \Gamma_0(N)$$

which is finite by(15.11.1.3).

By decomposition(15.11.1.2), the transposition on $G(N)$ is an involution that identifies every double coset $\Gamma(1)\alpha \Gamma(1)$, thus $\sum_i \Gamma(1)\alpha_i = \sum_i \alpha_i^h \Gamma(1)$, and also $\Gamma(1)\alpha_i \cap \alpha_i^h \Gamma(1) \neq \emptyset$, as $\Gamma(1)\alpha_i, \Gamma(1) = \Gamma(1)\alpha_i^h \Gamma(1)$, thus we can replace $\alpha_i$ by some element in $\Gamma(1)\alpha_i \cap \alpha_i^h \Gamma(1)$.
To show $\mathcal{R}_N$ is commutative, for any $\sigma \in \Gamma(1) \backslash GL(2, \mathbb{Q})^+ / \Gamma(1)$, denote $\deg(\sigma)$ to be the cardinality of $\Gamma(1) \backslash \Gamma(1) \sigma \Gamma(1)$, $\sigma[i], i \leq \deg(\sigma)$ be a set of representatives, and let $m(\alpha, \beta, \sigma[i])$ be the cardinality of $\{(i, j) | \Gamma(1) \alpha_i \beta_j = \Gamma(1) \sigma[i]\}$, then $m(\alpha, \beta, \sigma[i])$ is independent of $i$ as right action by $\Gamma(1)$ permutes $\{(i, j)\}$. Also we see $m(\alpha, \beta, \sigma[i])$ equals $1/\deg(\sigma)$ times the number of pairs $\{(i, j) | [\sigma] = [\alpha_i \beta_j]\}$, because $[\sigma] = [\alpha_i \beta_j]$ iff $\alpha_i \beta_j \in \Gamma(1) \sigma[i]$ for some $i$.

Then

$$m(\alpha, \beta, \sigma[i]) = \frac{1}{\deg(\sigma)} \# \{(i, j) | [\sigma] = [\alpha_i \beta_j]\} = \frac{1}{\deg(\sigma)} \# \{(i, j) | [\sigma'] = [\beta_j \alpha_i^t]\} = m(\beta, \alpha, \sigma'^t[i]).$$

But as $\sigma'^t[i]$ is a permutation of $\sigma[i]$, we see $\mathcal{R}$ is commutative.

\section*{Hecke Operators}

\textbf{Prop. (15.11.3.4).} If $\Gamma_1, \Gamma_2$ are congruence subgroups of $X$, then for any $\alpha \in GL^+(2, \mathbb{Q})$, the double coset

$$\Gamma_1 \alpha \Gamma_2 = \bigsqcup_i \Gamma_1 \beta_i$$

for some $\beta_i \in GL^+(2, \mathbb{Q})$. Then we can define a map

$$\text{Div}(X(\Gamma_1)) \to \text{Div}(X(\Gamma_2)) : [\tau] \mapsto [\beta_i \tau],$$

which induces a morphism $\text{Jac}(\Gamma_1) \to \text{Jac}(\Gamma_2)$.

\textbf{Prop. (15.11.3.5)[Action on Modular Forms].} Let $\Gamma_1, \Gamma_2$ be congruence subgroups of $GL^+(2, \mathbb{R})$, then

\textbf{Prop. (15.11.3.6)[Hecke Operators].} The Hecke algebra $\Gamma \backslash GL^+(2, \mathbb{R})/\Gamma$ acts on $M_k(\Gamma)$ via

$$T_\alpha(f) = \sum_i f[\alpha]_{ik}(15.7.1.13), \text{ if } \Gamma \alpha \Gamma = \bigsqcup_i \Gamma \alpha_i.$$

and preserves $S_k(\Gamma)$.

\textbf{Proof:} This is an action because if $\Gamma_0(N) \alpha \Gamma_0(N) = \bigsqcup_i \Gamma_0(N) \alpha_i, \Gamma_0(N) \beta \Gamma_0(N) = \bigsqcup_j \Gamma_0(N) \beta_j$, then $[\alpha][\beta] = \bigsqcup_{i,j} \Gamma_0(N) \alpha_i \beta_j$.

Also $T_\alpha(\gamma | f)_k = T_\alpha(f)$ for $\gamma \in \Gamma_0(N)$ because $\Gamma_0(N) \backslash \Gamma_0(N) \alpha \Gamma_0(N)$ is right $\Gamma_0(N)$-invariant. And they are holomorphic at cusps because $f$ is holomorphic at cusps thus all $f[\alpha]_k$ are holomorphic at cusps. Moreover, if $f$ vanishes at cusps, then all $f[\alpha]_k$ vanishes at cusps.

\section*{$\Gamma_0(N), \Gamma_1(N)$ Cases}

\textbf{Prop. (15.11.3.7) [Self-Adjointness].} The action of $\mathcal{R}_N$ on $S_k(\Gamma(N))$ is self-adjoint w.r.t to the Petersson inner product $(15.11.1.12)$.

\textbf{Proof:} First notice $(\chi_d(\alpha)^{-1}f[\alpha]_k, g) = (f, \chi_d(\alpha)g[\alpha^{-1}]_k)$ for any $\alpha \in G_0(N)$ by $(15.11.1.13)$, and $f, g \in M_k(N, \chi)$, thus $(\chi_d(\alpha)^{-1}f[\alpha]_k, g)$ only depends on the double coset $\Gamma_0(N) \alpha \Gamma_0(N)$. Thus

$$(T_\alpha f, g) = \sum_i (\chi_d(\alpha_i)^{-1}f[\alpha]_k, g) = \deg(\alpha)(\chi_d(\alpha)^{-1}f[\alpha]_k, g) = \deg(\alpha)(f, \chi_d(\alpha)g[\alpha^{-1}]_k)$$
However, $\det(\alpha)\alpha^{-1}$ has the same Smith normal form as $\alpha$, thus it is in the same double coset as $\alpha$, thus

$$\deg(\alpha)(f, \chi_d(\alpha)g[\alpha^{-1}]_k) = \deg(\alpha)(f, \chi_d(\alpha)^{-1}g[\alpha]_k) = (f, T_\alpha g).$$

\[\square\]

**Cor. (15.11.3.8) [Hecke Eigenforms].** The Hecke algebra is commutative and acts as self-adjoint operators on $S_k(N, \chi)$, thus there is a basis consisting of eigenfunctions for each $T_\alpha$, called the **Hecke eigenforms**.

**Prop. (15.11.3.9) [$T(n)$].** Let $T(n)$ be the sum of operators $T_{\text{diag}(d_1, d_2)}$ where $d_1, d_2 \in \mathbb{N}, d_2|d_1$ and $d_1d_2 = n$.

Equivalently by Cartan decomposition, if $\Delta_n$ is the subset of $GL(2, \mathbb{Z}) \cap G_0(N)$ consisting of matrices of determinant $n$, then

$$\Delta_n = \coprod_{a, d > 0, ad = n, b \mod d} \Gamma_0(N) \begin{bmatrix} a & b \\ d & d \end{bmatrix}$$

and

$$T(n)f = \sum_{a, d > 0, ad = n, b \mod d} \chi(d)^{-1}f \begin{bmatrix} a & b \\ d & d \end{bmatrix}|_k.$$

**Proof:** By column reduction, we can make any matrix in $\Delta_n$ the form as above, and if two elements of the form $\begin{bmatrix} a & b \\ d & d \end{bmatrix}$ differ by an element of $\Gamma_0(N)$, they differ by an upper-triangular matrix in $\Gamma_0(N)$, thus $a, d$ are determined, and also $b \mod d$. \[\square\]

**Cor. (15.11.3.10).**

- $T(1) = \text{id}$.
- If $(m, n) = 1$, then $T(m) \cdot T(n) = T(mn)$.
- If $p$ is a prime that $(p, N) = 1$ and $n \geq 1$, then $T(p^n) \cdot T(p) = T(p^{n+1}) + pR(p) \cdot T(p^{n-1})$, where $R(p)$ is the coset $\Gamma_0(N) \begin{bmatrix} p \\ p \end{bmatrix}$.
- $\mathcal{R}_N$ is generated by $T(p), R(p), R(p)^{-1}$.

**Proof:**

1: Trivial.
2: This follows from Chinese remainder theorem.
3: Omitted. \[\square\]

**Prop. (15.11.3.11) [Explicit Hecke Operators].** Let $f = \sum A(m)q^m \in S_k(N, \chi)$, then for $(n, N) = 1, T(n)f$ has a Fourier expansion

$$T(n)f = \sum B(m)q^m,$$

where

$$B(m) = \sum_{ad = n, a|m} (\frac{a}{d})^{k/2}\chi(d)^{-1}dA\left(\frac{md}{a}\right).$$
Proof:
\[
(T(n)f)(z) = \sum_{ad=n,b \mod d} \left(\frac{a}{d}\right)^{k/2} \chi(d)^{-1} f\left(\frac{az + b}{d}\right)
\]
\[
= \sum_{ad=n,b \mod d} \left(\frac{a}{d}\right)^{k/2} \sum_{m=1}^{\infty} A(m) \exp\left(2\pi i \frac{amz}{d}\right) \exp\left(2\pi i \frac{mb}{d}\right)
\]
\[
= \sum_{m=1}^{\infty} \sum_{ad=n,d|m} \left(\frac{a}{d}\right)^{k/2} \chi(d)^{-1} dA(m) \exp\left(2\pi i \frac{amz}{d}\right)
\]
Thus \(B(m) = \sum_{ad=n,a|m} \left(\frac{a}{d}\right)^{k/2} \chi(d)^{-1} dA\left(\frac{md}{a}\right)\). \(\square\)

Prop. (15.11.3.12)[Normalized Hecke Eigenforms]. If \(f = \sum c_n q^n \neq 0 \in M_k(N, \chi)\) that satisfies \(T(n)f = n^{1-k/2}\chi(n)^{-1}\lambda(n)f\) for all \((n, N) = 1\) and \(\lambda(n) \in \mathbb{C}\), then \(c_1 \neq 0\), and if \(f\) is normalized that \(c_1 = 1\), then \(c_n = \lambda(n)\) for all such \(n\). In particular, \(c_n\) are all real, because \(T(n)\) is Hermitian (15.11.3.7).

Proof: By (15.11.3.11),
\[
n^{1-k/2}\lambda(n)A(m) = \sum_{ad=n,a|m} \left(\frac{a}{d}\right)^{k/2} \chi(d)^{-1} dA\left(\frac{md}{a}\right),
\]
thus for \((m, n) = 1\), \(\lambda(n)A(m) = A(mn)\), and \(\lambda(n) = A(n)\). \(\square\)

New Forms

Def. (15.11.3.13)[Old and New Forms]. Let \(\alpha_d = \text{diag}(d, 1)\), and let \(S_k(\Gamma_1(N))[d]\) be the subspace of \(S_k(\Gamma_1(N))\) consisting of elements of the form \(f + g[\alpha_d]k, f, g \in S_k(\Gamma_1(N/d))\), and let
\[
S_k(\Gamma_1(N))_{\text{old}} = \sum_{p \in \mathbb{P}, p \nmid N} S_k(\Gamma_1(N))[p],
\]
called the space of old forms of level \(N\). Also the space
\[
S_k(\Gamma_1(N))_{\text{new}} = S_k(\Gamma_1(N))_{\text{old}}^\perp,
\]
called the space of new forms of level \(N\).

Remark (15.11.3.14). Omitting the \(p \in \mathbb{P}\) condition in the definition of oldforms doesn’t change the space.

Remark (15.11.3.15). The dimension of newforms and oldforms are calculated by \[\text{Dimensions of the Spaces of Cusp Forms and Newforms on } \Gamma_0(N) \text{ and } \Gamma_1(N)\].

Prop. (15.11.3.16). \(S_k(\Gamma_1(N))_{\text{old}}\) and \(S_k(\Gamma_1(N))_{\text{new}}\) are both stable under action of \(\mathcal{R}_N\). In particular, they have a orthogonal basis of Hecke eigenforms for the Hecke operators, by (15.11.3.7)(15.11.3.8).

Proof: By (15.11.3.10), for \(R(n), R(n)(f + g[\alpha_p]p) = R(n)f + (R(n)g)[\alpha_p]\), for \(T(\ell), \ell \neq p, T(\ell)(f + g[\alpha_p]) = T(\ell)f + (T(\ell)g)[\alpha_p]\) because \(d\) is prime to \(\ell\). \(\square\)

Prop. (15.11.3.17)[Strong Multiplicity One]. If \(f \in S_k(\Gamma_0(N), \chi)_{\text{new}}, f' \in S_k(\Gamma_0(N'), \chi)_{\text{new}}\) are normalized new eigenforms having the same eigenvalues for a.e. \(T_p\), then \(N = N'\) and \(f = f'\).

Proof: Cf.[On some results of Artin and Lehner, Casselman]. \(\square\)
4 Dimension Formulae

Def. (15.11.4.1) [Notations]. In this subsection,
- \( \Gamma \) is a congruence subgroup of \( SL_2(\mathbb{Z}) \).
- \( g \) is the genus of \( X(\Gamma) \).
- \( d \) is the degree of the map \( X(\Gamma) \to X(1) \) which is equal to \([SL(2,\mathbb{Z}) : \{\pm 1\}\Gamma]\).
- \( \varepsilon_2 \) the number of elliptic points with period 2.
- \( \varepsilon_3 \) the number of elliptic points with period 3.
- \( \varepsilon_\infty \) the number of cusps.
- \( \varepsilon_\text{reg}_\infty \) the number of regular cusps (15.7.1.7).
- \( \varepsilon_\text{irr}_\infty \) the number of irregular cusps.

Prop. (15.11.4.2) [Genus Formula].
\[
g = 1 + \frac{d}{12} - \frac{\varepsilon_2}{4} - \frac{\varepsilon_3}{3} - \frac{\varepsilon_\infty}{2}.
\]

Proof: Cf. [Diamond, P68].

Prop. (15.11.4.3) [Zeros and Poles of Automorphic Forms]. Let \( f \) be a meromorphic forms for \( \Gamma \) of weight \( 2k \), then
\[
\frac{1}{2} \sum_{Q \text{ elliptic points with period } 2} \text{ord}_Q(f) + \frac{1}{3} \sum_{Q \text{ elliptic points with period } 3} \text{ord}_Q(f) + \sum_{Q \text{ others}} \text{ord}_Q(f) = kd/6,
\]
where the sum is over a set of representatives for points in \( \Gamma \backslash \mathcal{H}^* \).

Proof: Cf. [Milne, P53].

Prop. (15.11.4.4) [Dimension Formulae for \( k \) Even]. If \( k \) is even, then
\[
\dim(M_k(\Gamma)) = \begin{cases} 
\left\lfloor \frac{k-1}{12} \right\rfloor + \frac{1}{4} - \{\frac{k}{4}\} \varepsilon_2 + \frac{1}{3} - \{\frac{k}{3}\} \varepsilon_3 + \frac{1}{2} \varepsilon_\infty & k \geq 2 \\
1 & k = 0 \\
0 & k < 0 
\end{cases}
\]
and
\[
\dim(S_k(\Gamma)) = \begin{cases} 
\left\lfloor \frac{k-1}{12} \right\rfloor + \frac{1}{4} - \{\frac{k}{4}\} \varepsilon_2 + \frac{1}{3} - \{\frac{k}{3}\} \varepsilon_3 - \frac{1}{2} \varepsilon_\infty & k \geq 4 \\
g & k = 2 \\
0 & k \leq 0 
\end{cases}
\]

Proof: Cf. [Diamond P87].

Cor. (15.11.4.5) [Modular Forms for \( SL(2,\mathbb{Z}) \)].
\[
M(\Gamma(1)) = \mathbb{C}[E_4, E_6], \quad S(\Gamma(1)) = \Delta \cdot M(\Gamma(1)).
\]
Thus for \( k \geq 4 \) even,
\[
\dim(S_k(\Gamma(1))) = \begin{cases} 
\left\lfloor \frac{k}{12} \right\rfloor - 1 & k \equiv 2 \mod 12 \\
\left\lfloor \frac{k}{12} \right\rfloor & \text{otherwise}
\end{cases}
\]
\[
M_k(\Gamma(1)) = S_k(\Gamma(1)) \oplus \mathbb{C}E_k.
\]
Proof: Cf.[Diamond P88].

**Cor. (15.11.4.6).** $M(\Gamma(1)) = M(\Gamma(1), \mathbb{Z}) \otimes \mathbb{C}$, $S(\Gamma(1)) = S(\Gamma(1), \mathbb{Z}) \otimes \mathbb{C}(15.11.8.4)$.

**Proof:** By(15.11.5.8), $E_4, E_6$ have Fourier coefficients in $\mathbb{Z}$. □

**Prop. (15.11.4.7) [Dimension Formulae for $k$ Odd].** For $k$ odd,

- if $k < 0$ or $-I \in \Gamma$, then $M_k(\Gamma) = S_k(\Gamma) = 0$.
- If $k \geq 3$, $-I \not\in \Gamma$, then
  \[
  \dim(M_k(\Gamma)) = (k-1)(g-1) + \left[ \frac{k}{3} e_3 + \frac{k}{2} e_{\infty}^\reg + \frac{k-1}{2} e_{\infty}^{\irr} \right] \\
  \dim(S_k(\Gamma)) = (k-1)(g-1) + \left[ \frac{k}{3} e_3 + \frac{k}{2} e_{\infty}^\reg + \frac{k-1}{2} e_{\infty}^{\irr} \right]
  \]
- If $k = 1$, $-I \not\in \Gamma$, then
  \[
  \dim(M_1(\Gamma)) = \begin{cases} 
  \frac{e_{\infty}^{\reg}}{2} & \text{if } e_{\infty}^{\reg} > 2g-2 \\
  \frac{e_{\infty}^{\reg}}{2} & \text{if } e_{\infty}^{\reg} \leq 2g-2
  \end{cases}, \\
  \dim(S_1(\Gamma)) = \dim(M_1(\Gamma)) - \frac{e_{\infty}^{\reg}}{2}
  \]

**Proof:** Cf.[Diamond P91]. □

### Explicite Dimension Formulae for $\Gamma(N), \Gamma_1(N), \Gamma_0(N)$

**Lemma (15.11.4.8).**

\[ SL(2, \mathbb{Z}) \to SL(2, \mathbb{Z}/N\mathbb{Z}) \]

is surjective.

**Proof:** Cf.[D-S16]P101. □

**Prop. (15.11.4.9) [Degree].**

- The degree of the mapping $X(N) \to X(1)$ is
  \[ d = d_N = [SL(2, \mathbb{Z}) : \{\pm 1\}\Gamma(N)] = \begin{cases} 
  \frac{1}{6}N^3 \prod_{p \mid N}(1 - 1/p^2) & N > 2 \\
  1 & N = 2
  \end{cases} \]

  - There is a coset decomposition $\Gamma_1(N) = \prod_{j=1}^{N-1} \Gamma(N) \begin{bmatrix} 1 & j \\ 1 & 1 \end{bmatrix}$, in particular, $d = [SL(2, \mathbb{Z}) : \{\pm 1\}\Gamma_1(N)] = d_N/N, N \geq 2$.

  - There is a coset decomposition $\Gamma_0(N) = \prod_{y \mod N, (y,N)=1} \Gamma_1(N) \begin{bmatrix} x & k \\ N & y \end{bmatrix}$, where $x, k$ are chosen so that $xy - kN = 1$. In particular, $d = [SL(2, \mathbb{Z}) : \Gamma_0(N)] = 2d/N \varphi(N), N \geq 2$.

**Proof:** 1: By(15.11.4.8), the map $SL(2, \mathbb{Z}) \to SL(2, \mathbb{Z}/N\mathbb{Z})$ is surjective, so $[\Gamma(N) : \Gamma(1)] = \#SL(2, \mathbb{Z}/N\mathbb{Z})$. Let $N = \prod p_i^{n_i}$, then $SL(2, \mathbb{Z}/N\mathbb{Z}) \cong \prod_i SL(2, \mathbb{Z}/p_i^{n_i}\mathbb{Z})$, and calculating depending on $e_{11}$ is invertible or $e_{12}$ is invertible, $\#SL(2, \mathbb{Z}/p_i^{n_i}\mathbb{Z}) = 2(p^{n_i} - p^{n_i-1})p^{2n_i} - (p^{n_i} - p^{n_i-1})^2p^{n_i} = p_i^{3n_i} - p_i^{3n_i-2}$. Thus $\#SL(2, \mathbb{Z}/N\mathbb{Z}) = N^3 \prod_{p \mid N}(1 - p^{-2})$, and we get the desired formula. □

**Prop. (15.11.4.10) [Elliptic Points].**
Cor. (15.11.4.11) [Elliptic Points of $X_0(p)$]. Let $p$ be a prime, then

- $\varepsilon_3(\Gamma_0(p)) = 1 + \left(\frac{-1}{p}\right)$, where $\left(\frac{-1}{2}\right) = 0$.
- $\varepsilon_2(\Gamma_0(p)) = 1 + \left(\frac{-3}{2}\right)$, where $\left(\frac{-3}{2}\right) = -1$.

**Proof:** Firstly there is a coset decomposition $\Gamma(1) = \Gamma_0(p)\alpha_j$, where $\alpha_j = \begin{bmatrix} 1 & 1 \\ j & 1 \end{bmatrix}$ when $j = 0, \ldots, p - 1$ and $\alpha_\infty = \begin{bmatrix} 1 & -1 \\ 1 & 0 \end{bmatrix}$.

Because $-1 \in \Gamma_0(p)$, if $\alpha_j(i)$ or $\alpha(\omega)$ is an elliptic point, we may assume that it is fixed by an element of order 4 or 6 resp. by (15.11.1.9). Notice $\alpha_j(i)$ is an elliptic point or equivalently $\alpha_j = \begin{bmatrix} 0 & -1 \\ 1 & 0 \end{bmatrix}$, $\alpha^{-1}_j \in \Gamma_0(p)$ iff $j \neq \infty$ and $j^2 + 1 \equiv 0 \mod p$. Thus $\varepsilon_2(\Gamma_0(p))$ equals the number of solutions to $j^2 = 1$, which is $1 + \left(\frac{-1}{p}\right)$. Similarly $\alpha_j(\omega)$ is an elliptic point or equivalently $\alpha_j = \begin{bmatrix} 0 & -1 \\ 1 & 1 \end{bmatrix}$, $\alpha^{-1}_j \in \Gamma_0(p)$ iff $j \neq \infty$ and $j^2 - j + 1 \equiv 0 \mod p$. Thus $\varepsilon_2(\Gamma_0(p))$ equals the number of solutions to $j^2 = 1$, which is $1 + \left(\frac{-1}{p}\right)$.

**Lemma (15.11.4.12).** Let $s = a/c, s' = a'/c' \in \mathbb{P}^1(\mathbb{Q})$ with $(a, c) = (a', c') = 1$, then for any $\gamma \in SL(2, \mathbb{Z})$,

$$s' = \gamma(s) \iff \begin{bmatrix} a' \\ c' \end{bmatrix} = \pm \gamma \begin{bmatrix} a \\ c \end{bmatrix}.$$  

**Proof:**

**Lemma (15.11.4.13).** Let $s = a/c, s' = a'/c' \in \mathbb{P}^1(\mathbb{Q})$ with $(a, c) = (a', c') = 1$, then

- $\Gamma(N)s' = \Gamma(N)s \iff \begin{bmatrix} a' \\ c' \end{bmatrix} \equiv \pm \begin{bmatrix} a \\ c \end{bmatrix} \mod N$
- $\Gamma_1(N)s' = \Gamma_1(N)s \iff \begin{bmatrix} a' \\ c' \end{bmatrix} \equiv \pm \begin{bmatrix} a + jc \\ c \end{bmatrix} \mod N$, for some $j$.
- $\Gamma_0(N)s' = \Gamma_0(N)s \iff \begin{bmatrix} ya' \\ c' \end{bmatrix} \equiv \begin{bmatrix} a + jc \\ c \end{bmatrix} \mod N$, for some $y$ relatively prime to $N$ and some $j$.

**Proof:** Use (15.11.4.12).

1: One direction is clear, for the other, If $\begin{bmatrix} a' \\ c' \end{bmatrix} \equiv \pm \begin{bmatrix} a \\ c \end{bmatrix} \mod N$, take $b, d$ that $ac - bd = 1$, then $\gamma = \begin{bmatrix} a & b \\ c & d \end{bmatrix}$ maps $\begin{bmatrix} 1 \\ 0 \end{bmatrix}$ to $\begin{bmatrix} a \\ c \end{bmatrix}$. As $\Gamma(N)$ is normal in $\Gamma(1)$, it suffices to prove for $\begin{bmatrix} a \\ c \end{bmatrix} = \begin{bmatrix} 1 \\ 0 \end{bmatrix}$. Then $a' \equiv 1 \mod N$, take integers $\beta, \delta$ that $a'\delta - c'\beta = (1 - a')/N$, let $\gamma = \begin{bmatrix} a' \\ c' \end{bmatrix} \begin{bmatrix} \beta N \\ \delta N \end{bmatrix}$, then $\gamma \in \Gamma(N)$ and $\begin{bmatrix} a' \\ c' \end{bmatrix} = \gamma \begin{bmatrix} 1 \\ 0 \end{bmatrix}$.

2 follows from 1 and the coset decomposition $\Gamma_1(N) = \coprod_{j=1}^{N} \Gamma(1) \begin{bmatrix} 1 \\ j \end{bmatrix}$.
There is a coset decomposition $\Gamma_0(N) = \bigsqcup\limits_{y \mod N, (y,N)=1} \Gamma_1(N) \begin{bmatrix} x & k \\ N & y \end{bmatrix}$, where $x, k$ are chosen so that $xy - kN = 1$. Then

$$\Gamma_0(N)s' = \Gamma_0(N)s \iff \begin{bmatrix} a' \\ c' \end{bmatrix} \equiv \pm \begin{bmatrix} xa + kc + jcy \\ cy \end{bmatrix} \mod N, \exists j, (y, N) = 1$$

$$\iff \begin{bmatrix} ya' \\ c' \end{bmatrix} \equiv \begin{bmatrix} a + jc \\ cy \end{bmatrix} \mod N, \exists j, (y, N) = 1$$

Prop. (15.11.4.14) [Cusps].

- $\varepsilon_\infty(\Gamma_0(N)) = \sum_{d|N} \varphi((d, N/d))$.

- $\varepsilon_3(\Gamma_0(N)) = \sum_{d|N} \varphi((d, N/d))$.

Proof: 1: By (15.11.4.13), if $\Gamma_0(N)s' = \Gamma_0(N)s$, then $\begin{bmatrix} ya' \\ c' \end{bmatrix} \equiv \begin{bmatrix} a + jc \\ cy \end{bmatrix} \mod N$, which means first $(c, N) = (c', N)$. So we consider the equivalence classes with $(c, N) = d$. In this case any equivalence class has a representative that $c = d$. Consider the equivalence relations between them, then $\begin{bmatrix} a' \\ d \end{bmatrix}$ represents the same cusp as $\begin{bmatrix} a \\ d \end{bmatrix}$ iff $(y_0 + iN/d)a' \equiv a + jd \mod N$ for some $i, j$, which is equivalent to $a' \equiv y_0a \mod (c, N, a'N/d) = (d, N/d)$. So there are $\sum_{d|N} \varphi((d, N/d))$ many equivalence classes(cusps). □

Prop. (15.11.4.15) [Regular Cusps]. All the cusps of $\Gamma_0(N)$ and $\Gamma(N)$ are regular. The only irregular cusp of $\Gamma_1(N)$ are $s = 1/2$ for $N = 4$.

Proof: Cf.[?P103]. □

Lemma (15.11.4.16). Lists of statistics for $\Gamma_0(N), \Gamma_1(N), \Gamma(N)$.

<table>
<thead>
<tr>
<th>$\Gamma$</th>
<th>$d$</th>
<th>$\varepsilon_2$</th>
<th>$\varepsilon_3$</th>
<th>$\varepsilon_\infty$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\Gamma_0(N), N &gt; 2$</td>
<td>$\frac{2dN}{N\varphi(N)}$</td>
<td>$\prod_{p</td>
<td>N}(1 + (\frac{2}{p}))$</td>
<td>$\prod_{p</td>
</tr>
<tr>
<td>$\Gamma_1(2)(\Gamma_0(2))$</td>
<td>3</td>
<td>1</td>
<td>0</td>
<td>2</td>
</tr>
<tr>
<td>$\Gamma_1(3)$</td>
<td>4</td>
<td>0</td>
<td>1</td>
<td>2</td>
</tr>
<tr>
<td>$\Gamma_1(4)$</td>
<td>6</td>
<td>0</td>
<td>0</td>
<td>3</td>
</tr>
<tr>
<td>$\Gamma_1(N), N &gt; 4$</td>
<td>$d_N/N$</td>
<td>0</td>
<td>0</td>
<td>$\frac{2}{3} \sum_{d</td>
</tr>
<tr>
<td>$\Gamma(1)(\Gamma_1(1))$</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$\Gamma(N), N &gt; 1$</td>
<td>$d_N$</td>
<td>0</td>
<td>0</td>
<td>$d_N/N$</td>
</tr>
</tbody>
</table>

where

$$d_N = \begin{cases} 1/2 \prod_{p|N} N^2 (1 - 1/p^2) & N > 2 \\ 6 & N = 2 \end{cases}$$

Proof: Cf.[Diamond P107]. □
**Prop. (15.11.4.17)** [List of Dimension Formulae]. Lists of dimension formulae for $\Gamma_0(N), \Gamma_1(N), \Gamma(N)$.

<table>
<thead>
<tr>
<th>$\Gamma$</th>
<th>$g$</th>
<th>$\dim(M_k(\Gamma)) &amp; \dim(S_k(\Gamma))$</th>
<th>$\dim(M_k(\Gamma)) &amp; \dim(S_k(\Gamma))$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$\Gamma_0(N), N &gt; 2$</td>
<td>expression too long</td>
<td>expression too long</td>
<td>expression too long</td>
</tr>
<tr>
<td>$\Gamma_1(2)(\Gamma_0(2))$</td>
<td>0</td>
<td>$[\frac{k}{4}] + 1$</td>
<td>0</td>
</tr>
<tr>
<td>$\Gamma_1(3)$</td>
<td>0</td>
<td>$[\frac{k}{3}] + 1$</td>
<td>$[\frac{k}{3}] + 1$</td>
</tr>
<tr>
<td>$\Gamma_1(4)$</td>
<td>0</td>
<td>$\frac{k-1}{2} \pm \frac{3}{2}$</td>
<td>$\frac{k-1}{2} \pm \frac{3}{2}$</td>
</tr>
<tr>
<td>$\Gamma_1(N), N &gt; 4$</td>
<td>$1 + \frac{d_N}{12N} - \frac{1}{4} \sum_{d</td>
<td>N} \varphi(d) \varphi(N/d)$</td>
<td>$\frac{(k-1)d_N}{12N} + \frac{1}{4} \sum_{d</td>
</tr>
<tr>
<td>$\Gamma(1)(\Gamma_1(1))$</td>
<td>0</td>
<td>1</td>
<td>1</td>
</tr>
<tr>
<td>$\Gamma(2)$</td>
<td>0</td>
<td>$\frac{k-1}{2} \pm \frac{3}{2}$</td>
<td>0</td>
</tr>
<tr>
<td>$\Gamma(N), N &gt; 2$</td>
<td>$1 + \frac{d_N(N-6)}{12N}$</td>
<td>0</td>
<td>$\frac{(k-1)d_N}{12N} + \frac{d_N}{2N}$</td>
</tr>
</tbody>
</table>

**Proof:** This follows from (15.11.4.4)(15.11.4.7)(15.11.4.16) and (15.11.4.15). \qed

**Remark (15.11.4.18).** The only case that is not calculated is the dimensions of $\dim(M_1(\Gamma))$.

**Cor. (15.11.4.19)** [Low Genus Cases]. For $N \in \mathbb{Z}_+$,

- $g(X(N)) = 0$ iff $N \in \{1, 2, 3, 4, 5\}$.
- $g(X(N)) = 1$ iff $N = 6$.
- $g(X_1(N)) = 0$ iff $N \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12\}$.
- $g(X_1(N)) = 1$ iff $N \in \{11, 14, 15\}$.
- $g(X_0(N)) = 0$ iff $N \in \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 12, 13, 16, 18, 25\}$.
- $g(X_0(N)) = 1$ iff $N \in \{11, 14, 15, 17, 19, 20, 21, 24, 27, 32, 36, 49\}$.

**Proof:** If $N = \prod_p p^{e_p}$,

1, 2:

3, 4:

$$g(X_1(N)) = 1 + \frac{1}{24} \prod_{p|N} p^{2e_p}(1 - \frac{1}{p^2}) - \frac{1}{4} \prod_{p} p^{e_p-2}(p - 1)(p + 1 - e_p(p - 1),$$

so if $g(X_1(N)) = 0$,

$$\prod_{p} \frac{p^{e_p}(p + 1)}{[(p + 1) + e_p(p - 1)]} < 6.$$ 

Then it can be verified that $e_2 \leq 3, e_3 \leq 2, e_5 \leq 1, e_7 \leq 1, e_{11} \leq 1, e_p = 0$ for $p > 11 \in \mathbb{P}$. Then the assertion follows. 4 is similar. \qed

**Applications**

**Prop. (15.11.4.20)**. Use dimension formula to prove four square problem, Cf. [D-S16] Chap1.
5 Eisenstein Series

Def. (15.11.5.1) [Eisenstein Series]. Let $\Gamma$ be a congruence subgroup of $\Gamma(1)$, define the space of Eisenstein series $E_k(\Gamma, \chi)$ to be the orthogonal complement of $S_k(\Gamma, \chi)$ in $M_k(\Gamma, \chi)$. Also denote $E_k(\Gamma) = E_k(\Gamma, 1)$.

Prop. (15.11.5.2) [Dimensions of Eisenstein Series]. Notation as in (15.11.4.1), by (15.11.4.4) and (15.11.4.7), the dimensions of the space of Eisenstein series satisfy:

$$\dim(E_k(\Gamma)) = \begin{cases} 
\varepsilon_{\infty} & k \geq 4, 2|k \\
\varepsilon_{\infty} - 1 & k = 2 \\
1 & k = 0 \\
\varepsilon_{\infty}^{\text{reg}} & k \geq 3, 2|k + 1, -1 \not\in \Gamma \\
\varepsilon_{\infty}^{\text{reg}}/2 & k = 1, -1 \not\in \Gamma \\
0 & k < 0 \text{ or } 2|k + 1, -1 \in \Gamma 
\end{cases}$$

And also the dimension of $E_k(\Gamma_0(N)), E_k(\Gamma_1(N)), E_k(\Gamma(N))$ can be read off from (15.11.4.17).

Eisenstein Series for $\Gamma(1)$

Def. (15.11.5.3). In this subsubsection, denote $q = e^{2\pi i z}$.

Prop. (15.11.5.4) [Weakly Modular Forms and Lattices]. Let $\mathcal{L}$ be the set of lattices in $\mathbb{C}$, If $F : \mathcal{L} \to \mathbb{C}$ is a function of weight $2k$, i.e. $F(\lambda \Lambda) = \lambda^{-2k} F(\Lambda)$ for $\lambda \in \mathbb{C}^*$, then $f(z) = F(\Lambda(z,1))$ is a weakly modular form on $\mathcal{H}$ for $\Gamma(1)$ of weight $2k$, and this is a bijection between functions of weight $2k$ on $\mathcal{L}$ and weakly modular functions on $\mathcal{H}$ for $\Gamma(1)$ of weight $2k$.

Proof: By the hypothesis, there is a function $f$ on $\mathcal{H}$ that for any $w_1, w_2$ with $w_1/w_2 \in \mathcal{H}$,

$$F(\Lambda(w_1, w_2)) = w_2^{-2k} f(w_1/w_2).$$

Then the invariance of $F$ under $SL(2, \mathbb{Z})$ action implies $f$ is weakly modular of weight $2k$. \qed

Prop. (15.11.5.5) [Eisenstein Series for $SL(2, \mathbb{Z})$]. Let $k > 2$ be an even integer and $\Lambda$ a lattice of $\mathbb{C}$, define the Eisenstein series of weight $k$ to be

$$G_k(\Lambda) = \sum_{\omega \in \Lambda, \omega \neq 0} \frac{1}{\omega^k},$$

and also for a complex number $z$, let $\Lambda_z$ be the lattice generated by $1$ and $z$, and let $G_k(z) = G_k(\Lambda_z)$. Then $G_k(z) \in M_k(\Gamma(1))$, and

$$G_k(z) = 2\zeta(k) + 2 \frac{(2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$$

And denote

$$E_k(z) = G_k(z)/2\zeta(k) = 1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$$

the normalized Eisenstein series.
Proof: $G_k(z)$ is weakly modular of weight $k$ by (15.11.5.4). For the expansion, notice by (10.5.3.12),

$$\pi \cot(\pi z) = \frac{1}{z} + \sum_{n=1}^{\infty} \left( \frac{1}{z+n} + \frac{1}{z-n} \right),$$

and by definition

$$z \cot(\pi z) = \pi i - \frac{\pi i}{1-q} = \pi i - 2\pi i \sum_{n=1}^{\infty} q^n$$

where $z \in \mathcal{H}$.

Taking $(k-1)$-th derivative of this, we get

$$\sum_{n \in \mathbb{Z}} \frac{1}{(z+n)^k} = \frac{(-2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} n^{k-1} q^n,$$

thus

$$G_k(z) = \sum_{(m,n) \neq (0,0)} \frac{1}{(nz+m)^k}$$

$$= 2\zeta(k) + 2 \sum_{n=1}^{\infty} \sum_{m \in \mathbb{Z}} \frac{1}{(nz+m)^k}$$

$$= 2\zeta(k) + \frac{2(-2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} d^{k-1} q^n$$

$$= 2\zeta(k) + \frac{2(2\pi i)^k}{(k-1)!} \sum_{n=1}^{\infty} \sigma_{k-1}(n) q^n$$

Finally the assertion about $E_k(z)$ follows from (16.2.3.27).

To show the Eisenstein series is orthogonal to any cusp form, notice for any cusp form $f \in S_k(\Gamma(1))$,

$$f(\gamma(z))(\text{Im}(\gamma z))^k = f(z) \frac{\tau(\gamma, z)^{-k}}{\text{Im}(z)^k}$$

and by (15.11.5.5)

$$G_k(z) = \sum_{(m,n) \neq (0,0)} \frac{1}{(nz+m)^k} = \sum_{\Gamma(1) \setminus \Gamma(1)} \frac{1}{\tau(\gamma, z)^k},$$

so

$$\int_{\Gamma(1) \setminus \mathcal{H}} f(z) \overline{G_k(z)} y^k \frac{dxdy}{y^2} = \int_{\Gamma(1) \setminus \mathcal{H}} \sum_{\Gamma(1) \setminus \Gamma(1)} f(z) \overline{\tau(\gamma, z)^{-k}} y^k \frac{dxdy}{y^2}$$

$$= \int_{\Gamma(1) \setminus \mathcal{H}} \sum_{\Gamma(1) \setminus \Gamma(1)} f(z)(\text{Im}(\gamma z))^k \frac{dxdy}{y^2}$$

$$= \int_{\Gamma(1) \setminus \mathcal{H}} f(z)(\text{Im} z)^k \frac{dxdy}{y^2}$$

$$= \int_{0}^{\infty} \left[ \int_{0}^{1} f(x+iy)dx \right] y^{k-2} dy = 0$$

as $f$ is a cusp form. \qed
Cor. (15.11.5.6). By \(15.11.5.5\) and \(10.5.3.10\):

\[
E_4(z) = 1 + 240 \sum_{n=1}^{\infty} \sigma_3(n)q^n, \quad E_6(z) = 1 - 504 \sum_{n=1}^{\infty} \sigma_5(n)q^n
\]

\[
E_8(z) = 1 + 480 \sum_{n=1}^{\infty} \sigma_7(n)q^n, \quad E_{10}(z) = 1 - 264 \sum_{n=1}^{\infty} \sigma_9(n)q^n
\]

\[
E_{12}(z) = 1 + \frac{65520}{691} \sum_{n=1}^{\infty} \sigma_3(n)q^n, \quad E_{14}(z) = 1 - 24 \sum_{n=1}^{\infty} \sigma_5(n)q^n.
\]

Cor. (15.11.5.7) [Ramanujan Identities]. By \(15.11.4.5\), \(\dim M_6(\Gamma(1)) = \dim M_8(\Gamma(1)) = \dim M_{10}(\Gamma(1)) = \dim M_{14}(\Gamma(1)) = 1\), thus there are equations

\[
E_2^2 = E_8, \quad E_4E_6 = E_{10}, \quad E_6E_8 = E_4E_{10} = E_{14}
\]

which give equations like:

\[
\sigma_7(n) = \sigma_3(n) + 120 \sum_{m=1}^{n-1} \sigma_3(m)\sigma_3(n-m)
\]

\[
11\sigma_9(n) = 21\sigma_5(n) - 10\sigma_3(n) + 1054 \sum_{m=1}^{n-1} \sigma_3(m)\sigma_5(n-m).
\]

Prop. (15.11.5.8) [Discriminant Function]. By \(15.11.5.6\), we can define the discriminant function

\[
\Delta(q(z)) = \frac{1}{1728}(E_4^3 - E_6^2) = q - 24q^2 + 252q^3 - 1472q^4 + \tau(5)q^5 + \ldots.
\]

So \(\Delta(z) \subset S_{12}(\Gamma(1))\), and the coefficients \(\tau(n)\) are called the Ramanujan \(\tau\)-function.

Cor. (15.11.5.9).

\[
E_6^2 - E_{12} = (-1008 - \frac{24 \cdot 2730}{691})\Delta.
\]

In particular, \(\tau(n) \equiv \sigma_{11}(n) \mod 691\).

Proof: Consider \(E_6^2 - E_{12} \in S_{12}(\Gamma(1))\), and \(S_{12}(\Gamma(1))\) is 1-dimensional and generated by \(\Delta(15.11.4.5)\), thus \(E_6^2 - E_{12} = c\Delta\) for some constant \(c \in \mathbb{C}\). By comparing the degree 1 term of both sides:

\[
\Delta(q(z)) = \frac{1}{1728}(E_4^3 - E_6^2) = q - 24q^2 + \ldots
\]

\[
E_{12}(z) = 1 + \frac{24 \cdot 2730}{691} \sum_{n=1}^{\infty} \sigma_{11}(n)q^n, \quad E_6(z) = 1 - 504 \sum_{n=1}^{\infty} \sigma_5(n)q^n
\]

by \(15.11.5.6\) and \(15.11.5.8\), so \(c = -1008 - \frac{24 \cdot 2730}{691}\). Then the formula

\[
691(E_6^2 - E_{12}) = 691c\Delta,
\]

modulo 691 gives \(\tau(n) \equiv \sigma_{11}(n) \mod 691\). \(\square\)
Cor. (15.11.5.10) [j-Function]. By (15.11.4.3), the discriminant function $\Delta(z)$ has exactly one simple zero at $\infty$, thus we can define the $j$-function on $H$ as

$$ j : H \to \mathbb{C}, j(q(z)) = \frac{E_4(z)^3}{\Delta(q(z))} = \frac{1}{q} + 744 + 196884q + 21493760q^2 + 864299970q^3 + \ldots \in \frac{1}{q} + \mathbb{Z}[[q]] $$

which is an automorphic function for $\Gamma(1)$, and it subjects onto $\mathbb{C}$.

Proof: To show it surjects onto $\mathbb{C}$, notice it induces a holomorphic map $X(1) \cong \mathbb{P}^1 \to \mathbb{P}^1$, and it maps $\infty$ to $\infty$ with no ramification, thus it has degree 1, so it is surjective. □

Prop. (15.11.5.11).

$$ \Delta(q(z)) = \eta(q(z))^{24} = q \prod_{n=1}^{\infty} (1 - q^n)^{24}. $$

where $\eta(z)$ is the Dedekind eta function from (7.5.2.6), and $\dim(S(SL(2, \mathbb{Z}))) = 1$, spanned by $\Delta$.

Proof: We show that $\eta^{24}(z)$ is a holomorphic cusp form in $S_{12}(\Gamma(1))$, and it has a first order pole at $\infty$ by the expression, and has no zero on $H$, thus it divides every cusp form in $S_{12}(\Gamma(1))$, and the quotient is a holomorphic modular function, thus is a constant. The assertion follows by comparing coefficients.

To show this, it suffices to show

$$ \eta(\gamma(z)) = \varepsilon(\gamma)(cz + d)^{1/2} \eta(z) $$

for every $\gamma \in \Gamma(1)$, where $\varepsilon(\gamma)$ is a 24-th root of unity. Because $[\gamma]_k$ is an action (15.11.1.10), by 6, it suffices to show for $S = \begin{bmatrix} 1 & -1 \\ 1 & 1 \end{bmatrix}$ and $T = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$. The case for $T$ is clear from the last expression of $\eta(z)$. For $S$: ? □

Def. (15.11.5.12) [Poincaré Series]. Let $\Gamma$ be a congruence subgroup, $T = \begin{bmatrix} 1 & 1 \\ 1 & 1 \end{bmatrix}$. Let $h$ be the minimal positive integer that $T^h \subset \Gamma$, and define $\Gamma_0$ the subgroup of $\Gamma$ generated by $T^h$. Then we define the Poincaré series of weight $2k$ and character $n$ for $\Gamma$ to be the series

$$ \varphi_n(z) = \sum_{\Gamma \setminus \Gamma'} \frac{\exp\left(\frac{2\pi i n \gamma(z)}{h}\right)}{(cz + d)^{2k}}, $$

where $\Gamma'$ is the image of $\Gamma$ in $\Gamma(1)/\{\pm 1\}$.

Prop. (15.11.5.13). For $k \geq 1, n \geq 0$, The Poincaré series converges absolutely on compact subsets of $H$, and is invariant under $\Gamma$-action, and it is a modular form of weight $2k$ for $\Gamma$. Moreover,

- $\varphi_0(z)$ vanishes at all finite cusps, and $\varphi_0(\infty) = 1$.
- for $n \geq 1$, $\varphi_n(z)$ are cusp forms.

Proof: Cf.[Mil, P62]. □

Prop. (15.11.5.14). The Poincaré series $\varphi_n(z)$ of weight $2k$ spans $S_{2k}(\Gamma)$.

Proof: Cf.[Mil17c]P62. □
General Eisenstein Series

Quasimodular Forms

Def.(15.11.5.15) [Almost Modular Forms and Quasimodular Forms]. For a discrete subgroup \( \Gamma \) of \( SL(2, \mathbb{R}) \), let \( \hat{M}_{k}^{\leq p}(\Gamma) \) be the space of functions in \( C^\infty(\mathcal{H}) \) of the form \( F(z) = \sum_{r=0}^{p} f_r(z)(-4\pi y)^{-r} \), where \( f_r \) are holomorphic on \( \mathcal{H} \) and holomorphic at the cusps, and \( F[\gamma]_k = F \) for any \( \gamma \in \Gamma \). Also denote \( \hat{M}_k(\Gamma) = \bigcup_{p=0}^{\infty} \hat{M}_{k}^{\leq p}(\Gamma) \) and the graded ring \( \hat{M}_*(\Gamma) = \bigoplus_{k \geq 0} \hat{M}_k(\Gamma) \), called the space of almost modular forms.

The graded ring \( \tilde{M}_*(\Gamma) \) consists of constant terms of functions in \( \hat{M}_*(\Gamma) \). Any almost modular function is determined by its constant term, so \( \tilde{M}_*(\Gamma) \) is canonically isomorphic to \( \hat{M}_*(\Gamma) \).

Def.(15.11.5.16) \([E_2(z)]\). Denote
\[
G_2(z) = \frac{1}{2} \sum_{n \neq 0} \frac{1}{n^2} + \sum_{m \neq 0} \sum_{n \in \mathbb{Z}} \frac{1}{(mz + n)^2}.
\]
This summation is convergent but not absolutely convergent, and
\[
E_2(z) = \frac{6}{\pi} G_2(z) = 1 - 24q - 72q^2 + \ldots \in \hat{M}_2^{\leq 1}(\Gamma(1))
\]
with
\[
G_2^* = G_2(z) - \frac{\pi}{2 \Im(z)}, \quad E_2^*(z) = \frac{6}{\pi} G_2^* = E_2(z) - \frac{3}{\pi y} \in \hat{M}_2^{\leq 1}(\Gamma(1)).
\]
In particular, \( E_2(z) \) satisfies
\[
E_2[\gamma]_2(z) = E_2(z) + \frac{12}{2\pi i cz + d}.
\]

Proof: \( \square \)

Prop.(15.11.5.17) [Derivations of Modular Forms]. Let \( f \in M_k(\Gamma(1)) \), then
\[
Df = f' = \frac{1}{2\pi i} \frac{\partial}{\partial z} f = \frac{q}{\partial q} f = \sum_{n=1}^{\infty} na_n q^n
\]
satisfies
\[
(Df)[\gamma]_{k+2}(z) = (Df)(z) + \frac{k}{2\pi i cz + d} f(z).
\]
In particular, by (15.11.5.16), \( \theta_k(f) = D(f) - \frac{k}{12} E_2 f \in M_{k+2}(\Gamma(1)) \), called the Serre derivation of \( f \).

Proof: This follows from differentiating the equation \( f(\frac{az+b}{cz+d}) = (cz+d)^k f(z) \). \( \square \)

Cor.(15.11.18).
\[
D(E_2) = \frac{E_2^2 - E_4}{12}, \quad D(E_4) = \frac{E_2 E_4 - E_6}{3}, \quad D(E_6) = \frac{E_2 E_6 - E_4}{2}
\]
Proof: \( D(E_4) \) and \( D(E_6) \) follows from (15.11.5.17) by comparing coefficients, for \( D(E_2) \), differentiating the equation \( E_2(\frac{az+b}{cz+d}) = (cz + d)^2 E_2(z) + \frac{12}{2\pi i} (cz + d) \), we get

\[
D(E_2)[\gamma](z) = D(E_2)(z) + \frac{2c}{2\pi i} E_2(z) + \frac{12c^2}{(2\pi i)^2} \frac{1}{(cz + d)^2}.
\]

Thus by (15.11.5.16), we see \( D(E_2) - \frac{E_2^2}{24} \in M_4(\Gamma(1)) \), then we can compare coefficients. \( \square \)

Prop. (15.11.5.19) [Structure of \( \tilde{M}_* (\Gamma) \)]. Let \( \Gamma \) be a discrete subgroup of \( SL(2, \mathbb{R}) \), then

- \( D(\tilde{M}_k^{\leq p}(\Gamma)) \subset \tilde{M}_k^{\leq p+1}(\Gamma) \). In particular, \( D(\tilde{M}_* (\Gamma)) \subset \tilde{M}_* (\Gamma) \).
- If \( \varphi \in \tilde{M}_2^{\leq 1}(\Gamma) \), then \( \tilde{M}_k^{\leq p}(\Gamma) = \oplus_{r=0}^{p} M_{k-2r}(\Gamma) \varphi^r \), for all \( k, p \geq 0 \). In particular, \( \tilde{M}_* (\Gamma(1)) = \mathbb{C}[E_2, E_4, E_6] \).
- If \( \varphi \in \tilde{M}_2^{\leq 1}(\Gamma) \), then for \( p, k \geq 0 \),

\[
\tilde{M}_k^{\leq p}(\Gamma) = \begin{cases} \oplus_{r=0}^{p} D^r(M_{k-2r}(\Gamma)), & p < k/2 \\ \oplus_{r=2}^{k/2-1} D^r(M_{k-2r}(\Gamma)) \oplus \mathbb{C} \cdot D^{k/2-1} \varphi, & p \geq k/2 \end{cases}
\]

Proof: Cf.[BGHZ]P59. \( \square \)

6 Eichler-Shimura Relations

7 Moduli Characterization

Prop. (15.11.7.1) [Elliptic Curves and Modular Curves]. Modular curves \( Y_0(N), Y_1(N), Y(N) \) parametrizes elliptic curves over \( \mathbb{C} \) with additional structures.

Proof: \( \square \)

Thm. (15.11.7.2) [Modularity Theorem]. Any elliptic curve over \( \mathbb{C} \) with rational \( j \)-invariant arises from a modular form.

8 Arithmetics

Prop. (15.11.8.1) [Number Field of \( f \)]. If \( f \in S_k(\Gamma_1(N)) \) is a normalized eigenform, then the coefficients \( a_n(f) \) are algebraic integers, and generate a number field \( K_f \), called the number field of \( f \).

Proof: Cf.[Diamond, P238]. \( \square \)

Prop. (15.11.8.2). if \( f \in S_2(N, \chi) \) is a normalized eigenform, then for any \( \sigma \in \text{Gal}_\mathbb{Q} \), \( f^\sigma \) is also a normalized eigenform in \( S_2(N, \chi^\sigma) \), where \( \chi^\sigma(n) = \chi(n)^\sigma \). And if \( f \) is a newform, then so is \( f^\sigma \).

Proof: Cf.[Diamond, P239]. \( \square \)

Cor. (15.11.8.3) [Integrality of Modular Forms]. \( S_2(\Gamma_1(N)) \) has a basis of modular forms with integral coefficients.
Proof: Let \( f \in S_2(\Gamma_1(N)) \) be a newform of level \( M|N \), and \( K_f \) the number field of \( f \). Let \( \alpha_1, \ldots, \alpha_d \) be a \( \mathbb{Z} \)-basis of \( \mathcal{O}_K \), and \( \Sigma = \{ \sigma_1, \ldots, \sigma_d \} \) the set of embeddings of \( K \) into \( \mathbb{C} \). Let

\[
g_i = \sum_{j=1}^{d} \sigma_j(\alpha_i)f^{\sigma_j},
\]

then by linear independence of characters, the matrix \((\sigma_i(\alpha_j))\) is non-degenerate, so \( \text{span}\{g_1, \ldots, g_d\} = \text{span}\{f, \ldots, f^{\sigma_d}\} \) by (15.11.8.2). Then by (15.11.3.13), applying this for all old and new forms of \( S_2(\Gamma_1(N)) \), the assertion follows. \( \square \)

**Prop.(15.11.8.4)** [Integral Modular Forms]. If \( A \subset \mathbb{C} \) be a subring, denote \( M_k(\Gamma, A) = M_k(\Gamma) \cap A[[q]] \).

**Def.(15.11.9.1)** [Modular Forms Mod \( p \)]. Define \( M_k(\Gamma, F_p) = M_k(\Gamma, \mathbb{Z}) \otimes F_p \), called the space of modular forms mod \( p \) of weight \( k \).

**Prop.(15.11.9.2)** [Serre’s Equality]. There is an isomorphism \( M_{p+1}(SL(2, \mathbb{Z}), F_p) \cong M_2(\Gamma_0(p), F_p) \).

**Proof:** Because \( E_k(z)1 - \frac{2k}{B_k} \sum_{n=1}^{\infty} \sigma_{k-1}(n)q^n \), and by Kummer’s congruence (16.4.1.1) \( \text{ord}_p(B_{p-1}) = -1 \), thus \( E_{p-1} \mod 1 \mod p \). Then multiplying by \( E_{p-1} : M_2(\Gamma_0(p), F_p) \rightarrow M_{p+1}(\Gamma_0(p), F_p) \) raises the level by \( p - 1 \). Then we compose with the natural averaging map \( M_{p+1}(\Gamma_0(p), F_p) \rightarrow M_{p+1}(SL(2, \mathbb{Z}), F_p) \), which is dual to the natural inclusion \( M_{p+1}(SL(2, \mathbb{Z}), F_p) \rightarrow M_{p+1}(\Gamma_0(p), F_p) \).

Why isomorphism? \( \square \)

**10 Non-Congruent Modular Forms**

Cf.[Non-Congruent Modular Forms, Ling Long].

**Thm.(15.11.10.1)** [Unbounded Denominators Conjecture]. Let \( N \) be any positive integer and let \( f(\tau) \in \mathbb{Z}[[q^{1/N}]] \) for \( q = \exp(\pi i \tau) \) be a holomorphic function on the upper half plane. Suppose there exists an integer \( k \) and a finite index \( \Gamma \subset SL(2, \mathbb{Z}) \) that \( f \) is \( \Gamma \)-invariant, and \( f \) is meromorphic at the cusps of \( \Gamma \), then \( f(\tau) \) is a modular form for some congruent subgroup of \( SL(2, \mathbb{Z}) \).

**Proof:** Cf.[the Unbounded Denominator Conjecture]. \( \square \)
15.12 Overview of the Langlands Program

1 Langlands Program

Main references are [Lan70].

Def. (15.12.1.1) [Langland Dual Groups]. For any connected reductive group $G$ over a global field $F$, we want to define a complex analytic group $^LG_F$, and for each place $p$, a complex analytic group $^LG_{F_p}$, and complex analytic homomorphisms $^LG_{F_p} \to ^LG_F$ defined up to conjugacy. The definition is given in [Lan70].

Then for each complex analytic representation $\sigma$ of $^LG_F$ and automorphic representation $\pi$ of $G_{A(F)}$, we want to define an $L$-function

$$L(s, \sigma, \pi) = \prod_p L(s, \sigma_p, \pi_p)$$

that is convergent in some right half plane, and

$$L(s, \sigma_p, \pi_p) = \prod_{i=1}^n \frac{1}{1 - \alpha_i |\omega_p|^s}$$

for any non-Archimedean plane $p$, where $n = \text{deg} (\sigma_p)$.

Also there is a functional equation

$$L(s, \sigma, \pi) = \varepsilon(s, \sigma, \pi) L(1 - s, L\sigma, \pi)$$

with

$$\varepsilon(s, \sigma, \pi) = \prod_p \varepsilon(s, \sigma_p, \pi_p, \psi_{F_p})$$

for any non-trivial character $\psi$ of $F \backslash A(F)$, where the product is finite.

Conj. (15.12.1.2). Is it possible to define the local $L$-functions $L(s, \rho, \pi)$ and the local factors $\varepsilon(s, \rho, \pi, \psi_F)$ at the ramified primes that

$$L(s, \sigma, \pi) = \prod_p L(s, \sigma_p, \pi_p)$$

is meromorphic in the entire complex plane with only a finite number of poles and satisfies the functional equation.

Conj. (15.12.1.3). Suppose $G, G'$ are reductive groups over the local field $F$ and $G$ is quasi-split and $G'$ is an inner twist of $G$, then $^LG_F = ^LG'_{F}$. Is there a correspondence $\text{Irr}(G'_F) \to \text{Irr}(G_F)$ s.t. if $\pi = R(\pi')$, then $L(s, \rho, \pi) = L(s, \rho, \pi')$ for any representation $\rho$ of $^LG_F$?

Conj. (15.12.1.4) [Local Functorial Lifting]. Let $G, G'$ be two quasi-split groups over the local field $F$. Let $G$ split over $K$ and $K'$ where $F \subset K \subset K'$. Suppose $\varphi: ^LG'_{K'/F} \to ^LG_{K/F}$ is a complex analytic homomorphism that makes the diagram

$$
\begin{align*}
^LG'_{K'/F} & \to G(K'/F) \\
\downarrow \varphi & \\
^LG_{K/F} & \to G(K/F)
\end{align*}
$$
15.12. OVERVIEW OF THE LANDLANS PROGRAM 1577

commutative, is there a correspondence \( r_\varphi : \text{Irr}(G'_F) \rightarrow \text{Irr}(G_F) \) that if \( \pi = R_\varphi(\pi') \), then for any representation \( \rho \) of \( L^G_F \),

\[
L(s, \rho, \pi) = L(s, \rho \circ \varphi, \pi'), \varepsilon(s, \rho, \pi, \psi_F) = \varepsilon(s, \rho \circ \varphi, \pi', \psi_F).
\]

Such a correspondence is called a functorial lifting of \( \pi' \).

Some evidences of (15.12.1.6) is given in [Lan70]P17.

**Global Langlands Conjectures**

**Prop. (15.12.1.5) [Langlands L-function].** Let \( F \) be a global field, \( A = A_F \), and \( G \) a reductive algebra over \( F \), \((\pi, V)\) an automorphic cuspidal representation of \( G(A) \), \((\pi, V) = \prod_v(\pi_v, V_v)\). Let \( S \) be a finite set of primes including the Archimedean ones and places that \( \pi_v \) is ramified or the field \( \Omega/F \) defining \( L^G \) is unramified. Let \( r : L^G \rightarrow GL(m, C) \) be a complex homomorphism, for \( v \notin S \), let \( \alpha_v \) be the semisimple conjugacy class in \( L^G_v \) parametrizing \( \pi_v \), then we define

\[ L_v(s, \pi_v, r_v) = \frac{1}{\det(I - q_v^{-s}r_v(\alpha_v))}, \quad L_S(s, \pi, r) = \pi_{v\notin S}L_v(s, \pi_v, r_v) \]

called the Langlands L-functions attached to \( \pi \) and \( r \). Langlands proved in [Euler Products, 1971] that such a product is convergent and analytic for \( \text{Re}(s) \) sufficiently large.

**Conj. (15.12.1.6) [Global Functorial Lifting].** Suppose \( G, G' \) are two quasi-split groups over the global field \( F \). Let \( G \) split over \( K \) and \( K' \) where \( F \subset K \subset K' \). Suppose \( \varphi : L^G_{K'/F} \rightarrow L^G_{K/F} \) is a complex analytic homomorphism that makes the diagram

\[
\begin{array}{ccc}
L^G_{K'/F} & \rightarrow & G(K'/F) \\
\downarrow \varphi & & \downarrow \\
L^G_{K/F} & \rightarrow & G(K/F)
\end{array}
\]

commutative. If \( \mathfrak{P}' \) is a prime of \( K' \), \( \mathfrak{P} = \mathfrak{P}' \cap K, p = \mathfrak{P}' \cap F \), then \( \varphi \) determines a homomorphism \( \varphi_p : L^G_{K'_{\mathfrak{P}'}/F_p} \rightarrow L^G_{K_{\mathfrak{P}}/F_p} \) that makes the diagram

\[
\begin{array}{ccc}
L^G_{K'_{\mathfrak{P}'}/F_p} & \rightarrow & G(K'_{\mathfrak{P}'}/F_p) \\
\downarrow \varphi_p & & \downarrow \\
L^G_{K_{\mathfrak{P}}/F_p} & \rightarrow & G(K_{\mathfrak{P}}/F_p)
\end{array}
\]

commutative. If \( \pi' = \otimes_p \pi'_p \) is an automorphic representation of \( G'_F \), is it true that \( \pi = \otimes_p R_{\varphi_p}(\pi'_p) \) is an automorphic representation of \( G_F \)? Such an automorphic representation is called a functorial lifting or \( \pi' \).

**Remark (15.12.1.7).** This conjecture reduces the conjecture about a general group to the case of \( GL(n, F) \), which can be handled, such as by [Zeta Functions of Simple Algebras, Godement/Jacquet].

**Conj. (15.12.1.8).** If (15.12.1.3) is true, if \( G, G' \) are defined over the global field \( F \) and \( G \) is quasi-split and \( G' \) is an inner twist of \( G \), suppose \( \pi' = \otimes_p \pi'_p \) is an automorphic representation of \( G'_F \), is it true that \( \pi = \otimes_p R(\pi'_p) \) is an automorphism representation of \( G_F \)?

**Conj. (15.12.1.9).**
Relation to Artin L-Functions

If $F$ is a local field and $\phi_F$ is a non-trivial additive character of $F$, then for any representation $\sigma$ of $W_{K/F}$ we can define a local L-function $L(s, \sigma)$ and local factors $\varepsilon(s, \sigma, \psi_F)$ that if $F$ is a global field and $\sigma$ is a representation of $W_{K/F}$, then

$$L(s, \sigma) = \prod_p L(s, \sigma_p), \quad \varepsilon(s, \sigma) = \prod_p \varepsilon(s, \sigma_p, \psi_{F_p})$$

satisfies the functional equation

$$L(s, \sigma) = \varepsilon(s, \sigma)L(1 - s, L\sigma).$$

Conj. (15.12.1.10). Suppose $G$ is quasi-split over the local field $F$ and splits over the Galois extension $K$. Let $LU_K$ be a maximal compact subgroup of $L_G F$. Let $K'$ be a Galois extension of $F$ containing $K$ and let $\varphi : W_{K'/F} \to LU_F$ be a homomorphism that makes the diagram

$$\begin{array}{ccc}
W_{K'/F} & \longrightarrow & G(K'/F) \\
\downarrow \varphi & & \downarrow \\
LU_F & \longrightarrow & G(K/F)
\end{array}$$

commutative, then there is an irreducible unitary representation $\pi(\varphi)$ of $G_F$ s.t. for any representation $\sigma$ of $L_G F$, $L(s, \sigma, \pi(\varphi)) = L(s, \sigma \circ \varphi)$, and $\varepsilon(s, \sigma, \pi(\varphi), \psi_F) = \varepsilon(s, \sigma \circ \varphi, \psi_F)$.

Conj. (15.12.1.11). Suppose $G$ is quasi-split over the local field $F$ and splits over the Galois extension $K$. Let $LU_K$ be a maximal compact subgroup of $L_G F$. Let $K'$ be a Galois extension of $F$ containing $K$ and let $\varphi : W_{K'/F} \to LU_F$ be a homomorphism that makes the diagram

$$\begin{array}{ccc}
W_{K'/F} & \longrightarrow & G(K'/F) \\
\downarrow \varphi & & \downarrow \\
LU_F & \longrightarrow & G(K/F)
\end{array}$$

commutative. If $\mathfrak{p}'$ is a prime of $K'$ and $\mathfrak{p} = \mathfrak{p}' \cap F$, then $\varphi_{\mathfrak{p}} = \varphi \circ \alpha_\mathfrak{p}$ takes $W_{K'_\mathfrak{p}'/F_\mathfrak{p}}$ into $LU_{F_\mathfrak{p}}$. If $\pi(\varphi) = \otimes_\mathfrak{p} \pi(\varphi_{\mathfrak{p}})$, is $\pi(\varphi)$ an automorphic representation?

Relation to Elliptic Curves

Conj. (15.12.1.12). If $C$ is an elliptic curve defined over a local number field $F$, we can associate to it a representation $\pi(C/F)$ of $GL(2, F)$? If $C$ is an elliptic curve defined over a global number field $F$, then for any place $\mathfrak{p}$, $\pi(C/F_\mathfrak{p})$ is defined. Is it true that $\pi(C/F) = \otimes_\mathfrak{p} \pi(C/F_\mathfrak{p})$ is an automorphism representation?

2 Local Langlands

Archimedean Local Langlands for $GL(n)$

Cf. [Local Langlands Correspondence, the Archimedean case, Knapp(1994)].
LLC for GL(n) over Function Fields


3 Global Langlands Correspondence

Def. (15.12.3.1) [L-Packets]. It is possible that two automorphic representations $\pi$ and $\pi'$ of $G(A)$ have the same L-function, and for any reductive group $H$ over $F$ and $\sigma$ an automorphic representation of $H(A)$ and $r_1$ a complex analytic representation of $^L H$,

$$L_S(s, \pi \otimes \sigma, r \otimes r_1) = L_S(s, \pi' \otimes \sigma, r \otimes r_1).$$

In this case, $\pi, \pi'$ are called to be in the same L-packet.

Prop. (15.12.3.2). Any L-packet is finite. And it is conjectured that every L-packet contains a generic representation.

4 Beyond Endoscopy

References are [Problems Beyond Endoscopy, Arthur].
15.13 Local Langlands for $GL(n)$ over $p$-Adic Fields

Main references are [?], [Bus19] and [The Local Langlands correspondence, the Non-Archimedean Case, Kudla(1994)].

Let $F$ be a $p$-adic local field.

Prop. (15.13.0.1). If $G$ is a split almost simple algebraic group defined over $F$, then it is isogenous to one of the following groups: $SL(n), SO(n), Sp(n), G_2, F_4, E_6, E_7, E_8$.

It is false in general that maximal compact subgroups of $G$ are conjugate. However, there are special maximal compact subgroups, and an irreducible admissible representation of $G(F)$ is called spherical if it is fixed by the special maximal compact subgroup.

Proof: ?

Prop. (15.13.0.2) [Langland’s Formation of the Satake Isomorphism]. If $G$ is split, then $H_K$ is isomorphic to ring generated by the characters of irreducible analytic f.d. representations of $L^0 G$, and the spherical representations of $G(F)$ are parametrized by the semisimple conjugacy classes in $L^0 G$.

If $G$ is non-split but splits over an unramified Galois extension $\Omega/F$, let $\Phi$ be the Frobenius element in $G(\Omega/F)$, and consider the cosets $L^0 G \Phi \subset L^0 G$, then $H_K$ is isomorphic to the ring of functions on this coset that are generated by the restrictions of characters of irreducible representations of $L^0 G$, and the spherical representations of $G(F)$ are parametrized by the semisimple conjugacy classes in $L^0 G$ in this coset.

1 Local Langlands for $p$-adic $GL(n)$

References are [M. Harris, R. Taylor: The geometry and cohomology of some simple Shimura varieties], [The Local Langlands Correspondence for GL(n) over p-adic Fields, Wedhorn], [Yao17].

For representations of the Weil group $W_F$, Cf.3.

Cor. (15.13.1.1) [LLC for $GL(1)$].

Local class field theory told us that $W^\text{ab}_K$ is isometric to $K^*$. And notice by Schur’s lemma, any smooth representation of $K^*$ is 1-dimensional and factors through some $U_K$.

And a Weil-Deligne representation is now a continuous $W^\text{ab}_K \rightarrow \mathbb{C}^*$. but it must factor through some $U_K$, so these two are equivalent.

Lemma (15.13.1.2) [Jacquet-Langlands]. Let $F$ be a local field and $E/F$ be a quadratic extension.

If $\chi$ is a quasi-character of $W_E$, and $\rho : W_F \rightarrow GL(2, \mathbb{C})$ the induced representation of $W_F$, then $\pi(\rho)$ in (15.12.1.10) exists.

Proof: Cf.[Bump, P556].

Thm. (15.13.1.3) [LLC for $GL(n)$]. There exists a unique collection of bijections $\text{rec}_n$ between sets:

$$\text{rec}_n : \text{Irr}^\text{adm}(GL(n, F)) \cong w^\text{ss}_{\dim - n}(W_F).$$

satisfying the following properties:

- For a quasi-character $\chi$ of $K^*$, $\text{rec}_1(\chi) = \chi \circ \text{Art}$.
15.13. LOCAL LANGLANDS FOR $GL(N)$ OVER $P$-ADIC FIELDS

- For every pair $\pi_1, \pi_2 \in \text{Irr}^{\text{ad}}(GL(n, F))$,
  
  $$L(\pi_1 \times \pi_2, s) = L(\text{rec}_{n_1}(\pi_1) \otimes \text{rec}_{n_2}(\pi_2), s), \quad \varepsilon(\pi_1 \times \pi_2, s) = \varepsilon(\text{rec}_{n_1}(\pi_1) \otimes \text{rec}_{n_2}(\pi_2), s).$$

- For a quasi-character $\chi$ of $K^*$ and $\pi \in \text{Irr}^{\text{ad}}(GL(n, K))$,
  
  $$\text{rec}_n((\chi \circ \text{det}) \otimes \pi) = \text{rec}_n(\pi) \otimes \text{rec}_1(\chi).$$

- For any $\pi \in \text{Irr}^{\text{ad}}(GL(n, F))$ with central character $\omega$, $\text{det} \circ \text{rec}_n(\pi) = \text{rec}_1(\omega)$.

Moreover, these bijections also preserves two more invariants:

- Conductor: $c(\pi) = c(\text{rec}_n(\pi))$.
- Depth: $d(\pi) = d(\text{rec}_n(\pi))$.


Lemma (15.13.1.4) [Plan of Proof]. By Bernstein-Zelevinsky classification(15.8.4.1), it suffices to construct $\text{rec}_n$ for irreducible cuspidal representations, then for any $\pi = Q(\Delta_1, \ldots, \Delta_r) \in \text{Irr}^{\text{ad}}(GL(n, F))$, where $\Delta_i = \Delta_i(\pi_i, m_i), \sum n_im_i = n$, we can define

$$\text{rec}_n(\pi) = \bigoplus_{i=1}^r \text{Sp}_{m_i}(\text{rec}_{n_i}(\pi_i)).$$

By work of Henniart, it suffices to prove there exist maps $\text{rec}_n$ on irreducible cuspidal representations that satisfies these properties, because it will be automatically bijective and unique. His method is to use the numerical local Langlands correspondence.

Remark (15.13.1.5). It seems Scholze’s approach bypasses Henniart numerical local Langlands correspondence.

Prop. (15.13.1.6). Under the local langlands correspondence(15.13.1.3), $\pi \in \text{Irr}^{\text{ad}}(GL(n, F))$ is

- supercuspidal iff $\text{rec}_n(\pi)$ is irreducible.
- essentially square integrable iff $\text{rec}_n(\pi)$ is indecomposable.
- generic iff $L(\text{ad} \circ \text{rec}_n(\pi), s)$ has no pole at $s = 1$.

Proof: □

Prop. (15.13.1.7) [Inertia Correspondence]. Under the local langlands correspondence(15.13.1.3), for $\pi, \pi' \in \text{Irr}^{\text{ad}}(GL(n, F))$,

- $\pi|_K \cong \pi'|_K$ iff $\text{rec}_n(\pi)|_{I_F} \cong \text{rec}_n(\pi')|_{I_K}$.

- (Paskunas) Let $\tau$ be a Weil-Deligne inertia type of $I_K$ that extends to an $n$-dimensional irreducible $F$-semisimple representation of $W_K$, then there exists a unique irreducible smooth representation $\sigma_\tau$ of $K$ s.t. for any irreducible infinite-dimensional representation $\pi$ of $GL(n, F)$, $\pi|_K$ contains $\sigma_\tau$ iff $\text{rec}_n(\pi)|_{I_F} \cong \sigma$.

Proof: □

Prop. (15.13.1.8) [LLC for $GL(2)$]. Under the classification of $\text{Irr}^{\text{ad}}(GL(2, F))$ given in(15.8.4.4), the corresponding Weil-Deligne representations are

1. For $\pi$ supercuspidal, $\text{rec}_2(\pi) = (\rho, 0)$, $\rho$ irreducible, by(15.13.1.6).

2. For principal series $\chi_1 \times \chi_2$, $\text{rec}_2(\pi) = (\chi_1 \otimes \chi_2, 0)$.

3. For $1(\chi)$, $\text{rec}_2(\pi) = (\chi \oplus \chi(1), 0)$.

4. For $\pi = \text{St}_2(\chi)$, $\text{rec}_2(\chi) = \text{Sp}_2(\chi) = (\chi \oplus \chi(1), N)$, where $N$ sends $\chi$ to $\chi(1)$.

Proof: □
2 Cuspidal Representations
3 Simple Characters
4 Tame Lifting
5 Description of the Langlands Correspondence
15.14 Automorphic Forms Beyond GL(2)

Prop. (15.14.0.1) [Ramakrishnan, 2000]. Multiplicity one theorem is true for cuspidal representations on $SL(2)$.

Proof: □

Prop. (15.14.0.2) [Blasius, 1994]. Multiplicity one theorem is false for cuspidal representations on $SL(n)$, $n \geq 3$.

Proof: □

1 Automorphic Forms on Unitary Groups

Main references are [Automorphic Forms on Unitary Groups, Eischen].

Unitary groups provide a particularly fruitful setting in which to work. Unitary groups have associated Shimura varieties, which provide convenient structure for studying algebraic aspects of automorphic forms (which, in turn, arise as sections of a vector bundle over Shimura varieties). We have substantial results about Galois representations associated to automorphic forms on unitary groups (e.g. [Ski12, Che04, Che09, CH13, Har10]). In addition, we have convenient representations of the L-functions associated automorphic forms on unitary groups, which are useful both for proving analytic properties and for extracting algebraic information (and even p-adic properties, as seen in [EHLS20]). Working with unitary groups has enabled major developments, including a proof of the main conjecture of Iwasawa Theory for GL2 [SU14] and the rationality of special values of certain automorphic L-functions (including [Shi00, Har97, Har08, Har84, Bou15]), as well as progress toward cases of the Bloch–Kato conjecture (including [SU06, Klo09, Klo15, Wan19]), and the Gan–Gross–Prasad conjecture (many recent developments, including [Xue14, Xue19, Zha14, Liu14, Yun11, JZ20, He17, BP20, BPLZZ21]).

2 Quaternionic Modular Forms

Main references are [Modular Forms on Exceptional Groups, Pollack].

3 Theta Correspondence

Classical Theta Functions

Def. (15.14.3.1) [Poisson Summation for Lattices]. Let $V$ be a vector space of dimension $n$ with an Haar measure $\mu$, $\Gamma \subset V$ a full lattice, and $\Gamma' \subset V^\vee$ be its $\mathbb{Z}$-dual, Let $V = \mu(V/\Gamma)$, then for any Schwartz function $f \in \mathcal{S}(V)$,

$$\sum_{x \in \Gamma} f(x) = \frac{1}{V} \sum_{y \in \Gamma'} \hat{f}(y).$$

Proof: This is just??.

Def. (15.14.3.2) [Theta function]. Let $\Gamma \subset V$ be a real inner product space with an Haar measure $\mu$ normalized that for an orthonormal basis $e_i$ of $V$, $V/\mathbb{Z}\{e_i\}$ has volume 1, then we can identify $V$ with $V^\vee$ by this inner product. Let $\Gamma$ be a full lattice, then its $\mathbb{Z}$-dual $\Gamma'$ is identified with a lattice in $V$ that $(x, y) \in \mathbb{Z}$ for any $x \in \Gamma, y \in \Gamma'$. 

Proof: This is just??.
The theta function \( \theta_{\Gamma}(z) \) is defined to be
\[
\theta_{\Gamma}(z) = \sum_{x \in \Gamma} q^{-(x,x)/2} = \sum_{x \in \Gamma} e^{-\pi i z (x,x)}, \text{Im}(z) > 0,
\]
and
\[
\Theta_{\Gamma}(t) = \theta_{\Gamma}(it) = \sum_{x \in \Gamma} e^{-\pi t (x,x)}
\]

**Cor. (15.14.3.3)**. With the notation as in (15.14.3.2), the theta function satisfies
\[
\Theta_{\Gamma}(t) = \frac{t^{-n/2}}{\mu(V/\Gamma)} \Theta_{\Gamma}(t^{-1})
\]

*Proof:* Notice that \( \Theta_{\Gamma^{-1}}(t) = \Theta_{\Gamma}(s^2 t) \), so this formula follows from (15.14.3.1) applied to \( t^{-1/2} \Gamma \) and \( f(x) = e^{-\pi (x,x)} \).

**Def. (15.14.3.4) [Self-Dual Lattices].** Situation as in (15.14.3.2), a self-dual lattice is a lattice \( \Gamma \) in \( V \) that \( V' = V \). Equivalently, if \( \{f_i\} \) is a \( \mathbb{Z} \)-basis of \( \Gamma \), then the matrix \( A = ((e_i, e_j)) \) is a matrix with integer coefficients and determinant 1. The last equivalence is because \( \Gamma' \subset \Gamma \) equals \( \Gamma \) if \( \mu(V/\Gamma) = \mu(V/\Gamma') \), but this is equivalent to \( \mu(V/\Gamma) = 1 \), because \( \mu(V/\Gamma) \cdot \mu(V/\Gamma') = 1 \).

A self-dual lattice is called even if \( (x, x) \in 2\mathbb{Z} \) for any \( x \in \Gamma \).

**Example (15.14.3.5) [\( E_{sk} \)].** Let \( V = \mathbb{R}^{sk} \) with the canonical inner product, denote \( E_{sk} \) the set of vectors \( \sum_i x_i e_i \) in \( V \) that
\[
2x_i \in \mathbb{Z}, x_i - x_j \in \mathbb{Z}, \sum_{i=1}^{sk} x_i \in 2\mathbb{Z}.
\]

Notice \( E_s \) is just the \( \mathbb{Z} \)-span of the root system \( E_s(2.7.3.2) \), and the root system just consists of all vectors in \( E_s \) of length \( \sqrt{2} \).

Then \( E_{sk} \) is a self-dual and even.

**Cor. (15.14.3.6).** Let \( k \geq 2 \), then all the vectors in \( E_{sk} \) of length \( \sqrt{2} \) are \( \{ \pm e_i \pm e_j | i \neq j \} \).

**Remark (15.14.3.7).** For more examples of self-dual lattices, see [Ser73] Chap 5.

**Prop. (15.14.3.8) [Theta Function for Self-Dual Even Lattices].** Let \( \Gamma \subset V \) be a self-dual even lattice (15.14.3.4), then the dimension \( n \) of \( V \) is divisible by 8, and the theta function \( \theta_{\Gamma}(z) \) is a modular form for \( \Gamma(1) \) of weight \( n/2 \).

*Proof:* We first show that
\[
\theta_{\Gamma}(-1/z) = (-iz)^{n/2} \theta_{\Gamma}(z)
\]
and because both sides are holomorphic functions on \( \mathcal{H} \), it suffices to show this for \( z = it, t > 0 \). Thus it suffices to show
\[
\Theta_{\Gamma}(t^{-1}) = t^{-n/2} \Theta_{\Gamma}(t).
\]
And this is just (15.14.3.3), because \( \Gamma \) is self-dual (15.14.3.4).

Then \( \theta_{\Gamma}[ST]_{n/2} = (-i)^{n/2} \theta_{\Gamma}(15.11.1.6) \), but \( (ST)^3 = 1 \), so \( (-i)^{3n/2} = 1 \), so \( 8|n \), and \( \theta_{\Gamma} \in M_{n/2}(\Gamma(1)) \).

\( \square \)
Prop. (15.14.3.9) [Theta Function for Non-Even Self-Dual Lattices]. If we consider theta function for non-even self-dual lattices in $\mathbb{R}^n$, then we get a modular form of weight $n/2$ w.r.t. the subgroup of $SL(2, \mathbb{Z})$ generated by the elements $S$ and $T^2$. This image of this subgroup has index 3 in $PSL(2, \mathbb{Z})$, and it has two cusps, thus two Eisenstein series.

In particular, we can apply this to the lattice $\{e_i\}$, and use this information to obtain formula giving the number of ways to represent an integer into a sum of $n$ squares.

Proof: 

4 Weil Representations

We use notations as in 3.

Def. (15.14.4.1) [Heisenberg Group of $O(V)$]. Let $F$ be a local or finite field of characteristic $\neq 2$, $(V, B)$ a quadratic space over $F$ of dimension $n$, $O(V) = O(V, B)$. Then the Heisenberg group $H$ is the group $V \times V \times F$ with the group law

$$(v^*_1, v_1, x_1)(v^*_2, v_2, x_2) = (v^*_1+v^*_2, v_1+v_2, x_1+x_2+B(v_2, v^*_1)-B(v_1, v^*_2)).$$

Let $\psi : F \rightarrow \mathbb{C}$ a non-trivial character. We may identify $V$ with $V^*$ via the pairing $(v, v^*) \mapsto \psi(-2B(v, v^*))$. Then the group $A(V)$ is $V \times V \times \mathbb{T}$ with multiplication

$$(v^*_1, v_1, t_1)(v^*_2, v_2, t_2) = (v^*_1+v^*_2, v_1+v_2, t_1t_2\psi(-2B(v_1, v^*_2))).$$

Then there is a surjective homomorphism $\tau : H \rightarrow A(V)$.

$A(V)$ acts on $L^2(G)$: $(\rho(v^*, v, t)\Phi)(u) = t\psi(-2B(u, v^*))\Phi(u+v)(10.9.3.20)$, and this induces an action $\pi$ of $H$ on $L^2(G)$: $(\rho(v^*, v, x)\Phi)(u) = t\psi(-2B(u, v^*))\Phi(u+v)$.

$SL(2, F)$ acts on $H$: $\begin{bmatrix} a & b \\ c & d \end{bmatrix} (v_1, v_2, x) = (av_1 + bv_2, cv_1 + dv_2, x)$, and acts on $A(V)$: $\begin{bmatrix} a & b \\ c & d \end{bmatrix} (v_1, v_2, t) = (av_1 + bv_2, cv_1 + dv_2, t\psi(-acB(v_1, v_1) - bdB(v_2, v_2)))$, these two actions are compatible with $\tau$.

$O(V)$ acts on $H$: $g(v_1, v_2, x) = (gv_1, gv_2, x)$, and a similar action on $A(V)$, compatible with $\tau$.

Recall the Fourier transform on $V$ w.r.t. the pairing $(v, v^*) \mapsto \psi(-2B(v, v^*))$.

Prop. (15.14.4.2). There exists a unitary projective representation $\omega_1$ of $Sp(2n, B)$ on $L^2(V)$ that for the subgroup $SL(2, F) \subset Sp(2n, B)$,

- For $g \in SL(2, F), h \in H, \omega_1(g)\pi(h)\omega_1(g)^{-1} = \pi(g(h)).$

- $$(\omega_1(\begin{bmatrix} 1 \\ x \\ 1 \end{bmatrix})\Phi)(v) = \psi(xB(v, v))\Phi(v).$$

- $$(\omega_1(\begin{bmatrix} a \\ a^{-1} \end{bmatrix})\Phi)(v) = |a|^{d/2}\chi(a)\Phi(av),$$ where $\chi(a)$ is any element that $|\chi(a)| = 1$.

- $\omega_1(w_1)\Phi = \gamma(B)\tilde{\Phi}$, where $\gamma(B)$ is any element that $|\gamma(B)| = 1$.

and there is a unitary representation $\omega_2$ of $O(V)$ on $L^2(V)$ that

- $\omega_2(k)\pi(h)\omega_2(k)^{-1} = \pi(k(h)).$

- $(\omega_2(k)\Phi)(v) = \Phi(k^{-1}v).$
\* \(\omega_2\) commutes with \(\omega_1\).

where \(\pi\) is a Schrödinger representation of \(A(V)\) on \(L^2(V)\) (10.9.3.21).

\textit{Proof:} Because the action of \(Sp(2n,B)\) on \(A(V)\) is in \(B_0(V)\), thus by (10.9.3.21), there are unitary automorphisms of \(L^2(G)\) that

\[
\omega_1(g)\pi(h)\omega_1(g)^{-1} = \pi(g(h)).
\]

Now to check the properties of \(\omega\), it suffices to check this equation for \(h = (v,0,1)\) or \((0,v,1)\) because these elements generate \(A(V)\), using the fact \(\rho\) action on \(L^2(V)\) is irreducible (10.9.3.21) ?

For \(O(V)\), just verify directly. \(\square\)

\textbf{Prop. (15.14.4.3) [dim \(V\) Even Case].} If \(F\) is a local or finite field of characteristic \(\neq 2\), \(V\) has dimension \(2n\), and if we define \(\Delta = (-1)^n \det(B) \in F^*/(F^*)^2\), \(\chi : F^* \to \{\pm 1\}\) the quadratic character \(a \mapsto (\Delta,a)_F(12.3.5.8)\), and \(\gamma(B)\) as defined in (12.3.5.9), then the projection representation of \(SL(2,F)\) in (15.14.4.2) is a true representation.

It suffices to check the relations (2.1.6.8). Use (12.3.5.14) to show that \(\gamma(B)^2 = \chi(-1)\). And it suffices to show that

\[
w_1\begin{bmatrix} a^{-1} & 1 \\ 1 & a \end{bmatrix} \begin{bmatrix} -a & 1 \\ 1 & -a \end{bmatrix} w_1 \begin{bmatrix} 1 & a \\ a & 1 \end{bmatrix} \Phi = \begin{bmatrix} 1 & a \\ a & 1 \end{bmatrix} w_1 \Phi
\]

The LHS equals \(\gamma(B)^2 |a|^{-n} F(\Phi \ast F_{-a^{-1}B})\), which by (12.3.5.9) and (12.3.5.13) equals \(\gamma(B) F(\Phi) F_{aB}\), which is just the RHS.

\textbf{Conj. (15.14.4.4) [Theta Correspondence (Special Case)].} Let \(\omega\) be the action of \(SL(2,F) \times O(V)\) on \(L^2(V)\) as in (15.14.4.3) and (15.14.4.2), then its smooth part \(C^\infty_c(V)\) is a smooth representation \(\omega_\infty\). Let \(\pi_1\) be an irreducible admissible representation of \(SL(2,F)\), \(\pi_2\) an irreducible admissible representation of \(O(V)\), they are said to correspond if there exists a non-zero intertwining operator \(\omega_\infty \to \pi_1 \otimes \pi_2\).

Then each \(\pi_1\) can corresponds to at most one \(\pi_2\), and vise versa.

\textit{Proof:} This is proved for non-Archimedean local fields of odd residue characteristic by Waldspurger (1990). \(\square\)

\textbf{Def. (15.14.4.5) [Setup for Dihedral Weil Representation].} Let \(F\) be local or finite field, and \(E\) be a 2-dimensional commutative semisimple algebra over \(F\), then \(E = F \oplus F\) and \(F\) embeds diagonally, called the split case; or \(E\) is the unique quadratic extension of \(F\), called the anisotropic case. Let the automorphism of \(E\) given by

\[
x \mapsto \overline{x} : \begin{cases} (\xi,\eta) = (\eta,\xi), \\ \text{The non-trivial Galois automorphism, } \ E = F \oplus F \end{cases}
\]

Let \(\text{tr}(x) = x + \overline{x}, N(x) = x\overline{x}\). Let \(E_1^* = \{x \in E^* | N(x) = 1\}\).

There is an embedding \(\iota\) of \(E\) into \(GO(E) \subset GL(2,F)\): for \(E = F \oplus F\), it embeds diagonally, and for \(E\) a field, \(E\) embeds by left action on itself. Notice \(\iota(x)(\overline{y}) = \iota(x)(y)\), thus \(GO(E) \cong E^* \rtimes \{\}\) ?.

Let \(\psi\) be a character of \(E^*\) that is non-trivial on \(E_1^*\).

\textbf{Prop. (15.14.4.6) [Howe Duality of Dihedral Representations].} Let \(\psi\) be a character of \(E^*\), then by (15.1.1.11), \(\psi\) extends to a representation of \(GO(E)\) iff \(\psi(x) = \psi(\overline{x})\), which is equivalent to
ψ(x) = 1 on $E_1^*$, by Hilbert’s theorem90 or direct inspection. Then by (15.1.1.11), in the other case, $\text{ind}^{GO(E)}_E\psi$ is an irreducible representation of $GO(E)$, and Howe duality predicts an irreducible smooth representation of $GL(2, F)$. In case $E$ is a field or $F$ is finite, we can construct this representation directly, in (15.14.4.7) and (15.4.10).8

Prop. (15.14.4.7) [Dihedral Representations]. Let $E/F$ be a quadratic extension of non-Archimedean local fields, then $E$ is a quadratic space over $F$ by the norm form, and let $\xi$ be a quasi-character of $E^*$ that does’t factor through the norm map $N : E^* \to F^*$. Let $U_{\xi,\psi}$ be the space of functions $\Phi \in C_c^\infty(E)$ that satisfy

$$\Phi(yv) = \xi(y)^{-1}\Phi(v), \quad \forall y \in E^*, N(y) = 1,$$

and let $\chi : F^* \to \{±1\}$ be the quadratic character attached to the extension $E/F$(12.4.2.13), and let $GL(2, F)_+$ be the subgroup of $GL(2, F)$ that the determinants are norms from $E$, which is an open normal subgroup of index2, then there exists an irreducible admissible representation $\omega_{\xi,\psi}$ of $GL(2, F)_+$ on $U_{\xi,\psi}$ s.t.

$$\omega_{\xi,\psi}\begin{bmatrix} a \\ 1 \end{bmatrix}(\Phi)(v) = |a|^{1/2}\xi(b)\Phi(bv), \quad \forall b \in E^*, N(b) = a \in F^*$$

$$\omega_{\xi,\psi}\begin{bmatrix} 1 \\ x \\ 1 \end{bmatrix}(\Phi)(v) = \psi(xN(v))\Phi(v)$$

$$\omega_{\xi,\psi}\begin{bmatrix} a \\ a^{-1} \end{bmatrix}(\Phi)(v) = |a|\xi(a)\Phi(av)$$

$$\omega_{\xi,\psi}(w_1)(\Phi) = \gamma(N)\Phi.$$

Then the representation $\omega_\xi$ of $GL(2, F)$ induced from this representation of $GL(2, F)_+$ is irreducible and cuspidal.

Remark (15.14.4.8). For $F$ with odd residue characteristic, this dihedral representation is the only cuspidal representation of $GL(2, F)$, by Tunnell 1978 or 1979.9

Proof: Notice in this case, the character $\chi$ defined in (15.14.4.3) is the same as the quadratic character corresponding to $E/F$: let $E = F(\sqrt{D})$, then $N_{E/F} = \langle 1, -D \rangle$, thus $(a, D)_F = 1$ iff $\langle a, D, -1 \rangle$ is universal iff $a$ is represented by $(1, -D)$, which is equivalent to $a \in N_{E/F}(E^*)$. Then by (15.14.4.3), we have an action of $SL(2, F)$ on $L^2(E)$, and we can extend it to $GL(2, F)_+$ satisfying all these equations(9) by direct verification. And it can be verified $U_{\xi,\psi}$ is stable under this action.

We show this action is smooth: Every $\varphi \in U_{\xi,\psi}$ is stable under some $K(p^n)$ for $n$ large. By (15.8.1.9), it suffices to prove it is stable under $N_-(p^n)$, $T(p^n)$ and $N(a)$. By action of $w_1$, it suffices to show it is stable under the latter two. But this is clear from the equations above.

Similarly, to show it is admissible, it suffices to show for any ideal $a$, the space of functions fixed by $N(a)$ and $N_-(a)$ is of f.d.: It is clear from equation2 that if $\varphi$ is fixed by $N(a)$, then there is a fractional ideal $a'$ that $\text{Supp}(\varphi) \subseteq N^{-1}(a')$. Similarly for $F(\varphi)$. These two conditions means $\varphi$ has bounded support and fixed by some open subgroup, these functions are f.d..

To show $\omega_{\xi,\psi}$ and $\omega_\xi$ are irreducible: Let $B_1(F)_+$ be the subgroup of $B_1(F)$ consisting of matrices

$$\left\{ \begin{bmatrix} a & b \\ 0 & 1 \end{bmatrix} | a \in N_{E/F}(E^*) \right\},$$

let $\mathcal{K}_+$ the restriction of $\omega_{\xi,\psi}$ to $B_1(F)_+$. Define a map

$$\Lambda : C_c^\infty(N(E^*)) \to \mathcal{K}_+ : (\Lambda \varphi)(v) = \xi(v)^{-1}|N(v)|^{-1/2}\varphi(N(v)),$$
then this is an isomorphism, and is $B_1(F)$-invariant, where $B_1(F)$ acts on $C^\infty_c(N(E^*))$ as in (15.8.3.15). Thus by Mackey decomposition (15.1.4.49),
\[
\text{res}_{B_1(F)} \text{ind}_{GL(2, F)_+} \omega_{\xi, \psi} \cong \text{ind}_{B_1(F)_+} \omega_{\xi, \psi} \cong \text{ind}_{N(F)} \psi,
\]
which is irreducible by (15.8.3.16). thus $\omega_{\xi}$ is irreducible, thus also does $\omega_{\xi, \psi}$.

A byproduct of the above argument is that $\omega_{\xi}$ is cuspidal. □

5 Gan-Gross-Prasad Conjecture

Main References are [Background on the Gan-Gross-Prasad Conjecture, David Schwein].
15.15 Representations of Semisimple Lie Algebras and Category \( \mathcal{O} \)

Main references are [Eti21] and [Car05].

This section studies representations of split semisimple Lie algebras. For a split semisimple Lie algebra \((\mathfrak{g}, \mathfrak{h})\), we use notations as in (2.5.3.30).

1 Semisimple Representations

**Lemma (15.15.1.1).** If \( \mathfrak{g} \) is a semisimple Lie algebra over \( k \), then every 1-dimensional representation of \( \mathfrak{g} \) is trivial.

**Proof:** Such a representation vanishes at \([\mathfrak{g}, \mathfrak{g}]\), which equals \( \mathfrak{g} \) by (2.5.2.4). \( \square \)

**Prop. (15.15.1.2)[Weyl].** For a Lie algebra \( \mathfrak{g} \) over a field \( k \),
- If the adjoint representation \( \mathfrak{g} \to \mathfrak{gl}(\mathfrak{g}) \) is semisimple, then \( \mathfrak{g} \) is semisimple.
- If \( \mathfrak{g} \) is semisimple and \( k \) has characteristic 0, then \( \text{Rep}(\mathfrak{g}) \) is semisimple.

**Proof:** If the adjoint representation of \( \mathfrak{g} \) is semisimple, then every ideal of \( \mathfrak{g} \) has a complement, thus if \( \mathfrak{g} \) is not semisimple, it has a dimension 1 quotient. But notice the Lie algebra \( k \) of dimension 1 has non-semisimple representations, for example \( c \mapsto \begin{bmatrix} 0 & 0 \\ c & 0 \end{bmatrix} \), contradiction.

Semisimplicity of a Lie algebra is invariant under base change, also does simplicity of the category of representations (15.15.1.4), so we can assume that \( k \) is alg.closed. Now we need to show that any proper submodule \( W \) of a \( \mathfrak{g} \)-module \( V \) has a complement.

Assume first that \( \dim V/W = 1 \) and \( W \) is a simple \( \mathfrak{g} \)-module. This implies \( \mathfrak{g} \) acts trivially on \( V/W \) by (15.15.1.1). Let \( c_V \) be the Casimir element of \( V(2.5.9.11) \), then \( c_V \) is also trivial on \( V/W \). And \( c_V \) acts as a nonzero scalar on \( W \) as \( W \) is simple, by (2.5.9.11). Then the kernel of \( c_V \) is of 1-dimensional, and is a \( \mathfrak{g} \)-complement of \( W \) in \( V \).

Next if \( \dim V/W = 1 \) but \( W \) is not simple \( \mathfrak{g} \)-module, then there is a submodule \( W' \subset W \). By induction, the \( \mathfrak{g} \)-submodule \( W/W' \) has a complement \( V'/W' \) in \( V/W' \). Then \( V'/W' \) has dimension 1, thus by induction, \( V' = W' \oplus L \) for some 1-dimensional \( \mathfrak{g} \)-module. Then \( L \) is complementary to \( W \) in \( V \).

Finally for the general case, let \( \mathfrak{g} \) acts on \( \text{Hom}_k(V, W) \), consider the subspaces \( V_1, W_1 \) of \( \text{Hom}_k(V, W) \), where \( V_1 \) is the subspace of maps that restriction to \( W \) is a constant multiple of identity, and \( W_1 \) is the subspaces of \( W \) consisting of maps vanishing on \( W \). They are both \( \mathfrak{g} \)-modules and \( \dim V_1/W_1 = 1 \). Then the above case shows \( V_1 = W_1 \oplus L \) for some 1-dimensional \( \mathfrak{g} \)-module \( L \). Because \( \mathfrak{g} \) acts trivially on \( L(15.15.1.1) \), this means \( L = \mathbb{F} f \) consists of \( \mathfrak{g} \)-homomorphisms. But \( f|_W \) is non-zero constant, so the kernel of \( f \) is a complement of \( W \) in \( V \). \( \square \)

**Cor. (15.15.1.3).** Let \((V, \rho)\) be a representation of a semisimple Lie algebra \( \mathfrak{g} \) and \( f : \mathfrak{g} \to V \) a linear map that
\[
 f([x, y]) = \rho(x)f(y) - \rho(y)f(x),
\]
then there exists a \( v_0 \in V \) that \( f(x) = \rho(x)v_0 \).

**Proof:** The condition on \( f \) is equivalent to \((f, \rho) : \mathfrak{g} \to \mathfrak{gl}(V)(2.5.1.11) \) is a homomorphism of Lie algebras. And this induces a representation \( \rho' \) of \( \mathfrak{g} \) on \( V' = V \oplus k \) that \( \rho'(x)(V') \subset V \) for all \( x \in \mathfrak{g} \). Because \( \mathfrak{g} \) is semisimple, there is a line \( L \subset V' \) that \( V' = V \oplus L \) and \( \mathfrak{g} \) acts trivially on \( L(15.15.1.1) \).
In other words, there is a vector \((-v_0, 1)\) that \(\rho'(x)(-v_0, 1) = 0\) for all \(x \in \mathfrak{g}\). So \(f(x) = \rho(x)(v_0)\) for all \(x\). So we are done. □

Prop. (15.15.1.4) [Semisimplicity and Extension]. Let \(\mathfrak{g}\) be a Lie algebra over a field \(k\). If \(\text{Rep}(\mathfrak{g}_K)\) is semisimple for some extension field \(K/k\), then also is \(\text{Rep}(\mathfrak{g})\).

Proof: This is because for any representation \((V, \rho)\) of \(\mathfrak{g}\), \(K \otimes_k \text{End}(\rho) \cong \text{End}(\rho_K)\), because this is true for \(\text{End}(V)\), and being \(\mathfrak{g}\)-equivariant is a linear condition. Then we can use(2.4.1.25) and(2.4.1.26). □

Prop. (15.15.1.5) [Semisimple Representations]. The following conditions on a representation \(\mathfrak{g} \to \mathfrak{gl}_V\) are equivalent:
- \(\rho\) is semisimple.
- \(\rho(\mathfrak{g})\) is reductive and its center consists of semisimple endomorphisms.
- \(\rho(\mathfrak{r})\) consists of semisimple endomorphisms.
- The restriction of \(\rho\) to \(\mathfrak{r}\) is semisimple.

Proof: 1 → 2: If \(\rho\) is semisimple, then \(\rho(\mathfrak{g})\) is reductive by (2.5.4.4). Its center consists of semisimple endomorphisms by [Mil13]P60?.

2 → 3: This is because if \(\rho(\mathfrak{g})\) is reductive, then its center equals its radical and contains \(\rho(\mathfrak{r})\), so \(\rho(\mathfrak{r})\) consists of semisimple endomorphisms.

3 → 4: [Mil13]P60?.

4 → 1: [Mil13]P60?. □

Cor. (15.15.1.6). Let \(\rho\) and \(\rho'\) be representations of \(\mathfrak{g}\). If \(\rho\) and \(\rho'\) are semisimple, then so are \(\rho \otimes \rho'\) and \(\rho'\).

In particular, the category \(\text{Rep}^{ss}(\mathfrak{g})\) of semisimple representations of a Lie algebra \(\mathfrak{g}\) form a Tannakian category, thus there is an algebraic group \(G\) that \(\text{Rep}^{ss}(\mathfrak{g}) = \text{Rep}(G)\).

Proof: Use the third criterion, for any \(x \in \mathfrak{r}\), as \(\rho(x), \rho'(x)\) are semisimple, so is \(\rho(x) \otimes \rho'(x)\), so \(\rho \otimes \rho'\) is also semisimple by(15.15.1.5). □

representations of \(\mathfrak{sl}_2(\mathbb{C})\)

Def. (15.15.1.7) [Primitive Element]. Let \(V\) be a \(\mathfrak{sl}_2\)-module, an element \(v \in V\) is called primitive of weight \(\lambda\) if it is non-zero and \(Xe = 0, He = \lambda e\).

Prop. (15.15.1.8). Every non-zero f.d. \(\mathfrak{sl}_2\)-module contains a primitive element.

Proof: en element \(e\) is primitive iff the line generated by \(e\) is stable under the action of \(\{X, H\}\): if \(Xe = \lambda e\) and \(He = \mu e\), then using the \([H, X] = 2X\), we see that \(2\lambda 0\), thus \(\lambda = 0\), and \(e\) is primitive. So each f.d. \(\mathfrak{sl}_2\)-module contains a primitive element, by Lie’s theorem(2.5.1.24). □

Prop. (15.15.1.9) [Submodule Generated by Primitive Element]. Let \(V\) be a \(\mathfrak{sl}_2\)-module and \(e \in V\) a primitive element of weight \(\lambda\). Let \(e_n = Y^n e/n!\), and \(e_{-1} = 0\), then we have

\[He_n = (\lambda - 2n)e_n, \quad Ye_n = (n + 1)e_{n+1}, \quad Xe_n = (\lambda - n + 1)e_{n-1}.\]
Proof: By induction on $n$,
\[
HY^n e = ([H,Y] + YH)Y^{n-1}e = (\lambda - 2(n-1) - 2)Y^{n-1}e = (\lambda - 2n)e.
\]

$Ye_n = (n+1)e_{n+1}$ is obvious.

And
\[
nXe_n = XYe_{n-1} = [X,Y]e_{n-1} + XYe_{n-1}
\]
\[
= He_{n-1} + (\lambda - n + 2)Ye_{n-2}
\]
\[
= (\lambda - 2n + 2 + (\lambda - n + 2)(n-1))e_{n-1}
\]
\[
= n(\lambda - n + 1)e_{n-1}
\]

\[\square\]

Cor. (15.15.1.10). Only two cases arise: either
- The elements $\{e_n\}$ are linearly independent.
- The elements $e_0, e_1, \ldots, e_m$ are linearly independent, and $e_{m+1} = e_{m+2} = \ldots = 0$, and weight $\lambda$ of $e$ equals $m$.

And if $V$ is f.d., then case 1 cannot happen, and the subspace $W$ generated by $e_0, \ldots, e_m$ is a $g$-module and it is irreducible.

Proof: Because each $e_i$ has different eigenvalue under action of $H$, thus if they are all nonzero, then they are linearly independent. If $e_0, e_1, \ldots, e_m$ are linearly independent, and $e_{m+1} = e_{m+2} = \ldots = 0$, then by the proposition,
\[
Xe_{m+1} = (\lambda - m)e_m
\]
and $e_{m+1} = 0$ with $e_m \neq 0$, thus $\lambda = m$. Now the formulas in (15.15.1.9) shows that $W$ is a $g$-module. And if $W' \subset W$ is a subspace invariant under $g$, then it contains some eigenvalues $e_k$ of $H$, and then the formulas in (15.15.1.9) shows it contains all $e_0, e_1, \ldots, e_m$, thus $W' = W$. Thus $W$ is irreducible.

\[\square\]

Prop. (15.15.1.11) [Irreducible Representations of $\mathfrak{sl}_2(\mathbb{C})$]. Let $W_m = \{e_0, \ldots, e_m\}$ be a $m+1$-dimensional vector space and $\mathfrak{sl}_2$ acts on $W_m$ by
\[
He_n = (m - 2n)e_n, \quad Ye_n = (n+1)e_{n+1}, \quad Xe_n = (m - n + 1)e_{n-1}.
\]

Then $W_n$ is a f.d. irreducible representation of $\mathfrak{sl}_2$, and any f.d representation of $\mathfrak{sl}_2$ of dimension $m + 1$ is isomorphic to one of $W_m$.

Proof: The first assertion follows from (15.15.1.10) and the fact $e_0$ is a primitive element. For the second assertion, notice any f.d. representation $W$ of $g$ contains a primitive element (15.15.1.8) thus by (15.15.1.10) generates an irreducible $\mathfrak{sl}_2$-submodule $W_n$, thus this submodule equals $W$, and $n + 1 = m + 1$, thus $n = m$.

\[\square\]

Remark (15.15.1.12). Notice this is special case of (15.15.2.15).

Cor. (15.15.1.13). $W_0$ is the just trivial action of $\mathfrak{sl}_2$, $W_1$ is isomorphic to the natural action of $\mathfrak{sl}_2$ on $\mathbb{C}^2$, and $W_2$ is isomorphic to the adjoint action of $\mathfrak{sl}_2$ on itself.
Proof: In fact, $W_1$ can be identified with the vector space $\mathbb{C}\{x, y\}$ where
\[
Hx = x, Hy = -y, Yx = y, Yy = 0, Xy = x, Xx = 0.
\]
Then the $m$-th symmetric tensor of $W_1$ is isomorphic to the vector space of polynomials in $x, y$ of degree $m$, and by (2.5.9.2),
\[
H(C_m^k y^k x^{m-k}) = (m-2k)(C_m^k y^k x^{m-k}),
\]
\[
Y(C_m^k y^k x^{m-k}) = (k+1)(C_m^{k+1} y^{k+1} x^{m-k-1}),
\]
\[
X(C_m^k y^k x^{m-k}) = (m-k+1)(C_m^{k-1} y^{k-1} x^{m-k+1}).
\]
So it is isomorphic to $W_{m+1}$.

Cor. (15.15.1.14) [Representations of $\mathfrak{sl}_2(\mathbb{K})$]. Let $\mathbb{K} = \mathbb{R}$ or $\mathbb{C}$,
- Any f.d. representation $V$ of $\mathfrak{sl}_2(\mathbb{K})$ is isomorphic to a direct sum of $W_m$s, and
- The endomorphism on $V$ induced by $H$ is diagonalizable and with integral eigenvalues. if $\pm n$ are eigenvalues of $H$, then so are $n-2, n-4, \ldots, 4-n, 2-n$.
- For any $n \geq 0$, the linear maps
  \[
  Y^n : V^n \to V^{-n}, X^n : V^{-n} \to V^n
  \]
  are isomorphisms. In particular, $V^{-n}$ and $V^n$ have the same dimensions.

Proof: by Weyl’s theorem (15.15.1.2), any representation of $\mathfrak{sl}_2(\mathbb{K})$ is isomorphic to a direct sum of irreducible representations, and the irreducible representations of $\mathfrak{sl}_2(\mathbb{C})$ clearly come from real representations of $\mathfrak{sl}_2(\mathbb{R})$, thus irreducible representations of $\mathfrak{sl}_2(\mathbb{R})$ must be of the same form (otherwise tensor with $\mathbb{C}$ and decompose, and use conjugation).

Because we can assume $V$ is one of $W_m$, so the other assertions are clear.

2 Verma Modules

Def. (15.15.2.1) [Weights]. Let $(\mathfrak{g}, \mathfrak{h})$ be a semisimple Lie algebra with root system $R$ and $V$ is a $\mathfrak{g}$-module. If $\lambda \in \mathfrak{h}^\ast$, a vector $v \in V$ is said to have weight $\lambda$ iff $hv = \lambda(h)v$ for any $h \in \mathfrak{h}$. The space of vectors in $V$ of weight $\lambda$ is denoted by $V[\lambda]$. An integral weight is a weight $\lambda$ of the form $\lambda = \sum n_i \alpha_i^\vee$, where $\alpha_i \in R$, equivalently its values on $h_i$ are all integers.

$V$ is said to have a weight decomposition if $V = \oplus_{\lambda \in \mathfrak{h}^\ast} V[\lambda]$.

Prop. (15.15.2.2). Any f.d. $\mathfrak{g}$-module $V$ has a weight decomposition, and the weights are all integral.

Proof: For any $i$, $V$ is a $\mathfrak{s}_i = \{e_i, h_i, f_i\}$-module (2.5.3.20), so by the representation theory of $\mathfrak{sl}_2$, $h_i$ acts semisimply on $V$, and the eigenvalues are integers. Thus $\mathfrak{h}$ acts semisimply on $V$, thus there is a weight decomposition, and the weights are all integral.

Def. (15.15.2.3) [Highest Weight Representations]. A vector $v \in V$ is called a highest weight vector if it is a weight vector and $n_+ v = 0$, or equivalently $e_i v = 0$ for any $e_i$. A highest weight representation with highest weight $\lambda$ is a representation that is generated by a highest weight vector of weight $\lambda$.

Prop. (15.15.2.4). Any f.d. $\mathfrak{g}$-module contains a highest weight vector, thus any irreducible f.d $\mathfrak{g}$-representation is a highest weight representation.

Proof: Let $P = \sum_i \alpha_i^\vee$, and choose a weight $\lambda$ that $(\lambda, P)$ is maximal, then $e_i v$ has weight $\lambda + \alpha_i$, thus $e_i v = 0$ for any $i$. 
\]
15.15. REPRESENTATIONS OF SEMISIMPLE LIE ALGEBRAS AND CATEGORY $\mathcal{O}$

Verma Modules

**Def. (15.15.2.5)**[Verma Modules]. Let $\lambda \in \mathfrak{h}^*$, $I_\lambda \subset U(\mathfrak{g})$ be the left ideal generated by the elements $h - \lambda(h)$ and $e_i$, then the Verma module $M_\lambda = U(\mathfrak{g})/I_\lambda$. has a weight decomposition, and it is a highest weight representation with highest vector $v_{\lambda} = 1$ with weight $\lambda$.

**Prop. (15.15.2.6)**[M$_\lambda$ is Noetherian]. $M_\lambda$ satisfies ascending chain condition on f.d. submodules.

**Proof:** This is because $U(\mathfrak{g})$ is left Noetherian(2.5.8.16) and $M_\lambda = U(\mathfrak{g})/I_\lambda$. □

**Prop. (15.15.2.7).** The map $\varphi : U(\mathfrak{u}_-) \rightarrow W_\lambda : \varphi(x) = xv_\lambda$ is an isomorphism of left $U(\mathfrak{u}_-)$-modules.

**Proof:** This follows from PBW theorem. □

**Cor. (15.15.2.8).** $M_\lambda$ has a weight decomposition with $P(M_\lambda) = \lambda - Q^+$, and weight spaces of $M_\lambda$ are all of f.d..

**Prop. (15.15.2.9).** If $V$ is a $\mathfrak{g}$-module and $v \in V$ is a highest weight vector, then there is a unique homomorphism $M_\lambda \rightarrow V$ of $\mathfrak{g}$-modules that maps $v_{\lambda}$ to $v$.

**Cor. (15.15.2.10).** Every highest weight representation has a decomposition into f.d. weight spaces. And they have a unique highest weight vector up to a scalar.

**Prop. (15.15.2.11)**[Quotient of Verma Modules]. $M_\lambda$ has a unique irreducible quotient $L_\lambda$. In particular, $L_\lambda$ is a quotient of every highest weight representation of $\mathfrak{g}$ with weight $\lambda$, by(15.15.2.9).

**Proof:** As $M_\lambda$ has a weight decomposition, any submodule $Y$ of $M_\lambda$ has a weight decomposition, and cannot have weight $\lambda$, otherwise it generates $M_\lambda$ by(15.15.2.10). Then the sum $J_\lambda$ of all proper submodules of $M_\lambda$ also cannot have weight $\lambda$, thus also proper. Then $L_\lambda = M_\lambda/J_\lambda$ is the unique irreducible quotient of $M_\lambda$. □

**Cor. (15.15.2.12)**[Classification of Irreducible Highest Weight Representations]. Any irreducible highest weight representation of $\mathfrak{g}$ is of the form $L_\lambda$ where $\lambda \in \mathfrak{h}^*$.

**Prop. (15.15.2.13)**[Composition Factors of Verma Modules]. The Verma module $M_\lambda$ has a finite composition series $M_\lambda = N_0 \supset N_1 \supset \ldots \supset N_r = 0$ that each $N_i/N_{i+1}$ is irreducible and isomorphic to $L_{\omega(\lambda + \rho) - \rho}$ for some $\omega \in W$.

**Proof:** We can find a(not necessarily finite) series of submodules of $M_\lambda$ that the subquotients are irreducible as $M_\lambda$ satisfies ascending chain condition on submodules(15.15.2.6). □

**Lemma (15.15.2.14).** Let $V$ be a $\mathfrak{g}$-module with weight decomposition into f.d. weight spaces. If $V$ is a sum of f.d. $\mathfrak{g}$-modules for each $i$, then for each $\lambda \in P$ and $w \in W$, dim $V[\lambda] = \dim V[w\lambda]$.

**Proof:** As $W$ is generated by $s_i$, it suffices to prove for $w = s_i$, dim $V[\lambda] = \dim V[w\lambda]$.

If $(\lambda, \alpha_i^\vee) = m \geq 0$ for some $i$, consider the operator $f_i^m : V[\lambda] \rightarrow V[s_i\lambda]$ is an isomorphism by hypothesis and the representation theory of $\mathfrak{sl}_2$. Similarly, if $(\lambda, \alpha_i^\vee) = -m \leq 0$, then $e_i^m : V[\lambda] \rightarrow V[s_i\lambda]$ is an isomorphism. □

**Prop. (15.15.2.15)**[Classification of F.D. Irreducible Representations]. F.d. irreducible representations of $\mathfrak{g}$ are classified by their highest dominant integral weights $\lambda \in P^+$ via the bijection $\lambda \mapsto L_\lambda$. Moreover, for any $\mu \in P$ and $w \in W$, dim $L_\lambda[\mu] = \dim L_\lambda[w\mu]$. 
\textbf{Prop. (15.15.2.16).} \(L_\lambda = L_{-w_0\lambda}\).

\textit{Proof:} It suffices to show the lowest weight of \(L_\lambda\) is \(w_0\lambda\): \(w_0\lambda\) is a weight by (15.15.2.15), and if \(\lambda < w_0\lambda\), then \(w_0\lambda > \lambda\).

\textbf{Lemma (15.15.2.17).} The representation \(L_n\) of \(\mathfrak{sl}_2\) is of real type if \(n\) is even and of quaternion type if \(n\) is odd.

\textit{Proof:} \(L_n = \text{Sym}^n L_1\), thus we can take the bilinear form \(\text{Sym}^n B\), where \(B\) is the alternating form on \(L_1 \cong \mathbb{C}^2\), which is symmetric if \(n\) is even and alternating if \(n\) is odd.

\textbf{Prop. (15.15.2.18) [Type of Irreducible Representations].} Let \(\lambda \in \mathbb{P}^+\) that \(\lambda = -w_0\lambda\), so \(L_\lambda\) is self-dual by (15.15.2.16), and it is of real type if \(n = (2\rho',\lambda)\) is even and of quaternion type if \((2\rho',\lambda)\) is odd.

\textit{Proof:} The number \(n\) is the eigenvalue of \(h\) on \(v_\lambda\), where \(\{h, e, f\}\) is the principal \(\mathfrak{sl}_2\)-subalgebra, and the other eigenvalues are all smaller. Then \(L_\lambda \cong L_n \oplus \bigoplus_{-i<n} L_{m_i}\), so the invariant form on \(L_\lambda\) restricts to a non-zero invariant form on \(L_n\), so the assertion follows from (15.15.2.17).

\textbf{Fundamental Representations}

\textbf{Prop. (15.15.2.19) [Fundamental Representations].} The following are equivalent for a dominant integral weight \(\omega\) of a split semisimple Lie algebra \(\mathfrak{g}\):

- \(\omega\) is minuscule (2.7.3.15).
- All weights of the representation \(L_\omega\) belong to the orbit \(W\omega\).
- The restriction of \(L_\omega\) to \(\mathfrak{s}_i\) is a direct sum of 1-dimensional and 2-dimensional subrepresentations.

Such a representation \(L_\omega\) is called a \textbf{fundamental representation} of \(\mathfrak{g}\).

\textit{Proof:} 1 \(\rightarrow\) 2: By (15.15.2.15), for any weight \(\mu\) of \(L_\omega\), there is a \(w \in W\) that \(w\mu\) is dominant and \(\omega - w\mu \in Q^+\). Thus \(w\mu = \omega\) by (2.7.3.17), and \(\mu \in W\omega\).

2 \(\rightarrow\) 1: If \(\omega\) is not minuscule, then there is some positive \(\alpha\) that \((\omega, \alpha') > 1\), so \(2(\omega, \alpha) < (\alpha, \alpha)\), and \(\omega - \alpha\) is a weight of \(L_\omega\) (the weight of \(f_\alpha v_\omega\), and it is not conjugate to \(\omega\), as \((\omega - \alpha, \omega - \alpha) = (\omega, \omega) - 2(\alpha, \omega) + (\alpha, \alpha) < (\omega, \omega)\).

2 \(\iff\) 3: If \(\omega\) is minuscule and \(v \in \Lambda_\omega\) be a highest weight vector for \(\mathfrak{s}_i\), then \(h_{\alpha_i} v = \omega(h_{\alpha_i}) = (\omega, \alpha_i') = 0\) or \(v(2.5.3.21)\). Thus we get 4 by the representation theory of \(\mathfrak{sl}_2\). The reverse argument is also true.

\textbf{Cor. (15.15.2.20).} The character for a fundamental representation \(L_\omega\) is

\[\chi_\omega = \sum_{w \in W} e^{w\omega}.\]
Prop. (15.15.2.21). Let \( \omega \) be a minuscule weight, then for any dominant integral weight \( \lambda \),

\[
L_\omega \otimes L_\lambda \cong \oplus_{w \in W, \lambda + w \omega \in P^+} L_{\lambda + w \omega}.
\]

Proof: By Weyl’s character formula and (15.15.2.20),

\[
\chi_{L_\omega \otimes L_\lambda} = \sum_{\mu \in W \omega} \sum_{w \in W} \varepsilon(w)e^{w(\lambda + \rho + \mu)} = \sum_{\gamma \in W \omega} \sum_{w \in W} \varepsilon(w)e^{w(\lambda + \rho + \gamma)}
\]

If \( \lambda + \gamma \notin P^+ \), then \((\lambda + \gamma, \alpha_i) < 0 \) for some \( i \). But \((\gamma, \alpha_i) \geq -1 \) as \( \omega \) is minuscule, so \((\lambda + \gamma, \alpha_i) = -1 \), and \((\lambda + \gamma + \rho, \alpha_i) = 0 \). Then for such \( \gamma \), in the summand the \( w \) term cancels with \( ws_i \) term. Thus the summand equals the character for \( \sum_{w \in W} e^{w \omega} \). Then we finish by (15.15.3.3).

Prop. (15.15.2.22) [Fundamental Representations for Simple Lie Algebras]. By (2.7.3.20),

- for \( B_n \), the fundamental representation corresponding to the minuscule weights \( \omega_n \) is called the Spin representation, denoted by \( S \).
- for \( C_n \), the fundamental representation corresponding to the minuscule weights \( \omega_1 \) is the standard representation of \( \mathfrak{sp}_{2n} \).
- for \( D_n \), the fundamental representation corresponding to the minuscule weights \( \omega_1, \omega_{n-1}, \omega_n \) are the standard representation and two Spin representations \( S^+, S^- \).
- for \( E_7 \), the unique fundamental representation has dimension 56?.
- for \( E_6 \), the two fundamental representations are dual, and have dimensions 27?.

Prop. (15.15.2.23) [Bott Periodicity for Spin Representations]. Let \( \mathfrak{g} = \mathfrak{so}_m \), then the behavior of the spin representation of \( \mathfrak{g} \) is

- \( S \) is of real type if \( m \equiv 1, 7 \mod 8 \).
- \( S \) is of quaternionic type if \( m \equiv 3, 5 \mod 8 \).
- \( S_+, S_- \) are of real type if \( m \equiv 0 \mod 8 \).
- \( S_+ \cong S_- \) are of complex type if \( m \equiv 2, 6 \mod 8 \).
- \( S_+, S_- \) are of quaternionic type if \( m \equiv 4 \mod 8 \).

Proof: We use (15.15.2.18). If \( \mathfrak{g} = \mathfrak{so}_{2n} \), then \( \rho^\vee = \rho = \sum \omega_i = (n - 1, n - 2, \ldots, 1, 0) \), so \((2\rho^\vee, \omega_{n-1}) = (2\rho^\vee, \omega_n) = \frac{n(n-1)}{2} \).

If \( \mathfrak{g} = \mathfrak{so}_{2n+1} \), then it can be verified that \( \rho^\vee = (n, n - 1, \ldots, 0) \), so \((2\rho^\vee, \omega_n) = \frac{n(n+1)}{2} \).

Also we need to consider \( w_0 \), so \( \mathfrak{so}_{4n+2} \) are of complex type.

3 Weyl Character Formula

Def. (15.15.3.1) [Central Characters of a Representation]. Let \( V = \oplus_{\mu \in P} V[\mu] \) be a f.d. representation of a split semisimple Lie algebra \( \mathfrak{g} \), the central character \( \chi \) is an analytic function on \( \mathfrak{h} \) that

\[
\chi_\nu(h) = \sum_{\mu \in P} \dim V[\mu]e^{\mu(h)}.
\]

In fact \( \chi \) is an element in \( \mathbb{Z}[e^{\alpha_1}, \ldots, e^{\alpha_r}, e^{-\alpha_1}, \ldots, e^{-\alpha_r}] \).
Prop. (15.15.3.2) [Weyl Character Formula]. Let $\lambda \in P^+$, then the character $\chi_\lambda = \chi_{L_\lambda}$ of the f.d. irreducible representation $L_\lambda$ of $\mathfrak{g}(15.15.2.15)$ is given by

$$\chi_\lambda = \frac{\sum_{w \in W} \varepsilon(w) e^{w(\lambda + \rho)}}{\Delta}.$$ 

where $\Delta$ is the Weyl denominator (15.15.4.3).

Proof: We already know that $\Delta \chi_\lambda \sum_{\mu \in P} c_\mu e^{\mu}$ is $W$-anti-invariant, $c_{\lambda + \rho} = 1$, and $c_\mu = 0$ unless $\mu \in \lambda + \rho - Q^+$, so it suffices to show $c_\mu = 0$ if $\mu \in P^+ \cap (\lambda + \rho - Q^+)$ and $\mu \neq \lambda + \rho$. □

Cor. (15.15.3.3) [Characters Determine Representations]. F.d. representations of a semisimple Lie algebra is determined by its characters, as the maximal exponent of $\chi_\lambda$ are different for different $\lambda$.

Cor. (15.15.3.4). For $\mathfrak{sl}_2(\mathbb{C})$, $\chi_{W_n}(z) = e^{nz} + e^{(n-2)}z + \ldots + e^{-nz} = \frac{e^{(n+1)z} - e^{-(n+1)}z}{e^z - e^{-z}}$. Notice these functions are linearly independent, so by (15.1.14), representations of $\mathfrak{sl}_2(\mathbb{C})$ are determined by their characters.

Cor. (15.15.3.5) [Weyl Denominator Formula].

$$\Delta = \sum_{w \in W} \varepsilon(w) e^{w\rho}.$$ 

Proof: This follows from the Weyl character formula by setting $\lambda = 0$. □

Prop. (15.15.3.6) [Kostant’s Multiplicity Theorem]. Let $\mathfrak{g}$ be a split semisimple Lie algebra and $\lambda \in P^+$, then

$$\dim L_\lambda[\gamma] = \sum_{w \in W} \varepsilon(w) \Psi(w(\lambda + \rho) - \rho - \gamma).$$ 

where $\Psi$ is the Kostant’s partition function (2.7.2.19).

Proof: This follows from the formula

$$\Delta^{-1} = e^{-\rho} \sum_{\alpha \in R^+} \frac{1}{(1 - e^{-\alpha})} = e^{-\rho} \sum_{\alpha \in Q(R)} \Psi(\alpha) e^{-\alpha}.$$ 

applied to Weyl’s character formula (15.15.3.2). □

Prop. (15.15.3.7) [Steinberg’s Multiplicity Formula]. Let $\lambda, \mu \in P^+$, then

$$L_\lambda \otimes L_\mu \cong \sum_{\nu \in P^+} c_{\lambda \mu \nu} L_\nu,$$ 

where

$$c_{\lambda \mu \nu} = \sum_{w, w' \in W} \varepsilon(w) \varepsilon(w') \Psi(w(\lambda + \rho) + w'(\mu + \rho) - (\nu + 2\rho)).$$ 

where $\Psi$ is the Kostant’s partition function (2.7.2.19).

Proof: Cf. [Cartar, P265]. □
Cor. (15.15.3.8) [Clebsch-Gordan Rule]. The tensor products of representations of $\mathfrak{sl}_2(\mathbb{C})$ satisfy

$$W_m \otimes W_n \cong \bigoplus_{i=0}^{\min(m,n)} W_{|m-n|+2i}.$$

Proof: This follows from (15.15.3.7) or from (15.15.3.4).

Prop. (15.15.3.9) [Weyl Dimension Formula]. Let $\mathfrak{g}$ be a split semisimple Lie algebra and $\lambda \in P^+$, then

$$\dim L_\lambda = \frac{\prod_{\alpha \in R^+ (\alpha, \lambda + \rho)} (\alpha, \lambda + \rho)}{\prod_{\alpha \in R^+ (\alpha, \rho)} (\alpha, \lambda + \rho)}.$$

Proof: Choose an element $h_\rho \in \mathfrak{h}$ that corresponds to $\rho \in \mathfrak{h}^*$ via the Killing form, then

$$\chi_\lambda(2th_\rho) = \frac{\sum_{w \in W} \varepsilon(w) e^{2t(w(\lambda+\rho),\rho)}}{\prod_{\alpha \in R^+ (\alpha, \lambda + \rho)} (\alpha, \lambda + \rho)}.$$

The crucial fact is that we can use Weyl’s denominator formula (15.15.3.5) on the nominator, to get

$$\chi_\lambda(2th_\rho) = \frac{\prod_{\alpha \in R^+ (\alpha, \lambda + \rho)} (\alpha, \lambda + \rho)}{\prod_{\alpha \in R^+ (\alpha, \lambda + \rho)} (\alpha, \lambda + \rho)}.$$

Now taking limit $t \to 0$, we get the desired formula.

Remark (15.15.3.10). The Weyl dimension formula can be used to determine a representation $V$ is irreducible or not: First calculate the maximal weight, then use the Weyl dimension formula to calculate the dimension to see if it is equal to the dimension of $V$.

4 Category $\mathcal{O}$

Def. (15.15.4.1) [$\mathcal{O}_{int}$]. Let $(\mathfrak{g}, \mathfrak{h})$ be a split semisimple Lie algebras, the category $\mathcal{O}_{int}$ is the category of representations $V$ of $\mathfrak{g}$ that with weight decomposition into f.d. weight spaces that the weights $P(V)$ is contained in the union of sets $\lambda^i - Q^+$ for f.m. weights $\lambda^1, \ldots, \lambda^N \in P^\vee(R)$.

Def. (15.15.4.2) [Characters]. The character for a f.d. representation can be extended to category $\mathcal{O}_{int}$ as a formal Laurent series

$$\chi \in \mathbb{Z}[[e^{-\alpha_i^\vee}, \ldots, e^{-\alpha_r^\vee}][e^{\alpha_i^\vee}, \ldots, e^{\alpha_r^\vee}]: \chi_V(h) = \sum \dim V[\mu] e^{\mu(h)}.$$

Prop. (15.15.4.3). The character of $M_\lambda$ is given by

$$\chi_{M_\lambda} = \frac{e^\lambda}{\prod_{\alpha \in R^+ (1 - e^{-\alpha})} = \frac{e^{\lambda + \rho}}{\Delta}, \quad \Delta = \prod_{\alpha \in R^+} (e^{\alpha/2} - e^{-\alpha/2}),$$

where $\Delta$ is called the Weyl denominator of $\mathfrak{g}$. 
15.16 Trace Formulae

Main references are [Introductory notes on the trace formula, Lapid], [Trace formula, Whitehouse] and [Trace Formula, Arthur].

1 Introduction

Remark (15.16.1.1). Delete this subsection.

The trace formula was introduced by Selberg in his seminal work. Selberg mostly developed the trace formula for quotients of the hyperbolic plane by a Fuchsian group \( \Gamma \) of the first kind (both in the co-compact and the non co-compact case). One of his original motivations and applications was to show the existence of Maass forms with respect to \( \Gamma = SL(2, \mathbb{Z}) \). It was subsequently vastly generalized by Arthur in the context of adelic quotients \( G(F) \backslash G(A) \) of a reductive group \( G \) over a number field \( F \). Arthur’s main driving force was the functoriality conjectures of Langlands.

Selberg’s trace formula is a far-reaching non-commutative generalization of the Poisson summation formula. It underlines a duality between geometric and spectral objects.

2 Trace Formulae

Trace Formula for Compact Quotient

Prop. (15.16.2.1). Consider the right action of \( G \) on \( L^2(\Gamma \backslash G, \chi) \)(15.7.1.22), let \( \varphi \in C_c^\infty(G) \), then \( \varphi \) can act on \( L^2(\Gamma \backslash G, \chi) \) by (10.7.3.24), and:

- \( \rho(\varphi) \) is an integration operator, in particular Hilbert-Schmidt and compact. And \( \text{Im}(\rho(\varphi)) \subset C^\infty(\Gamma \backslash G, \chi) \).
- If \( \varphi(g^{-1}) = \overline{\varphi(g)} \), then \( \rho(\varphi) \) is self-adjoint.
- If \( \varphi(kg) = e^{-ik\theta}\varphi(g) \), then \( \text{Im}(\rho(\varphi)) \subset C^\infty(\Gamma \backslash G, \chi, k) \).

Compare with (15.16.2.4).

Proof: These follows from (15.16.2.4). \( \square \)

Cor. (15.16.2.2). Let \( H \) be a nonzero closed \( G \)-subrepresentation of \( L^2(\Gamma \backslash G, \chi) \), then \( H \) decomposes as \( \oplus_k H^k \) w.r.t. action of \( SO(2, \mathbb{R}) \). And if \( H^k \neq 0 \), then \( \Delta \) has a nonzero eigenvector in \( H^k \cap C^\infty(\Gamma \backslash G, \chi) \).

Proof: The decomposition is clear from (10.9.4.3). It’s left to show \( \Delta \) has an eigenvalue in \( H^k \cap C^\infty(\Gamma \backslash G, \chi) \). By lemma (15.6.4.1) above, for \( f_0 \in H^k \), there is a \( \varphi \in C_c^\infty(G) \) s.t. \( \rho(\varphi)f_0 \neq 0 \), and \( \varphi(kg) = e^{-ik\theta}\varphi(g) \). So (15.16.2.1) shows \( \rho(\varphi) \) maps \( H \) into \( H^k \cap C^\infty(\Gamma \backslash G, \chi) \) and induces a compact self-adjoint operator on \( H^k \). So we can choose a f.d. eigenspace of it. Notice \( \Delta \) commutes with the action \( \rho(\varphi) \), so \( \Delta \) fixes this eigenspace, thus it has an eigenvalue on \( H^k \cap C^\infty(\Gamma \backslash G, \chi) \). \( \square \)

Prop. (15.16.2.3) [L^2(\Gamma \backslash G) Totally Decomposable]. Let \( G \) be a unimodular locally compact topological group and \( \Gamma \subset G \) be a discrete subgroup that \( \Gamma \backslash G \) is compact, \( \chi \in \hat{\Gamma} \), then the space \( L^2(\Gamma \backslash G, \chi) \) decomposes as

\[
L^2(\Gamma \backslash G, \chi) = \bigoplus_{\pi \in \hat{G}} m_\pi V_\pi
\]

that each \( m_\pi \) is finite.
Proof: Let $\Sigma$ be the set of sums of irreducible invariant subspaces of $L^2(\Gamma \backslash G, \chi)$ that is mutually orthogonal. Then choose by Zorn’s lemma a maximal one in $\Sigma$, and we prove the orthogonal complement $H = 0$ otherwise we construct an irreducible subspace of $H$.

Let $f \neq 0 \in H$, choose by (15.6.4.1) and (15.16.2.1) a $\varphi \in C_c(G)$ that $\rho(\varphi)$ is compact self-adjoint and $\rho(\varphi)f \neq 0$. So $\rho(\varphi)$ has a non-zero eigenvalue and the eigenspace $L$ is of f.d.

Let $L_0$ be a minimal nonzero subspace of $L$ that is an intersection of $L$ with a nonzero closed invariant subspace of $H$, and let $V$ be the intersection of all closed invariant subspaces $W$ of $H$ that $L_0 = L \cap W$. We show $V$ is irreducible, if not, then $V = V_1 \cap V_2$, and if $0 \neq f_0 \in L_0$, then $f_0 = f_1 + f_2$ and both $f_1, f_2$ are eigenfunctions of $\rho(\varphi)$ of eigenvalue $\lambda$. Now if $f_1 \neq 0$, then by minimality, $V_1 \cap L = L_0$.

The finiteness of $m_\pi$ follows from the fact that $\rho(f)$ is Hilbert-Schmidt for every $f \in C_c(G)$.

\[\Box\]

**Prop. (15.16.2.4).** If $\Gamma \subset G$ is a discrete subgroup that $\Gamma \backslash G$ is compact, consider the right action of $G$ on $L^2(\Gamma \backslash G)(10.9.2.9)$, let $\varphi \in C_c(G)$, then $\varphi$ can act on $L^2(\Gamma \backslash G, \chi)$ by (10.7.3.24), and:

- $\rho(\varphi)$ is an integration operator, in particular Hilbert-Schmidt and compact.
- If $\varphi(g^{-1}) = \overline{\varphi(g)}$, then $\rho(\varphi)$ is self-adjoint.

**Proof:**

1. 
\[
\rho(\varphi)f(g) = \int_G f(h)\varphi(g^{-1}h)dh = \int_{\Gamma \backslash G_1} \sum_{\gamma \in \Gamma} f(\gamma h)\varphi(g^{-1}\gamma h)dh = \int_{\Gamma \backslash G_1} f(h)K_{\varphi}(g,h)dh
\]

where
\[
K_{\varphi}(g,h) = \sum_{\gamma \in \Gamma} \varphi(g^{-1}\gamma h).
\]

Because $\varphi$ is compactly supported, this is a smooth function in $g$ and $h$, in particular square integrable on $\Gamma \backslash G$ compact. And $\rho(\varphi)(f)(g)$ is smooth in $g$ because $f \in L_1(\Gamma \backslash G_1, \chi)$ as $\Gamma \backslash G_1$ is compact, and $K(g,h)$ is smooth in $g$.

2 is easy.

\[\Box\]

**Prop. (15.16.2.5) [Trace of $\rho(f)$].** If $\varphi = \varphi_1 \ast \varphi_2$ where $\varphi_i \in C_c(\Gamma \backslash G)$, then $\rho(\varphi) = \rho(\varphi_1)\rho(\varphi_2)(10.7.3.24)$ and hence a trace class (10.8.5.7). And its integral kernel is
\[
K_{\varphi}(x,y) = \int_{\Gamma \backslash G} K_{\varphi_1}(x,z)K_{\varphi_2}(z,y)dz.
\]

and
\[
\text{tr} \rho(f) = \int_{\Gamma \backslash G} K_{\varphi}(x,x)dx = \int_{\Gamma \backslash G} \int_{\Gamma \backslash G} K_{\varphi_1}(x,y)K_{\varphi_2}(y,x)dxdy.
\]

**Proof:** This follows from (10.8.5.10).

\[\Box\]

**Cor. (15.16.2.6) [the Geometric Side of Trace Formula].** If $G$ is unimodular, let $f = f_1 \ast f_2$, $c(\gamma)$ be a representative for the conjugacy classes of $\Gamma$, then
\[
\text{tr}(\rho(f)) = \sum_{\gamma \in c(\Gamma)} \int_{\Gamma \backslash G} f(x^{-1}\gamma x)dx.
\]

And if $G_{\gamma}$ is unimodular for every $\gamma \in \Gamma$, then
\[
\text{tr}(\rho(f)) = \sum_{\gamma \in c(\Gamma)} V(\Gamma \backslash G_{\gamma}) \int_{G_{\gamma} \backslash G} f(x^{-1}\gamma x)dx.
\]
Proof:

\[ K_f(x,x) = \sum_{\gamma \in \Gamma} f(x^{-1}\gamma x) = \sum_{\gamma \in \Gamma} \sum_{\delta \in \Gamma \setminus \Gamma} f(x^{-1}\delta^{-1}\gamma \delta x), \]

so we have

\[ \int_{\Gamma \setminus G} K_f(x,x) dx = \int_{\Gamma \setminus G} \sum_{\gamma \in \Gamma} \sum_{\delta \in \Gamma \setminus \Gamma} f(x^{-1}\delta^{-1}\gamma \delta x) = \sum_{\gamma \in \Gamma} \int_{\Gamma \setminus G} f(x^{-1}\gamma x) dx. \]

\[ \square \]

Cor. (15.16.2.7) [Trace Formula for \( \Gamma \setminus G \) Compact]. Let \( G \) be a unimodular locally compact topological group and \( f = f_1 * f_2 \) where \( f_i \in C_c(G) \), and \( \Gamma \) be a discrete subgroup of \( G \) with \( \Gamma \setminus G \) compact and \( G_\gamma \) is unimodular for every \( \gamma \in \Gamma \), then \( \rho(f) \) is a trace class with

\[ \sum_{\pi \in \hat{\Gamma}} m_\pi \text{tr}(\pi(f)) = \text{tr}(\rho(f)) = \sum_{\gamma \in \Gamma} V(\gamma \setminus G_\gamma) \int_{\Gamma \setminus G} f(x^{-1}\gamma x) dx. \]

Proof: Follows from (15.7.5.2) and (15.16.2.6). \[ \square \]

Lemma (15.16.2.8). Let \( G = GL(2, \mathbb{R}) \), \( K = SL(2, \mathbb{R}) \), \( \Gamma \setminus G \) be compact, \( \rho \) be the principal series \( P(\lambda, 0)(15.6.4.15) \) of \( G \), and \( s = \frac{1}{2}(s_1 - s_2 + 1), \lambda = s(1 - s), \mu = (s_1 + s_2) \), then for any \( f \in C_c(\mathbb{K} \setminus K/K) \), \( \rho(f) \in V^K_\rho \), which has dimension1, so \( f \) is a trace class and

\[ \text{tr}(\rho(f)) = \int \int f \begin{bmatrix} e^{u/2} & x \\ 0 & e^{-u/2} \end{bmatrix} e^{\frac{x}{2}} du dx. \]

Proof: The trace of \( \rho(f) \) is just the scalar by which \( \rho(f) \) acts on a non-zero vector of \( \rho^K \). Take \( \varphi \in \rho^K \subset H(s_1, s_2, 0) \) normalized that \( \varphi(I) = 1 \), then

\[ (\rho(f)\varphi)(I) = \int_G f(g)\varphi(g) dg = \int_K \int_A \int_N f(ank)\varphi(ank) dAdNd\theta = \int_A \int_N f(an)\varphi(an) dAdN \]

\[ \square \]
16 | L-Functions

16.1 L-Functions Attached to Motives

Main references are [Conjectures in Arithmetic Algebraic Geometry, Hulsbergen, 1992].

Remark (16.1.0.1). In short, nineteenth century number theory showed that much, if not all, of number theory is reflected by properties of L-functions.

1 over Finite Fields

Def. (16.1.1.1) [Zeta-Functions]. Let $X$ be an algebraic scheme over a finite field $F_q$, then its Zeta function is defined to be the power series

$$Z(X; T) = \exp(\sum_{n \geq 1} \#X(F_{q^n}) T^n/n) \in \mathbb{Q}[[T]].$$

Notice that we can get the information of number of rational points of $X$ by the formula

$$\#X(F_{q^n}) = \frac{1}{(n-1)!} \frac{d^n}{dT^n} \log Z(X; T)|_{T=0}.$$

Prop. (16.1.1.2) [Euler Product]. There is an Euler product formula for $Z(X; T)$ by (13.12.2.2)(13.12.2.3).

$$Z(X; T) = \prod_{x \text{ closed in } X} \frac{1}{1 - T^{\deg(x)}}.$$

Thm. (16.1.1.3) [Weil Conjecture]. Let $X$ be a smooth proper variety over $F_q$ of dimension $n$, then

1. (Rationality): $Z(X; T)$ is a rational function in $\mathbb{Q}[T]$.

2. (Riemann Hypothesis): $Z(X; T)$ is of the form

$$Z(X; T) = \frac{P_1(X; T)P_3(X; T)\ldots P_{2n-1}(X; T)}{P_0(X; T)P_2(X; T)\ldots P_{2n}(X; T)}$$

s.t.

- $P_0(X; T) = 1 - T$,
- $P_{2n}(X; T) = 1 - q^n T$,
- For $0 \leq i \leq 2n$, $P_i(X; T) = \prod_{j \leq k} (1 - \alpha_{ij} T) \in \mathbb{Z}[T]$ and each $\alpha_{ij}$ is an algebraic integer s.t. $|\iota(\alpha_{ij})| = q^{i/2}$, where $\iota$ is any embedding $\mathbb{Z}[\alpha_{ij}] \to \mathbb{Z}$. In particular, $\alpha_{ij}$ appear in conjugate pairs.
• The degree of $P_i(X; T)$ is called the $i$-th **Betti number** of $X$, and $\deg P_i(X; T) = \deg P_{2n-i}(X; T)$.

3. **(Functional Equation):**
   
   $$Z(X; \frac{1}{q^nT}) = \pm q^{n/2}T^\chi Z(X; T),$$
   
   where $\chi$ is a Euler character $\Delta \cdot \Delta = \sum_{i=0}^{2n}(-1)^i \dim P_i(X; T)$.

4. If $X$ lifts to some proper smooth scheme $\mathcal{X}$ over $\mathcal{O}_K$ where $K$ is a global number field and $p$ is a prime of $K$ with residue field $\mathbb{F}_q$, then $\deg(P_i(X; T))$ equals the $i$-th Betti number of $\mathcal{X}_C$.

**Proof:**  
1: This follows from trace formula (13.12.2.6) and (7.5.1.14).

2: This follows from trace formula (13.12.2.6) and Deligne’s purity theorem (13.12.6.5): Let $Z(X; T) = P(T)/Q(T) \in \mathbb{Q}[T]$ by item 1, and

$$Z(X; T) = \frac{P_1(X; T)P_3(X; T)\ldots P_{2n-1}(X; T)}{P_0(X; T)P_2(X; T)\ldots P_{2n}(X; T)},$$

where the roots of $P_k(X; T)$ satisfies $|\iota(\alpha_{ij}^{-1})| = q^{-i/2}$, thus

$$P(T) = P_1(X; T)P_3(X; T)\ldots P_{2n-1}(X; T), \quad Q(T) = P_0(X; T)P_2(X; T)\ldots P_{2n}(X; T).$$

Also $P_i(X; T) \in \mathbb{Q}[T]$ because the its roots are stable under $\text{Gal}_Q$, because they are distinguished by their $\iota$-values.

$\alpha_{ij}$ are algebraic integers by Deligne’s integrality theorem (13.12.9.3). Notice by Poincaré duality (6.4.8.10), $H^{2n}(X, \mathbb{Q}_l(n)) \cong H^0_{et}(X, \mathbb{Q}_l)^\vee$, thus $F_X^*$ acts on $H^0_{et}(X, \mathbb{Q}_l)$ by $\text{id}$ and acts on $H^{2n}(X, \mathbb{Q}_l)$ by $q^n$. Thus $P_0(X; T) = 1 - T$, $P_{2n}(X; T) = 1 - q^n T$.

3: Apply (2.3.12.1) to $H^1 = H^1_{et}(X, \mathbb{Q}_l)$, trace map and perfect pairing given by Poincaré duality (6.4.8.10) and $\varphi_i = q^{-i/2}F_X^*$. Notice $\varphi_{2n} = \text{id}$ by item 2. Now (2.3.12.1) says $\varphi_i^{-1} = \varphi_{2d-i}^t$, thus $\varphi_i^{-1} = \varphi_{2d-i}$, then the theorem follows from a direct calculation. 

*Cor. (16.1.1.4)[Invariance of Characteristic Polynomial with $\ell$]. It follows from the proof above that $P_i$ is determined by $X$, and it is also the characteristic polynomial of $F_{\mathbb{F}_q}$ on $H^i_{et}(X, \mathbb{Q}_l)$ for any $\ell \in \mathbb{P} \setminus \text{char } k$, so the latter is independent of $\ell$ chosen.

**Points Counting**

**Prop. (16.1.1.5).** If $X$ is a proper smooth curve over $\mathbb{F}_q$, then by Weil conjecture (16.1.1.3),

$$|\#X(\mathbb{F}_q^n) - q^n - 1| = \left| \sum_j \alpha_{1j} \right| \leq 2g_Xq^{n/2}.$$

**Prop. (16.1.1.6)[Drinfeld-Vladut].** For $p \in \mathbb{P}$, $q = p^r$, let $A(q) = \lim_{g_X \to \infty} \frac{\#X(\mathbb{F}_q)}{g_X}$, where the limit is taken over all smooth proper curves over $\mathbb{F}_q$. Then $A(q) \leq \sqrt{q} - 1$.

**Proof:** Let $\alpha_{ij}$ as in (16.1.1.3), $\omega_i = \alpha_{1i}q^{-1/2}$, then $|\omega_i| = 1$ and inversion induces an automorphism of $\{\omega_i\}$. Then by (16.1.1.5), for any $r \in \mathbb{Z}_+$,

$$N = \#X(\mathbb{F}_q) \leq \#X(\mathbb{F}_q^r) = q^r + 1 - q^{r/2}\sum_i \omega_i^r.$$
And notice
\[ 0 \leq |1 + \omega_i + \ldots + \omega_i^r|^2 = (r+1) + \sum_{j=1}^r (r+1-j)(\omega_i^j + \omega_i^{-j}), \]

So
\[ 2g_X(r+1) \geq -\sum_{i,j=1}^r (r+1-j)(\omega_i^j + \omega_i^{-j}) = -2\sum_{j=1}^r (r+1-j)(\sum_i \omega_i^j) \]
\[ \geq N\sum_{j=1}^r (r+1-j)q^{-j/2} - \sum_{j=1}^r (r+1-j)(\alpha^j + \alpha^{-j}) \]

Thus
\[ \frac{N}{g_X} \leq (\sum_{j=1}^r \frac{r+1-j}{r+1} q^{-j/2})^{-1} \cdot (1 + \frac{1}{g} \sum_{j=1}^r \frac{r+1-j}{r+1} (\alpha^j + \alpha^{-j})) \]

Taking limit \( g \to \infty \),
\[ \frac{N}{g_X} \leq (\sum_{j=1}^r \frac{r+1-j}{r+1} q^{-j/2})^{-1}. \]

And taking limit \( r \to \infty \) gives
\[ \frac{N}{g_X} \leq (\sum_{j=1}^r q^{-j/2})^{-1} = \sqrt{q} - 1 \]

\[ \square \]

2 over Global Fields

**Prop. (16.1.2.1) [Hasse-Weil L-Functions].** Let \( X \) be a smooth proper variety over a global field \( F \), the \( \zeta \)-function of \( X \) is defined to be
\[ Z(X, s) = \prod_{v \in \Sigma_F} Z(X_v, q^{-s}), \]
where for \( v \) s.t. \( X_v \) has good reduction, \( Z(X_v, T) = Z(X_{k_v}, T) \) in (16.1.1.1), and for bad places \( v \), it needs to be defined otherwise.

**Prop. (16.1.2.2).** Let \( l_1, \ldots, l_N \) be linear forms in \( r \)-variables with rational coefficients, then
\[ \sum_{x \in \mathbb{Z}^r} \frac{1}{l_1(x) \ldots l_N(x)} \in \mathbb{Q}^N \]
if it is convergent.

**Proof:**
3 Motivic L-Functions

Main references are [Del79] and [Zag94].

**Def. (16.1.3.1) [Motivic L-Functions]**. Use the fact the Grothendieck motives over a finite field is a Tannakian category, we can define L-functions for any motives over a number field. Such an L-function is called a **motivic L-function**.

**Conj. (16.1.3.2) [Properties]**. The motivic L-functions are conjectured to satisfy the following properties:

**Algebraicity**: There are Dirichlet series expansions: 
\[ L(s) = \sum_{n \geq 1} a_n n^{-s} \] for \( \text{Re}(s) \) large, where \( \{a_n\} \in \mathbb{F} \) for some number field \( \mathbb{F} \).

**Euler Product**: There are Euler product expansions: 
\[ L(s) = \prod_{p \in \mathbb{P}} \Phi_p(p^{-s}) \] where \( \max_{p \in \mathbb{P}} \{\deg \Phi_p\} < \infty \). In particular, \( n \mapsto a_n \) is multiplicative.

**Functional Equation**: There is a \( \gamma \)-factor 
\[ \gamma(s) = A^s \cdot \prod_i \Gamma(\frac{1}{2}(s + m_i)) \] where \( A \in \mathbb{C}^*, m_i \in \mathbb{Z} \), s.t. \( \zeta(s) = \gamma(s)L(s) \) satisfies a functional equation 
\[ \zeta(s) = w\zeta(h - s) \] where \( w = \pm 1 \) called the **sign of functional equation** and \( h \in \mathbb{Z}_+ \). And in this way, \( L(s) \) extends to a meromorphic function on \( \mathbb{C} \) with only f.m. poles.

**Local Riemann Hypothesis**: The zeros of \( \Phi_p(p^{-s}) \) lie on the line \( \text{Re}(s) = \frac{k-1}{2} \).

**Riemann Hypothesis**: The zeros of \( L(s) \) are either integers or lie on the line \( \text{Re}(s) = \frac{k-1}{2} \).

**Special Values**: A **critical point** for \( L(s) \) is an integer \( m \in \mathbb{Z} \), s.t. neither \( m \) nor \( h - m \) is a pole of \( L(s) \). Then for a critical point \( m \) for \( L(s) \), the **critical value** \( L(m) = A(m)\Omega(m) \), where \( A(m) \) is a reasonable algebraic number and \( \Omega(m) \in \mathbb{P} \) is a reasonable period number.

**Central Special Values**: If \( h = 2m, m \in \mathbb{Z} \), then \( m \) is called a **central value** of \( L(s) \), and in this case, \( A(m) \) is a square times a simple factor.

**More...**

**Proof:**

**Conj. (16.1.3.3) [Big Modularity Conjecture]**. Every motivic L-function comes from a automorphism representation.

**Proof:**


4 Abelian Varieties

**Def. (16.1.4.1) [Motivic L-Function of Elliptic Curves]**. Let \( F \) be a global field \( F \) and \( A \in \text{AbVar}/F \), the motivic \( h^1 \) L-function is defined to be

\[ L(h^1 A, s) = \prod_{v \in \Sigma^1} L(h^1 A_v, s) \]

where \( L(E_v, s) \) is defined to be
• \( L(E_v, s) = (1 - a_v q_v^{-s} + q_v^{1-2s})^{-1} \) as in (16.1.5.1), where \( a_v = q_v + 1 - \#E_v(k_v) \), if \( E \) has good reduction at \( v \).

• \( (1 - q_v^{-s})^{-1} \) if \( E \) has split multiplicative reduction at \( v \).

• \( (1 + q_v^{-s})^{-1} \) if \( E \) has non-split multiplicative reduction at \( v \).

• 1 if \( E \) has additive reduction at \( v \).

Notice that in all cases we have \( L(E_v, 1) = q_v/\#E_{ns}(k_v) \).

5 Elliptic Curves

L-Factors

Def. (16.1.5.1) [L-Factors].

Def. (16.1.5.2) [Motivic L-Function of Elliptic Curves]. Let \( F \) be a global field \( F \) and \( E \in \mathcal{E}ll / F \), the motivic \( h^1 \) L-function is defined to be

\[
L(h^1 E, s) = \prod_{v \in \Sigma^0_F} L(h^1 E_v, s)
\]

where \( L(E_v, s) \) is defined to be

• \( L(E_v, s) = (1 - a_v q_v^{-s} + q_v^{1-2s})^{-1} \) as in (16.1.5.1), where \( a_v = q_v + 1 - \#E_v(k_v) \), if \( E \) has good reduction at \( v \).

• \( (1 - q_v^{-s})^{-1} \) if \( E \) has split multiplicative reduction at \( v \).

• \( (1 + q_v^{-s})^{-1} \) if \( E \) has non-split multiplicative reduction at \( v \).

• 1 if \( E \) has additive reduction at \( v \).

Notice that in all cases we have \( L(E_v, 1) = q_v/\#E_{ns}(k_v) \).

6 Tamagawa Number Conjecture

References are [A note on Height Pairings, Tamagawa Numbers and the Birch and Swinnerton-Dyer Conjecture, Bloch].

Conj. (16.1.6.1) [Tamagawa Number Conjecture]. Let \( F \) be a number field and \( G \in \text{AlgGrp} / F \), suppose that \( G(F) \) is discrete in \( G(A_F) \), then

\[
\tau(G) = \frac{\#\text{Pic}(G)_{\text{tor}}}{\#\Xi(G)}.
\]

Moreover, \( \text{ord}_{s=1} L(s) \leq 0 \), and \( r = 0 \) iff \( \text{Vol}(G(A_F)/G(F)) < \infty \).

Proof: \( \square \)

Thm. (16.1.6.2) [Bloch]. The Tamagawa number conjecture (16.1.6.1) implies that BSDT conjecture.
Equivariant Tamagawa Number Conjecture

7 Others

Invariants of Moduli Spaces

Prop. (16.1.7.1). Volumes and Euler characteristics of moduli spaces are often expressible by special values of ζ-functions.

Proof: □

Def. (16.1.7.2)[Witten ζ-Functions]. Because of the appearance in physics(Verlinde formula), people are interested in certain moduli spaces of vector bundles on curves.

Witten gave a formula expressing the volume of these moduli spaces in terms of special values of Witten ζ-functions:

Let $g$ be a semisimple f.d. Lie algebra, define

$$\zeta_g(s) = \sum_{\rho \in \text{Rep}(g)} \dim(\rho)^s.$$ 

Prop. (16.1.7.3). A consequence of Witten’s formula (16.1.7.2) is:

$$\zeta_g(2m) \in \mathbb{Q}\pi^{2rm}, m \in \mathbb{Z}_+$$

where $r$ is the number of positive roots of $g$.

Multiple ζ-Values

Cf.[Zag94].
16.2 L-Functions Attached to Automorphic Representations

Main references are [Bum98], [Cog00].

Notations (16.2.0.1).
- Use notations defined in Adelic Automorphic Representations of GL(n).
- Fix a global field $F$.
- Fix an additive character $\psi = \otimes \psi_v : A_F/F \to \mathbb{C}^\times$.
- Fix a linear algebraic group $G \in \text{Algebraic Groups} / F$ with center $Z$.
- Fix a central character $\omega : Z(A_F)/Z(F) \to \mathbb{C}^\times$. Notice if $G = \text{GL}(2)$, $\omega$ is just a Hecke character.

1 Introduction

Remark (16.2.1.1). Delete this subsection?.

Remark (16.2.1.2). According to https://mathoverflow.net/questions/44657/principal-l-functions-on-gln, there are several ways to attach L-functions to a cusp form on $\text{GL}(n)$ with functional equations:

1. Godement-Jacquet: In the spirit of Tate’s thesis, take a cusp form $f$ on $G = \text{GL}(n)$ (and $f'$ in the dual representation) and a Schwartz-Bruhat function $\Phi$ on $\text{Mat}(n, A_F)$ and integrate
\[ \int_{Z(A_F)G(F)\backslash G(A_F)} \langle \pi(g)f, f' \rangle \Phi(g) | \text{det}(g) |^s dg. \]

2. Rankin-Selberg: Take a cusp form $f$ on $G = \text{PGL}(n)$ (and $f'$ in the dual representation) and a specific Eisenstein series on $\text{PGL}(n^2)$ and integrate
\[ \int_{Z(A_F)(G \times G)(F)\backslash (G \times G)(A_F)} E(g_1, g_2)f(g_1)f'(g_2)dg_1dg_2, \]
where $Z$ is the center of $\text{PGL}(n^2)$. For this, Cf. [Bum98].

3. Eulerian integral: Take a cusp form $f$ on $\text{GL}(n)$ and $f'$ on $\text{GL}(m)$ with $n > m$, integrate
\[ \int_{\text{GL}(m,F)\backslash \text{GL}(m,A_F)} Pf(g)f'(g) | \text{det}(g) |^{s-1/2} dg. \]
where $P$ is the projection operator brilliantly designed s.t. this integral resolves to the product of Whittaker models for $f$ and $f'$. For this, Cf. [Cog00].

4. Langlands-Shahidi method:

2 Tate’s thesis (Godement-Jacquet for GL(1))

Main references are [Poo15], [R-V99] and [Tat65].
Lemma (16.2.2.1)[Dedekind Zeta Function]. For a global field $F$, the Dedekind zeta function is defined by

$$\zeta(F, s) = \prod_{p \in \Sigma_F} \frac{1}{1 - ||p||^{-s}}.$$ 

It converges absolutely for $\text{Re}(s) > 1$. Notice if $F$ is a number field, then

$$\zeta(F, s) = \sum_{a \in \text{Ideal}(O_F)} \frac{1}{||a||^s}.$$ 

Proof: It suffices to show $\prod_{p \in \Sigma_F} \frac{1}{1 - ||p||^{-s}} < +\infty$ for $\sigma > 1$.

If $F$ is a number field, let $d = [F : \mathbb{Q}]$, this is bounded by

$$\prod_{p} (1 - p^{-\sigma})^{-d} = (\sum_{n \geq 1} n^{-\sigma})^d < \infty.$$ 

If $F$ is a function field, let the number of irreducible polynomial modulo $p$ be $N_n$, then use the same method, it suffices to prove the convergence of

$$\prod_{p} \frac{1}{1 - (Np)^{-\sigma}} = \prod_{n \geq 1} (1 - q^{-n\sigma})^{-N_n}.$$ 

This is convergent iff $\sum_{n \geq 1} N_n q^{-n\sigma}$ is convergent(10.5.3.4), but the latter is bounded by

$$\sum_{n \geq 1} q^n q^{-n\sigma} = \sum_{n \geq 1} q^{-n(\sigma-1)} < \infty.$$ 

Def. (16.2.2.2)[Zeta Functions]. If $\Phi \in S(F)$ and $\chi$ is a Hecke character of $F$, $s \in \mathbb{C}$, the global zeta function is defined to be

$$\zeta(\chi, \Phi; s) = \int_{1_F} \Phi(a)\chi(a)|a|^s\text{d}^\times a.$$ 

When $\Phi = \otimes_v \Phi_v$ is a pure tensor,

$$\zeta(\chi, \Phi; s) = \prod_{v \in \Sigma_F} \zeta_v(s, \chi_v, \Phi_v) = \prod_{v \in \Sigma_F} \int_{F_v^*} \Phi_v(x)\chi_v(x)|x|^s\text{d}^\times x.$$ 

Where the local zeta functions $\zeta_v(\chi_v, \Phi_v; s)$ converge to a holomorphic function for $\text{Re}(s) > 0$ and the integral is absolutely convergent for $\text{Re}(s) > 1$.

Proof: For the local zeta function: $\Phi_v$ is rapidly decreasing, thus it suffices to integrate the part where $|x|_v < 1$. Then $\Phi_v$ is bounded on this compact region, thus it suffices to evaluate $\int_{|x|_v \leq 1} |x|^s\text{d}^\times x < \infty$ for $\text{Re}(s) > 0$, which can be done case by case.

To show the global integral converges, notice the local integrals is the same as the local L-factors for a.e. $v \in \Sigma_F$ by(16.2.2.3), so we can use Fubini and notice that $\prod_v \zeta_v(s, \chi_v, \Phi_v)$ converges by comparison with the Dedekind zeta function(16.2.2.1).
Prop. (16.2.2.3) [Unramified Factors]. For any place \( v \) that unramified in the sense of (12.2.6.19) and \( \Phi_v = 1_{\mathcal{O}_v} \),
\[
\zeta_v(\chi_v; \Phi_v; s) = L(\chi_v; s) = (1 - \chi_v(\varpi)(Np)^{-s})^{-1} (16.2.3.1).
\]

Proof: Notice the a.e. \( v \in \Sigma_F \) satisfies that unramified in the sense of (12.2.6.19) and \( \Phi_v = 1_{\mathcal{O}_v} \), and for such a \( v \),
\[
\zeta_v(\chi_v; \Phi_v; s) = \sum_{k \in \mathbb{N}} \int_{v(x)=k} \chi_v(x)|x_v|^s d^x x = \sum_{k \in \mathbb{N}} \int_{v(x)=k} (\chi_v(\varpi_v)|v|^{-s})^k = (1 - \chi_v(\varpi)(Np)^{-s})^{-1}.
\]

Prop. (16.2.2.4) [Global Functional Equation]. The global zeta function (16.2.2.2) can be extended to a meromorphic function for all \( s \), and it has poles iff \( \chi(x) = |x|^\lambda \) for some \( \lambda \in i\mathbb{R} \). In which case, it only has poles at
\[
s = \begin{cases} 
1 - \lambda, -\lambda & F \text{ is a number field} \\
1 - \lambda + \frac{2\pi i}{\log(q)}, -\lambda + \frac{2\pi i}{\log(q)} & F \text{ is a function field over } \mathbb{F}_q
\end{cases}
\]
with respectively residue \(-kf(0)\) and \(k\overline{f}(0)\), where \( k = V(I_F^1/F^\times)(12.2.6.20) \), and essentially bounded on the vertical strips away from the poles. And we have functional equations
\[
\zeta(\chi, \Phi; s) = \zeta(\chi^{-1}, \overline{\Phi}; 1 - s).
\]

Proof: Consider the exact sequence
\[
1 \to I_F^1 \to I_F \to |I_F| \to 1.
\]
Let \( I_F^1 \) be the inverse image of \( t \in |I_F| \), where \( |I_F| = \mathbb{R}_{>0} \) or \( q^\mathbb{Z} \), with Haar measure \( dt/t \log q \) or \( dt/t \), and choose Haar measure \( d^x \alpha \) and \( dt/t \). In particular, if \( |a_t| = t \),
\[
\int_{I_F^1} \int_{I_F^1} \Phi(a_t x)\chi(a_t x)t^s d^x x \frac{dt}{t} = \int_{I_F} \Phi(\alpha)\chi(\alpha)|\alpha|^s d^x \alpha.
\]
Then the measure \( d^x x \) and the counting measure on \( F^\times \) induces a measure \( d^x \alpha \) on \( I_F^1/F^\times \), in particular, for any \( f \in C(C_F) \), we have
\[
\int_{I_F^1/F^\times} f(x) d^x x = \int_{I_F^1/F^\times} f(a_t x) d^x x = \int_{I_F^1/F^\times} f(\frac{a_t}{x}) d^x x = \int_{I_F^1/F^\times} f(\frac{1}{x}) d^x x.
\]
Denote \( \zeta_t(\chi, \Phi; s) = \int_{I_F^1} \Phi(x)\chi(x)|x|^s d^x x \), then
\[
\zeta(\chi, \Phi; s) = \int_0^1 \zeta_t(\chi, \Phi; s) \frac{dt}{t} + \int_1^{\infty} \zeta_t(\chi, \Phi; s) \frac{dt}{t} = J + I
\]
where if \( |I_F| = q^\mathbb{Z} \) the value at 1 is counted half-half at this two part. Now for the \( I \)-part, if Re(\( s \)) is smaller, it is smaller, thus \( I \) extends to a holomorphic function to all \( s \in \mathbb{C} \). For the \( J \)-part, by lemmas (16.2.2.6)(16.2.2.5),
\[
J = \int_0^1 \zeta_1/t(\widehat{\Phi}, \chi^{-1}, 1-s) \frac{dt}{t} + \left[ \int_0^1 (k\Phi(0)(\frac{1}{t})^{1-s} - k\Phi(0)t^s) \frac{dt}{t} \right] \delta_{c,|t|}
\]
\[
\zeta_t(\tilde{\Phi}, \chi^{-1}, 1 - s) = \int_1^\infty \frac{\zeta_t(\tilde{\Phi}, \chi^{-1}, 1 - s)}{t} \, dt = \int_0^1 \left( k \tilde{\Phi}(0) t^{s-1} - k \Phi(0) t^s \right) \frac{dt}{t} \delta_c |1|
\]

So it can be extended, and the final part is

\[
\frac{k \tilde{\Phi}(0)}{s-1} - \frac{k \Phi(0)}{s}
\]

when \( F \) is number field, and when \( F \) is function field, it equals

\[
k \log q \left[ \tilde{\Phi}(0) \left( -\frac{1}{2} + \sum_{n=0}^{\infty} (q^{-n})^{s-1} \right) - \Phi(0) \left( -\frac{1}{2} + \sum_{n=0}^{\infty} (q^{-n})^{s} \right) \right] = \frac{k \log q}{2} \left( \tilde{\Phi}(0) \left( 1 + q^{1-s} \right) + \Phi(0) \left( 1 - q^s \right) \right).
\]

Now clearly \( \zeta(\chi, \Phi; s) = \zeta(\chi^{-1}, \tilde{\Phi}; 1 - s) \), and it has the desired residues at 1 and \(| \cdot |\). \( \square \)

**Lemma (16.2.2.5).** \( \int_{I_k/F^\times} \chi(x) |x|^s \, dx = kt^s \) if \( \chi = 1 \) and 0 otherwise.

*Proof:* \( \int_{I_k/F^\times} \chi(x) |x|^s \, dx = \chi(a_t) t^s \int_{I_k/F^\times} \chi(x) \, dx \), \( I_k/F^\times \) is compact (12.2.5.25) and \( \chi \) is trivial on \( I_k/F^\times \) iff \( \chi = 1 \), thus we can use (10.9.1.14). \( \square \)

**Lemma (16.2.2.6).** \( \zeta_t(\chi, \Phi; s) + \Phi(0) \int_{I_k/F^\times} \chi(x) |x|^s \, dx = \zeta_t(\tilde{\Phi}, \chi^{-1}; 1 - s) + \tilde{\Phi}(0) \int_{I_k/F^\times} \chi(x) |x|^s \, dx \).

*Proof:* \( \zeta_t(\chi, \Phi; s) + \Phi(0) \int_{I_k/F^\times} \chi(x) |x|^s \, dx = \int_{I_k/F^\times} \left( \sum_{a \in F^\times} \Phi(ax) \right) \chi(ax) |ax|^s \, dx + \int_{I_k/F^\times} \Phi(0) \chi(x) |x|^s \, dx \)

\[
= \int_{I_k/F^\times} \left( \sum_{a \in F} \tilde{\Phi}(a/x) \right) \chi(x) |x|^s \, dx
\]

(12.2.6.22) \( = \int_{I_k^*/K^\times} \left( \frac{1}{|x|} \right) \left( \sum_{a \in K} \tilde{\Phi}(a/x) \right) \chi(x) |x|^s \, dx \)

(by * \( ) \)

\[
= \int_{I_k^*/F^\times} \left( \sum_{a \in F} \tilde{\Phi}(ay) \right) |y| \chi^{-1}(y) |y|^{-s} \, dy \]

\[
= \zeta_t(\tilde{\Phi}, \chi^{-1}; 1 - s) + \tilde{\Phi}(0) \int_{I_k^*/F^\times} \chi(x) |x|^s \, dx.
\]

\( \square \)

**Local Functional Equations**

**Lemma (16.2.2.7).** For any \( \Phi_v, \Psi_v \in S(F_v), \chi_v \in \widehat{F_v^\times}, s \in \mathbb{C}, \)

\[
\frac{\zeta_v(\chi_v, \Phi_v; s)}{\zeta_v(\chi_v^{-1}, \tilde{\Phi_v}; 1 - s)} = \frac{\zeta_v(\chi_v, \Psi_v; s)}{\zeta_v(\chi_v^{-1}, \tilde{\Phi_v}; 1 - s)}.
\]
Proof:  

\[ \zeta(f, c)\zeta(\hat{g}, \overline{c}) = \int_{K} f(\alpha)c(\alpha) \int_{K} \hat{g}(\beta) c^{-1}(\beta) |\beta| d\beta = \int \int f(\alpha)\hat{g}(\beta)c(\alpha\beta^{-1})|\beta| d\alpha d\beta \]

by Fubini.

\[ = \int \int f(\alpha)\hat{g}(\alpha\beta)c(\beta^{-1})|\alpha\beta| d\alpha d\beta = \int (\int f(\alpha)\hat{g}(\alpha\beta)|\alpha| d\alpha)|\beta|c(\beta^{-1})d\beta \]

And notice

\[ \int_{K} f(\alpha)\hat{g}(\alpha\beta)|\alpha| |\beta|d\alpha = C \cdot \int_{K+\{0\}} f(\xi)\hat{g}(\xi\beta)d\xi = C \cdot \int_{K+} \int_{K+} f(\xi)g(\eta)e^{-2\pi i\Lambda(\xi\eta)}d\eta d\xi \]

which is clearly symmetric in \( f \) and \( g \). So the conclusion follows. \( \square \)

**Prop.(16.2.2.8)** [Local Functional Equations]. For any \( \Phi_v \in S(F_v), \chi_v \in (F_v^\times)^{v} \), the local zeta function \( \zeta_v(\chi_v, \Phi_v; s) \) can be extended to a meromorphic function to all \( s \in \mathbb{C} \) that is analytic for \( \text{Re}(s) > 0 \), and there is a function \( \gamma_v(\chi_v, \psi_v; s) \), meromorphic for \( s \) and independent of \( f \), such that

\[ \zeta_v(\chi_v^{-1}, \Phi_v; 1 - s) = \gamma_v(\chi_v, \psi_v; s)\zeta_v(\chi_v, \Phi_v; s). \]

**Proof:** By (16.2.2.2), both \( \zeta_v(\chi_v^{-1}, \Phi_v; 1 - s) \) and \( \zeta_v(\chi_v, \Phi_v; s) \) are holomorphic in \( 0 < \text{Re}(s) < 1 \), so we define \( \gamma_v(\chi_v, \psi_v; s) \) in this region, and try to extend it. Now (16.2.2.7) shows this is invariant of \( \Phi_v \), so we can take any \( \Phi_v \) we want. Notice if \( \Phi_v = 0 \) on a nbhd of 0, then \( \zeta_v(\chi_v, \Phi_v; s) \) is entire. Then because Fourier transform preserves \( S(F_v)(12.2.6.11) \), we can take \( \Phi_v \) to be 0 around 0 or \( \Phi_v \) to be 0 around 0, then \( \gamma_v(\chi_v, \psi_v; s) \) is analytic on both \( \text{Re}(s) > 0 \) and \( \text{Re}(s) < 1 \). \( \square \)

**Prop.(16.2.2.9).** Let \( v \in \Sigma_F^{\text{fin}} \) and \( \text{Re}(s) < 1 \), then for \( N \in \mathbb{Z}^+ \) sufficiently large,

\[ \gamma_v(s, \chi_v, \psi_v) = \int_{p^{-N}} |x|^{-s} \chi_v^{-1}(x)\psi_v(x)dx. \]

**Proof:** In (16.2.2.8), take \( \Phi_v = \mathbb{I}_{p^{+N}} \), then \( \hat{\Phi}_v = \mathbb{I}_{p^{-N}} \cdot \psi_v. \) \( \square \)

**Prop.(16.2.2.10).**

- \( \gamma(1 - s, \chi^{-1}, \psi) = \chi(-1)/\gamma(s, \chi, \psi). \)
- \( \rho(\overline{c}) = c(-1)\rho(c) \)

**Proof:**

1: \( \zeta(f, c) = \rho(c)\zeta(\hat{f}, \overline{c}) = \rho(c)\rho(\overline{c})\zeta(\hat{f}, c) = \rho(c)\rho(\overline{c})c(-1)\zeta(f, c) \)

2: \( \zeta(f, c) = \rho(c)\zeta(\hat{f}, \overline{c}), \quad \overline{\zeta(f, c)} = \overline{\zeta(\hat{f}, \overline{c})} = \rho(\overline{c})\zeta(\hat{\overline{f}}, \overline{c}) \)

And

\[ \overline{f}(\xi) = \int \overline{f}(\eta)e^{-2\pi i\Lambda(\xi\eta)}d\eta = \int f(\eta)e^{2\pi i\Lambda(\xi\eta)}d\eta = \overline{f}(-\xi) \]

so

\[ \rho(\overline{c})\zeta(\hat{f}, \overline{c}) = \rho(\overline{c})c(-1)\zeta(\hat{f}, \overline{c}) = \rho(\overline{c})c(-1)\zeta(f, c) \]

Thus \( \rho(\overline{c}) = c(-1)\rho(c). \) \( \square \)

**Cor.(16.2.2.11).** Because when \( \sigma(c) = \frac{1}{2}, \overline{c} = \overline{c} \), we have \( |\rho(c)| = 1 \) in this case.
3 Weber L-Functions (GL(1) Case)

**Def. (16.2.3.1) [Local L-Factors].** Given a Hecke character \( \chi \), for \( v \in \Sigma_F \) and \( s \in \mathbb{C} \) it is defined to be

\[
L(\chi_v; s) = \begin{cases} 
(1 - \chi_v(\infty) ||p||^{-s})^{-1} & v \in \Sigma_F^\infty, \chi_v \text{ unramified} \\
1 & v \in \Sigma_F^\infty, \chi_v \text{ ramified} \\
\pi^{-\frac{s+\varepsilon}{2}} \Gamma(s + v + \frac{|k|}{2}) & v \in \Sigma_F^R, \chi_v(x) = |x|^v \text{sgn}(x)^\varepsilon, \varepsilon = 0, 1, \\
2(2\pi)^{-s} & v \in \Sigma_F^C, \chi_v(x) = |x|^v e^{ik \arg(x)}, v \in i\mathbb{R}, k \in \mathbb{Z}.
\end{cases}
\]

Moreover, define

\[
L_R(s) = \pi^{\frac{s}{2}} \Gamma(s), \quad L_C(s) = 2(2\pi)^{-s} \Gamma(s).
\]

**Prop. (16.2.3.2) [Local L-factors are the Common Divisors].** Situation as in (16.2.2.8), \( \frac{\zeta_v(\chi_v, \Phi_v; s)}{L(\chi_v; s)} \) is entire for any \( \Phi_v \in S(F_v) \), and if \( v \in \Sigma_F^\infty \), it is a rational function of \( ||v||^{-s} \).

Moreover, if we take

\[
\Phi_v = \begin{cases} 
\tilde{\psi}_v & v \in \Sigma_F^\infty \\
x^{\varepsilon} e^{-\pi x^2} & v \in \Sigma_F^R, \chi_v(x) = \text{sgn}(x)^\varepsilon, \varepsilon = 0, 1, \\
(x)^{-k} e^{-2\pi|x|} & v \in \Sigma_F^C, \chi_v(x) = |x|^v e^{ik \arg(x)}, v \in i\mathbb{R}, k \in \mathbb{N} \\
x^{-k} e^{-2\pi|x|} & v \in \Sigma_F^C, \chi_v(x) = |x|^v e^{ik \arg(x)}, v \in i\mathbb{R}, k \in \mathbb{Z}.
\end{cases}
\]

then \( \zeta_v(\chi_v, \Phi_v; s) \) is of the form \( ab^s \) for \( a \in \mathbb{C}^* \), \( b \in \mathbb{R}_+ \).

**Proof:** For \( v \in \Sigma_F^\infty \),

\[
\zeta_v(\chi_v, \Phi_v; s) = \sum_{k \in \mathbb{Z}} q^k s \int_{v(x) = -k} \Phi_v(x) \chi_v(x) d^\times x
\]

As \( \Phi_v \in C_c^\infty(F_v) \), the summand is 0 for \( k \) large. And for \( k \) small, \( \Phi_v(x) \) is constant. If \( \chi_v \) is ramified, then these terms are 0, thus it is a polynomial in \( ||v||^{-s} \), and for \( \chi_v \) unramified, these terms are geometric series, which is easily seen to be a rational function of \( ||v||^{-s} \), and has the same pole as \( L(\chi_v; s) \).

For \( v \in \Sigma_F^R \), the poles of \( \zeta_v(\chi_v, \Phi_v; s) \) are the same as poles of \( \int_{|x| \leq 1} \Phi_v(x) \chi_v(x) |x|^s dx \), because \( \int_{|x| \geq 1} \Phi_v(x) \chi_v(x) |x|^s dx \) is convergent for any \( s \in \mathbb{C} \). For the former, we can write \( \Phi_v \) as a sum of an odd function and an even function. Only the part with the same parity of \( \chi_v \) will be non-zero, and for that part, by (10.5.3.6), its poles are all simple and are poles of \( L(\chi_v; s) \).

For \( v \in \Sigma_F^C \), if \( \chi_v(x) = |x|^v e^{ik \arg(x)}, v \in i\mathbb{R}, k \in \mathbb{Z} \),

\[
\zeta_v(\chi_v, \Phi_v; s) = \frac{1}{2\pi} \int_0^{\infty} \int_0^{2\pi} r^{2v+2s} e^{ik\theta} \Phi_v(re^{i\theta}) d\theta \frac{dr}{r} = \int_0^{\infty} r^{2v+2s} \varphi(r) \frac{dr}{r},
\]

where

\[
\varphi(r) = \frac{1}{2\pi} \int_0^{2\pi} e^{ik\theta} \Phi_v(re^{i\theta}) d\theta.
\]

Suppose \( \Phi_v(x) = \sum_{n,m \in \mathbb{N}} a(n, m) x^n \pi^m \), then \( \varphi(r) = \sum_{m-n=k} a(n, m) r^{m+n} \). Thus by (10.5.3.6), its pole are \( \{ s|2s + 2v - (|k| + 2l) \} \), which are all simple and are poles of \( L(\chi_v; s) \).

For the last assertion, we need direct calculations, Cf.[GTM186, P249].
Prop. (16.2.3.3) [Local \( \varepsilon \)-Factors]. Situation as in (16.2.2.8), there exists a non-vanishing holomorphic function \( \varepsilon_v(\chi_v, \psi_v) \) that
\[
\frac{\zeta_v(\chi_v^{-1}, \Phi_v; 1 - s)}{L(\chi_v^{-1}; 1 - s)} = \varepsilon_v(\chi_v, \psi_v; s) \frac{\zeta_v(\chi_v, \Phi_v; s)}{L(\chi_v; s)}.
\]
and \( \frac{\zeta_v(\chi_v, \Phi_v)}{L_v(\chi_v; s)} \) is holomorphic. Moreover, \( \varepsilon_v(\chi_v, \psi_v; s) \) is of the form \( ab^s \) for \( a \in \mathbb{C}^*, b \in \mathbb{R} \). And \( \varepsilon(\chi_v, \psi_v) = 1 \) if \( v \) is unramified in the sense of (12.2.6.19).

Proof: Such an \( \varepsilon_v(\chi_v, \psi_v; s) \) exists by (16.2.2.8). It is holomorphic and non-vanishing by (16.2.3.2) as both \( \frac{\zeta_v(\chi_v^{-1}, \Phi_v; 1 - s)}{L(\chi_v^{-1}; 1 - s)} \) and \( \frac{\zeta_v(\chi_v, \Phi_v; s)}{L(\chi_v; s)} \) are holomorphic and for any given \( s_0 \in \mathbb{C} \), \( \Phi_v \) can be chosen to make either one of them non-zero at \( s_0 \).

To show it is of the form \( ab^s \): If \( v \in \Sigma_F^{\text{fin}} \), it is a rational function in \( ||p||^{-s} \) with no zeros or poles, so it must be of the form \( ab^s \). And if \( v \) is unramified, then we can take \( \Phi_v = \mathbb{I}_{\mathcal{O}_F,v}, \Phi_v = \mathbb{I}_{\mathcal{O}_F,v} \) by (12.2.6.5), and both sides are 1 by (12.2.2.2).

If \( v \in \Sigma_F^\infty \), then we can take \( \Phi_v \) defined in (16.2.3.2) to do the calculation to show it directly, Cf.[Tate’s Thesis, P316]. \( \square \)

Prop. (16.2.3.4) [Global Hecke L-Functions]. For a Hecke character \( \chi = \prod_v \chi_v \) on \( F \) and \( s \in \mathbb{C} \), we define the global Hecke \( L \)-function as
\[
\Lambda(\chi; s) = \prod_v L(\chi_v; s)(16.2.3.1)
\]
which converges for \( \text{Re } s > 1 \) and has a meromorphic continuation to all \( s \in \mathbb{C} \).

Also, we can define the global \( \varepsilon \)-factor for \( \chi \) as
\[
\varepsilon(\chi; s) = \prod_v \varepsilon_v(\chi_v, \psi_v; s).
\]

All but f.m. of the product equals 1 by (16.2.3.3), and they are of the form \( ab^s \), so \( \varepsilon(s, \chi) \) is also of the form \( ab^s \), where \( a \in \mathbb{C}^*, b \in \mathbb{R} \). In particular, it is holomorphic and non-vanishing. The fact \( \varepsilon(s, \chi) \) is independent of \( \psi \) can be seen from (16.2.3.5).

Prop. (16.2.3.5) [Functional Equation of Hecke L-Functions]. For a Hecke character \( \chi \), \( L(\chi; s) \) has meromorphic continuation to all \( s \), and it has poles iff \( \chi(x) = |x|^\lambda \) for some \( \lambda \in i\mathbb{R} \). In this case, it only has simple poles at
\[
s = \begin{cases}
1 - \lambda, -\lambda & \text{if } F \text{ is a number field} \\
1 - \lambda + \frac{2\pi i}{\log(q)}, -\lambda + \frac{2\pi i}{\log(q)} & \text{if } F \text{ is a function field over } \mathbb{F}_q
\end{cases}
\]
with respectively residue \(-k\) and \( k||\mathbb{b}_F||^{-1/2} \), where \( k = V(I_F^1/F^\times)(12.2.6.20) \), and essentially bounded on the vertical strips away from the poles. And we have a functional equation
\[
\Lambda(\chi; s) = \varepsilon(\chi; s)\Lambda(\chi^{-1}; 1 - s),
\]
where \( \varepsilon(\chi; s) \) is of the form \( ab^s, a \in \mathbb{C}^\times, b \in \mathbb{R} \).
Proof: The functional equation follows from the definition of local $\varepsilon$-factors (16.2.3.3) and (16.2.2.4). To show it is essentially bounded on vertical strips, use

$$\frac{\Lambda(\chi; s)}{\zeta(\chi, \Phi; s)} = \prod_{v \in \Sigma_F} \frac{L(\chi_v; s)}{\zeta_v(\chi_v, \Phi_v; s)}$$

where we can take $\Phi_v$ s.t. each fraction is of the form $ab^s$, and a.e. term is 1, by (16.2.3.3). Then $L(\chi; s)$ is essentially bounded on vertical strips because $\zeta(\chi, \Phi; s)$ does (16.2.2.4).

To find the residues, if $\chi = 1$, we use the standard character on $A_F$ and look at $\Phi_v$ we take in (16.2.3.2), then we calculate $\Phi_v(0) = 1$ and $\hat{\Phi}_v(0) = ||b||^{-1/2}$, as we did in (12.2.6.5). □

**Dirichlet Characters**

Def. (16.2.3.6) [Dirichlet Character]. For a global field $F$ and a modulus $m$ for $F$, a **Dirichlet character modulo** $m$ is a functor $Cl_m(F) = \mathbb{J}^m/P^m \to \mathbb{C}^\times$.

A **primitive Dirichlet character** modulo $m$ is a Dirichlet character modulo $m$ that is injective.

Usually we consider the case $F = \mathbb{Q}$ and $m = m \cdot \infty$. In which case, a Dirichlet character is just a map $(\mathbb{Z}/(m))^\times \to \mathbb{C}^\times$.

Def. (16.2.3.7) [Gauss Sum]. Let $\chi$ be a primitive Dirichlet character mod $N$, then the **Gauss sum** of $\chi$ is defined to be

$$\tau(\chi) = \sum_{n \mod N} \chi(n)e^{2\pi in/N}.$$ 

Prop. (16.2.3.8). $\tau(\overline{\chi}) = \chi(-1)\overline{\tau(\chi)}$.

Prop. (16.2.3.9). $\sum_{n \mod N} \chi(n)e^{2\pi imn/N} = \overline{\chi(m)}\tau(\chi)(16.2.3.7)$.

Proof: If $(m, N) = 1$, then this follows from

$$\tau(\chi) = \sum_{n \mod N} \chi(mn)e^{2\pi imn/N} = \chi(m) \sum_{n \mod N} \chi(n)e^{2\pi imn/N}.$$ 

If $(m, N) \neq 1$, then we need to show the LHS is 0. Let $m = dM, N = dN_1$. Because $\chi$ is primitive character mod $N$, there is some $c \equiv 1$ mod $N_1$ that $\chi(c) \neq 1$, otherwise $\chi$ is defined mod $N_1$. Notice

$$\sum_{n \mod N} \chi(n)e^{2\pi imn/N} = \sum_{r \mod N_1} \left\{ \sum_{n \mod N, n \equiv r \mod N_1} \chi(n) \right\} e^{2\pi irM/N_1}$$

But $r \leftrightarrow cr$ is a permutation of $\{n \mod N, n \equiv r \mod N_1\}$, thus

$$\sum_{n \mod N, n \equiv r \mod N_1} \chi(n) = \sum_{n \mod N, n \equiv r \mod N_1} \chi(cn) = \chi(c) \sum_{n \mod N, n \equiv r \mod N_1} \chi(n)$$

which means this sum vanishes. □

Prop. (16.2.3.10). $|\tau(\chi)|^2 = N$. 
Proof: For any \(m\),
\[
| \sum_{n \mod N} \chi(n) e^{2\pi i m/n} |^2 = \sum_{(n_1n_2,N)=1} \chi(n_1)\overline{\chi(n_2)} e^{2\pi i (n_1-n_2)m/N},
\]
summing over \(m \in (\mathbb{Z}/N\mathbb{Z})^*\),
\[
\varphi(N)|\tau(\chi)|^2 = \sum_m \sum_{(n_1n_2,N)=1} \chi(n_1)\overline{\chi(n_2)} e^{2\pi i (n_1-n_2)m/N} = \sum_{n_1 \equiv n_2 \mod N,(n_1n_2,N)=1} N = \varphi(N)N.
\]
\(\square\)

Cor. (16.2.3.11). From this and (16.2.3.9) and also (16.2.3.8), we get that
\[
\chi(n) = \chi(1)N \frac{\tau(\chi)}{N} \sum_{m \mod N} \overline{\chi(m)} e^{2\pi i mn/N}.
\]

Prop. (16.2.3.12) [Gauss Sums]. Let \(\psi\) be a non-trivial character on a finite field \(F_q\), then let
\[
g_\psi = \sum_{x \in F_q} \psi(x^2),
\]
• \(|g_\psi|^2 = q^{1/2}.
• \(g_\psi(a) = (\frac{a}{F_q}) g_\psi(1).

Proof: Use Fourier transform on \(F_q^*\). \(\square\)

Def. (16.2.3.13) [Theta Function]. Let \(\chi\) be a primitive character modulo \(N\) s.t. \(\chi(-1) = 1\), define the Theta function
\[
\theta_\chi(t) = \frac{1}{2} \sum_{n=-\infty}^{\infty} \chi(n) e^{-\pi n^2 t} = \frac{1}{2} \chi(0) + \sum_{n=1}^{\infty} \chi(n) e^{-\pi n^2 t}.
\]

Dirichlet-Weber L-Functions

Cf.[Class Field Theory, Milne]

Def. (16.2.3.14) [Partial L-Functions]. Let \(F\) be a global field and \(m\) is a modulus for \(F\), \(\mathcal{R} \subset \text{Cl}_m(F)\) be an ideal class. Define the partial L-function
\[
\zeta(F,\mathcal{R};s) = \sum_{a \in \mathcal{R}} \frac{1}{(Na)^s}.
\]

Prop. (16.2.3.15). Situation as in (16.2.3.14), \(\zeta(F,\mathcal{R};s)\) is analytic for \(\Re(s) > 1 - 1/N\) except a simple pole at \(s = 1\), where it has residue \(g_m\) depending only on \(m\).

Proof: Cf.[Class Field Theory, Milne]. \(\square\)

Prop. (16.2.3.16) [Weber L-Functions]. Let \(F\) be a global field and \(m\) is a modulus for \(F\), \(\chi : \text{Cl}_m(F) \to \mathbb{C}^\times\) a Dirichlet character for \(F\), then the Weber L-function attached to \(\chi\) is defined to be the Euler product
\[
L(F,\chi; s) = \prod_{p|m} \frac{1}{1 - \chi(p)(Na)^s} = \sum_{(a,m)=1} \frac{\chi(a)}{(Na)^s} = \sum_{\mathcal{R} \in \text{Cl}_m(F)} \chi(\mathcal{R})\zeta(F,\mathcal{R};s).
\]
Thus by (16.2.3.15), \(L(K,\chi; s)\) is analytic for \(\Re(s) > 1 - 1/N\), except for possibly a simple pole at \(s = 1\). And for \(\chi \neq 1\), it is in fact analytic at \(s = 1\), as the residues cancelled out.
**Def. (16.2.3.17) [Dirichlet L-Functions].** For $F = \mathbb{Q}$, the characters of $\text{Cl}_m(\mathbb{Q})$ are just Dirichlet characters $\chi(12.2.5.33)$, thus the Weber L-function is

\[
L(s, \chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s},
\]

where $\Re s > 1$. Called the **Dirichlet L-function** attached to $\chi$.

**Prop. (16.2.3.18) [Functional Equation for Dirichlet L-Functions].** Let $\chi$ be a Dirichlet character with $\chi(-1) = (-1)^\varepsilon$ where $\varepsilon = 0$ or $1$, then

\[
\Lambda(\chi; s) = \pi^{-(s+\varepsilon)/2} \Gamma\left(\frac{s + \varepsilon}{2}\right) L(\chi; s),
\]

is the Hecke L-function attached to the Hecke character corresponding to $\chi(12.2.5.33)(16.2.3.4)$. Thus $L(s, \chi)$ can be extended to a meromorphic function for all $s \in \mathbb{C}$, and it has simple poles at $s = 0$ and $1$ when $\chi = 1$, and analytic otherwise. When $\chi = 1$, the residue of $\Lambda(\chi; s)$ at $s = 1$ is $-1$ by (16.2.3.21).

Moreover, there are functional equations

\[
\Lambda(\chi; s) = (-i)^\varepsilon \tau(\chi) N^{-s} \Lambda(\chi^{-1}; 1 - s),
\]

In other words,

\[
\varepsilon(\chi; s) = (-i)^\varepsilon \tau(\chi) N^{-s}.
\]

**Proof:** Cf. [Bum98] P10. \qed

**Prop. (16.2.3.19).** If $F$ is a number field and $\chi \neq 1$ is a Hecke character on $F$, then $L(\chi; 1 + it) \neq 0$ for any $t \in \mathbb{R}$.

**Proof:** Cf. [GTM186, P289]. \qed

### Riemann L-Functions

**Def. (16.2.3.20) [Riemann L-Functions].** For a global field $F$,

\[
\zeta(F; s) = L(F; 1; s)
\]

is called the **Riemann L-function** for $F$. Also denote

\[
\zeta(s) = \zeta(\mathbb{Q}; s), \quad \Lambda(s) = \Lambda(\mathbb{Q}, 1; s) = L_{\mathbb{R}}(s) \zeta(s).
\]

**Thm. (16.2.3.21) [Class Number Formula, Dirichlet].** By (12.2.6.20),

\[
-\text{res}_{s=1} \zeta_F(s) = \frac{2^{r_1}(2\pi)^{r_2}}{w_F \sqrt{|D_F|}} \text{Cl}_F \text{Reg}_F
\]

where $w_F = \# F^\times_{\text{tor}}$, $\text{Cl}_F = \text{Cl}(\mathcal{O}_F)$, and $\text{Reg}_F$ is the regulator.

In particular,

\[
\text{res}_{s=1} \zeta_{\mathbb{Q}}(s) = -1.
\]
Prop. (16.2.3.22) [Dirichlet’s Class Number Formula for Quadratic Fields]. Cf. [GTM 186 P288].

Prop. (16.2.3.23) [Kronecker’s First Limit Formula].

\[ \zeta(s) = \frac{1}{s-1} + \gamma_0 + O(s-1). \]

**Proof:** Cf. [Kronecker’s First Limit Formula, Revisited]. This can be deduced from (16.2.5.7). □

**Remark (16.2.3.24).** This is related to the the averaged Colmez’s Conjecture.

Prop. (16.2.3.25). \( \zeta(s) \neq 0 \) for \( \text{Re}(s) \geq 1 \).

Thm. (16.2.3.26) [Prime Number Theorem].

Prop. (16.2.3.27). For \( k \geq 1 \), \( \zeta(2k) = \frac{2^k}{(2k)!} B_{2k} \pi^{2k} \).

**Proof:** Because

\[ \cot(z) = i + \frac{2i}{e^{2iz} - 1}, \]
\[ z \cot(z) = 1 - \sum_{k=1}^{\infty} B_{2k} \frac{2^{2k} z^{2k}}{(2k)!} \]

where \( B_k \) are Bernoulli numbers (10.5.3.10). But also

\[ z \cot(z) = 1 - 2 \sum_{k=1}^{\infty} \zeta(2k) \frac{z^{2k}}{\pi^{2k}}. \]

by (10.5.3.12), thus the assertion follows. □

Prop. (16.2.3.28) [Leibniz Formula for \( \pi \)].

\[ 1 - \frac{1}{3} + \frac{1}{5} - \frac{1}{7} + \ldots = \frac{\pi}{4}. \]

**Proof:** Use the arctan integration formula. □

4 Godement-Jacquet Theory

Main references are [G-J72].

5 Rankin-Selberg Methods on \( \text{GL}(2) \times \text{GL}(2) \)

References are [Automorphic Forms on \( \text{GL}(2) \), Jacquet, 1972].

Def. (16.2.5.1) [Intro, Rankin-Selberg Method]. Delete this? . Converse theorems like (16.2.6.18), shows that a possible method of proving the existence of an automorphic form is to prove by any method the functional equations of sufficiently many of the the \( L \)-series attached to it. One of the most powerful methods of doing this is the **Rankin-Selberg method**, which seeks to represent an \( L \)-function as an integral of one or more automorphic forms against an Eisenstein series, itself a type of automorphic form.
Conj. (16.2.5.2) [Rankin-Selberg L-function]. For a global field $F$, assume the Langlands functoriality, for any $\pi_1 \in \operatorname{Irr}^{\text{auto}}(\text{GL}(n)/F)$ and $\pi_2 \in \operatorname{Irr}^{\text{auto}}(\text{GL}(m)/F)$, their product $\pi_1 \times \pi_2 \in \operatorname{Irr}^{\text{auto}}(\text{GL}(n) \times \text{GL}(m)/F)$, and there is a tensor product map $\otimes : \text{GL}(n) \times \text{GL}(m) \to \text{GL}(mn)$, which by functorial lifting (15.12.1.6) gives us an automorphic representation $\pi_1 \boxtimes \pi_2 \in \operatorname{Irr}^{\text{auto}}(\text{GL}(mn)/F)$, whose L-function is denoted by $L(s, \pi \times \pi')$ and for a finite set $S$ of places of $F$ large enough,

$$L_S(s, \pi_1 \times \pi_2) = \prod_{v \notin S} \prod_{1 \leq i,j \leq n} \frac{1}{1 - \alpha_i(\pi_{1,v})\beta(\pi_{2,v})q_v^{-s}}$$

called the (partial) Rankin-Selberg L-function of $\pi_1, \pi_2$. Here are some examples:

- $\pi_1 = \pi, \pi_2 = \hat{\pi}$, then for some $S$, then

$$L_S(s, \pi \times \hat{\pi}) = \prod_{v \notin S} \prod_{1 \leq i,j \leq n} \frac{1}{1 - \alpha_i(\pi_v)\alpha_j^{-1}(\pi_v)q_v^{-s}}.$$ 

In this case, this is the functorial lifting of

$$\text{GL}(n) \to \text{GL}(n) \times \text{GL}(n) \to \text{GL}(2n) : g \mapsto (g,g^{-t}) \mapsto g \otimes g^{-t}$$

by (15.10.3.7), which is isomorphic to the conjugation action of $\text{GL}(n)$ on $\text{Mat}(n)$. This action decomposes as a trivial action and a $n^2 - 1$-dimensional representation $\text{Ad}^0$. Thus there should be a decomposition

$$L_S(s, \pi \times \hat{\pi}) = \zeta_{F,S}(s)L_S(s, \pi, \text{Ad}^0)$$

where $\zeta_{F,S}(s)$ is the partial zeta function on $F$.

- $\pi_1 = \pi = \pi_2$, then for some $S$, then

$$L_S(s, \pi \times \hat{\pi}) = \prod_{v \notin S} \prod_{1 \leq i,j \leq n} \frac{1}{1 - \alpha_i(\pi_v)\alpha_j(\pi_v)q_v^{-s}}.$$ 

In this case, this is the functorial lifting of

$$\text{GL}(n) \to \text{GL}(n) \times \text{GL}(n) \to \text{GL}(2n) : g \mapsto (g,g) \mapsto g \otimes g$$

by (15.10.3.7), which decomposes as a $\frac{1}{2}n(n+1)$-dimensional symmetric square representation $\text{Sym}^2$, and a $\frac{1}{2}n(n-1)$-dimensional exterior square representation $\wedge^2$. Thus there should be a decomposition

$$L_S(s, \pi \times \hat{\pi}) = L_S(s, \text{Sym}^2\pi)L_S(s, \wedge^2\pi),$$

where $L_S(s, \text{Sym}^2\pi)$ and $L_S(s, \wedge^2\pi)$ are called the symmetric square L-functions and exterior square L-functions of $\pi$.

There are two Rankin-Selberg constructions of exterior square L-functions, which can be found in [Jacquet, H. and J. Shalika, Exterior square L-functions, in Automorphic Forms, Shimura Varieties and L-functions II, 1990] and [Bump, D. and S. Friedberg, The “exterior square” automorphic L-functions on GL(n), 47-65 in part 2 of Gelbart, Howe and Sarnak (1990)]. The construction of symmetric square L-functions can be found in [Bump, D. and D. Ginzburg, Symmetric square L-functions on GL(r), Annals of Math. 136 (1992)].
Prop. (16.2.5.3). For \( \pi_1 \in \text{Irr}^{\text{auto}}(\text{GL}(2)/F, \omega_1) \), \( \pi_2 \in \text{Irr}^{\text{auto}}(\text{GL}(2)/F, \omega_2) \), by tensor product theorem (15.10.2.12), we can fix a finite set \( \Sigma_F^\infty \subset S \subset \Sigma_F \) that any \( v \not\in S \) is unramified for both \( \pi_1, \pi_2 \) in the sense of (16.2.6.1). Let \( \alpha_i(v), \beta_i(v) \) be the Stake parameters of \( \pi_1, v, \pi_2, v \), then \( \pi_1 \cong \hat{\pi}_2 \) iff the Rankin-Selberg L-function (16.2.5.2)

\[
L_S(s, \pi_1 \times \pi_2) = \prod_{v \not\in S} \prod_{1 \leq i, j \leq 2} \frac{1}{1 - \alpha_i(v)\beta_j(v)}
\]

has a pole at \( s = 1 \).

Proof: Cf. [Bump, Chap3.8]. \( \square \)

Eisenstein Series

References are [Bump, Chap3].

Def. (16.2.5.4) [Non-Holomorphic Eisenstein Series]. The non-holomorphic Eisenstein series of weight \( s \) is defined to be

\[
E^*(z, s) = \frac{1}{2} L_R(2s) \sum_{(m,n) \neq 0 \in \mathbb{Z}^2} \frac{(\text{Im}(z))^s}{|mz + n|^{2s}} = L_R(2s) \sum_{\gamma \in \Gamma_{\infty} \setminus \Gamma(1)} (\text{Im}(\gamma(z)))^s
\]

It is absolutely convergent for \( \text{Re}(s) > 1 \), and is automorphic for \( \Gamma(1) \) (15.7.1.16).

Prop. (16.2.5.5) [Fourier Expansion of \( E(z, s) \)]. The Fourier coefficients of \( E(z, s) \) is of the form

\[
E^*(z, s) = \sum_{n=-\infty}^{\infty} a_n(y, s)e^{2\pi inz},
\]

where

\[
a_0(y, s) = \Lambda(2s)y^s + \Lambda(2 - 2s)y^{1-s}
\]

and for \( n \neq 0 \),

\[
a_n(y, s) = 2|n|^{-s+1/2} \sigma_{2s-1}(|n|) \sqrt{y} K_{s-1/2}(2\pi|n|y),
\]

where \( K_{s-1/2}(z) \) is the K-Bessel function (10.5.8.11). In particular,

\[
E^*(z, s) = \Lambda(2s)y^s + \Lambda(2 - 2s)y^{1-s} + 4\sqrt{y} \sum_{n \in \mathbb{Z}_+} n^{1/2-s} \sigma_{2s-1}(n) K_{s-1/2}(2\pi ny) \cos(2\pi nx)
\]

Proof:

\[
a_r(y, s) = \int_0^1 E^*(x + iy, s)e^{-2\pi irx}dx = \int_0^1 \frac{1}{2} \pi^{-s}\Gamma(s) \sum_{(m,n) \neq 0 \in \mathbb{Z}^2} \frac{y^s}{|mz + n|^{2s}} e^{-2\pi irx}dx.
\]

The term with \( m = 0 \) only contributes to \( a_0 \), and equals \( \pi^{-s}\Gamma(s)\zeta(2s)y^s \). For the rest we may assume \( m > 0 \) by symmetry, then they contribute to

\[
\pi^{-s}\Gamma(s)y^s \sum_{m=1}^{\infty} \sum_{n=-\infty}^{\infty} \int_0^1 \left[(mx + n)^2 + m^2y^2\right]^{-s} e^{-2\pi irx}dx.
\]


\[
\pi^{-s} \Gamma(s) y^s \sum_{m=1 \mod m} \sum_{n} e^{2\pi i n m} \int_{-\infty}^{\infty} \left( (mx+n)^2 + m^2 y^2 \right)^{-s} e^{-2\pi i m x} dx
\]

\[
= \pi^{-s} \Gamma(s) y^s \sum_{m=1 \mod m} \left( \frac{m^2 y^2}{m} \right) \int_{-\infty}^{\infty} \left( (mx+n)^2 + m^2 y^2 \right)^{-s} e^{-2\pi i m x} dx
\]

Notice \( \sum_{m=1 \mod m} e^{2\pi i n m} = \begin{cases} m | r & \text{if } m | r \\ 0 & \text{otherwise} \end{cases} \), thus the calculation reduces to (10.5.8.15).

**Prop. (16.2.5.6) [Functional Equation].** \( E^*(z, s) \) has meromorphic continuation to all \( s \in \mathbb{C} \), and it is analytic except at \( s = 1 \) or \( s = 0 \), where the residue at \( s = 1 \) is \( 1/2 \) for any \( z \), and it satisfies the functional equation

\[
E^*(z, s) = E^*(z, 1 - s).
\]

and \( E(x + iy, s) = O(y^\sigma) \) for \( y \to \infty \), where \( \sigma = \max(\text{Re}(s), 1 - \text{Re}(s)) \).

**Proof:** This follows from the Fourier expansion of \( E^*(z, s) \). Each term \( a_\tau(y, s) \) has analytic extension to all \( s \), except that \( a_0 \) has simple poles at \( s = 0 \) and \( s = 1 \) by (16.2.3.18) (the pole at \( s = 1/2 \) was neutralized). And the functional equation and the convergence is clear from the properties of K-Bessel functions (10.5.8.12). For the residue, it suffices to show the residue of \( \pi^{-s/2} \Gamma(s/2) \zeta(s) \) at 0 is \(-1\) (16.2.3.18).

**Prop. (16.2.5.7) [Kronecker’s First Limit Formula].**

\[
2E^*(z, s) = \frac{1}{s-1} + \gamma_0 - \log(4\pi y|\eta(z)|^4) + O(s-1).
\]

And a similar formula is true for \( s = 0 \), by the functional equation (16.2.5.6).

**Proof:** Cf. [Kronecker’s First Limit Formula, Revisited].

**Prop. (16.2.5.8) [Eisenstein Series of Mixed Type].** The Eisenstein series of mixed type is defined to be

\[
E_{k,s}(z) = \sum_{(m,n) \in \mathbb{Z}^2 \setminus (0,0)} \frac{y^s}{mz+n} \left( \frac{1}{k} \right)^{s+k} \left( \frac{mz+n}{2\pi} \right)^s, \quad k \in \mathbb{Z}, s \in \mathbb{C}.
\]

Then

\[
R_k(y^{k/2} E_{k,s}(z)) = (k+s)y^{(k+2)/2} E_{k+2,s}(z).
\]

and \( y^{k/2} E_{k,s}(z) \) is a Maass form in \( (z) \) of weight \( k \). Its better to consult the paper https://arxiv.org/abs/1803.08210 for the Fourier expansion of \( E_{k,s} \).

**Proof:**

\[
((z - \bar{z}) \frac{\partial}{\partial z} + k/2) \left( \frac{(z-\bar{z})^{s+k/2}}{(mz+n)^{s+k}} \right)
\]

\[
= (z - \bar{z}) \left( \frac{(z-\bar{z})^{s+k/2}}{(mz+n)^{s+k}} \right) + \frac{k}{2} \left( \frac{(z-\bar{z})^{s+k/2}}{(mz+n)^{s+k}} \right)
\]

\[
= \frac{(z-\bar{z})^{s+k/2}}{(mz+n)^{s+k+1}} [((s+k/2)(mz+n) - (z-\bar{z})m(s+k) + k/2(mz+n)]
\]

\[
= \frac{(z-\bar{z})^{s+k/2}}{(mz+n)^{s+k+1}} [(s+k/2)(mz+n) - (z-\bar{z})m(s+k) + k/2(mz+n)]
\]

\[
= \frac{(z-\bar{z})^{s+k/2}}{(mz+n)^{s+k+1}} [(s+k/2)(mz+n) - (z-\bar{z})m(s+k) + k/2(mz+n)]
\]

\[
= \frac{(z-\bar{z})^{s+k/2}}{(mz+n)^{s+k+1}} [(s+k/2)(mz+n) - (z-\bar{z})m(s+k) + k/2(mz+n)]
\]

\[
= \frac{(z-\bar{z})^{s+k/2}}{(mz+n)^{s+k+1}} [(s+k/2)(mz+n) - (z-\bar{z})m(s+k) + k/2(mz+n)]
\]

\[
= \frac{(z-\bar{z})^{s+k/2}}{(mz+n)^{s+k+1}} [(s+k/2)(mz+n) - (z-\bar{z})m(s+k) + k/2(mz+n)]
\]

\[
= \frac{(z-\bar{z})^{s+k/2}}{(mz+n)^{s+k+1}} [(s+k/2)(mz+n) - (z-\bar{z})m(s+k) + k/2(mz+n)]
\]

\[
= \frac{(z-\bar{z})^{s+k/2}}{(mz+n)^{s+k+1}} [(s+k/2)(mz+n) - (z-\bar{z})m(s+k) + k/2(mz+n)]
\]
16.2. L-FUNCTIONS ATTACHED TO AUTOMORPHIC REPRESENTATIONS

\[ (k + s) \left( \frac{z - \bar{z}}{2i} \right)^{s-1 + (k+2)/2} \]

\[ - \left( m \bar{z} + n \right)^{s+1} (m \bar{z} + n)^{s-1} \]

\[ (k + s) y^{(k+2)/2} E_{k+2,s-1}(z) \]

Prop. (16.2.5.9) [Rankin-Selberg]. Let \( \varphi \in C^\infty(\Gamma(1) \backslash \mathcal{H}) \) be decreasing rapidly along \( y \to \infty \) and \( \varphi(z) = \sum_{n \in \mathbb{Z}} \varphi_n(y) e^{2\pi i nz} \) be its Fourier expansion. Call \( \varphi_0 \) the constant term of \( \varphi \). Consider the Mellin transform

\[ M(s, \varphi_0) = \int_{0}^{\infty} \varphi_0(y) y^s \frac{dy}{y} \]

\[ \Lambda(s, \varphi_0) = \Lambda(2s) M(s - 1, \varphi_0). \]

As \( \varphi(s, \varphi_0) \) is bounded as a function on \( y \) and decay rapidly, \( M(s, \varphi) \) is absolutely convergent for \( \text{Re}(s) > 0 \).

Then

\[ \Lambda(s, \varphi_0) = \int_{\Gamma(1) \backslash \mathcal{H}} \mathcal{E}^*(z, s) \varphi(z) \frac{dxdy}{y^2} \]

and thus has a meromorphic continuation to all \( s \) and satisfies a functional equation, with at most simple poles at \( s = 0 \) or \( 1 \),

\[ \text{Res}_{s=1} \Lambda(s, \varphi_0) = \frac{1}{2} \int_{\Gamma(1) \backslash \mathcal{H}} \varphi(z) \frac{dxdy}{y^2}. \]

Proof: Using (16.2.5.4),

\[ \int_{\Gamma(1) \backslash \mathcal{H}} \varphi(z) \frac{dxdy}{y^2} = \Lambda(2s) \sum_{\gamma \in \Gamma_0(1)} \int_{\Gamma(1) \backslash \mathcal{H}} (\text{Im}(\gamma(z)))^s \varphi(\gamma(z)) \frac{dxdy}{y^2} \]

\[ = \Lambda(2s) \int_{\Gamma_0 \backslash \mathcal{H}} \text{Im}(z)^s \varphi(z) \frac{dxdy}{y^2} \]

\[ = \Lambda(2s) \int_{\infty}^{\infty} y^{s-1} \int_{0}^{1} \varphi(x + iy) dx \frac{dy}{y} \]

\[ = \Lambda(2s) \int_{\infty}^{\infty} \varphi_0(y) y^{s-1} dy \]

\[ = \Lambda(s, \varphi_0) \]

The assertion about the meromorphic continuation and the residue follows from the equation above and (16.2.5.6). □

Rankin-Selberg for Modular Forms

Prop. (16.2.5.10) [Convolution of Cusp Forms]. If \( f(z) = \sum A(n) q^n \in S_k(\Gamma(1)) \), \( g(z) = \sum B(n) q^n \in M_k(\Gamma(1)) \), define

\[ L(f \times g; s) = \zeta(2s - 2k + 2) \sum A(n) B(n) n^{-s}, \quad \Lambda(f \times g; s) = (2\pi)^{-2s} \Gamma(s) \Gamma(s - k + 1) L(f \times g; s), \]

then \( L(s, f \times g) \) is absolutely convergent for \( s \) large, \( \Lambda(s, f \times g) \) has a meromorphic continuation to all \( s \), analytic except for at most simple poles at \( s = k \) or \( s = k - 1 \), and it satisfies a functional equation

\[ \Lambda(s, f \times g) = \Lambda(2k - 1 - s, f \times g). \]
and the residue of $\Lambda$ at $s = k$ is $\frac{1}{2} \pi^{1-k}(f, g)(15.11.1.12)$. Moreover, if $f, g$ are Hecke eigenforms, let

$$1 - A(p)X + p^{k-1}X^2 = (1 - \alpha_1(p)X)(1 + \alpha_2(p)X),$$

$$1 - B(p)X + p^{k-1}X^2 = (1 - \beta_1(p)X)(1 - \beta_2(p)X),$$

then $L(s, f \times g)$ has an Euler product formula

$$L(s, f \times g) = \prod_p \prod_{n=1}^{2} \prod_{j=1}^{2} \frac{1}{1 - \alpha_j(p)\beta_j(p)p^{-s}}.$$

**Proof:** We may assume $f, g$ are Hecke eigenforms $(15.11.3.12)$, so $A(n), B(n)$ are real. Let $\varphi(z) = f(z)\overline{g(z)}y^k$, then $\varphi$ satisfies the condition of the Rankin-Selberg method $(16.2.5.9)$, thus we calculate

$$\varphi_0(y) = \int_0^1 f(x + iy)g(x + iy)y^k \, dx = \sum_{n=0}^\infty \int_{m=0}^\infty \int_0^1 A(n)B(n)e^{2\pi i(n-m)x}e^{-2\pi(n+m)y}y^k \, dx$$

$$= \sum_{n=0}^\infty A(n)B(n)e^{-4\pi ny}y^k$$

and

$$M(s, \varphi_0) = \sum_{n=0}^\infty A(n)B(n) \int_0^\infty e^{-4\pi ny}y^{s+k} \, dy = (4\pi)^{-s-k}\Gamma(s+k) \sum_{n=0}^\infty A(n)B(n)n^{-s-k}$$

and

$$\Lambda(s, \varphi_0) = 4^{-s-k+1}\pi^{-2s-k+1}\Gamma(s)\Gamma(s+k-1)\zeta(2s) \sum_{n=0}^\infty A(n)B(n)n^{-s-k+1}.$$ 

Thus

$$\Lambda(s - k + 1, \varphi_0) = \pi^{k-1}\Lambda(s, f \times g),$$

and the assertion follows from $(16.2.5.9)$. The residue is also clear.

The Euler product formula follows from $(7.5.2.3)$ applied to $z = p^{-s}$ for all $p \in \mathbf{P}$. □

**Remark (16.2.5.11) [Averaged Ramanujan Conjecture].** By the Ramanujan conjecture $(16.2.6.16)$, for any cuspidal form $f = \sum a(n)q^n$, $L(s, f) = \sum a_n n^{-s}$ is convergent for $\text{Re}(s) > \frac{k+1}{2}$. But we can prove this directly: as $\sum a_n^2 n^{-s}$ is convergent for $\text{Re}(s) > k$, and $|a(n)| \leq \max(n^{\frac{k+1}{2}}, n^{-\frac{k+1}{2}}|a(n)|^2)$.

**Waldspurger’s Theorem**

Cf.[Explicit application of Waldspurger’s theorem].

**Thm. (16.2.5.12) [Waldspurger].** Let $\chi$ be a character, $k \in 2\mathbf{Z}$ and $\varphi \in S_{k-1}(N, \chi^2)$, then there exists a function $A_\varphi$ on $\mathbf{N}^{sc}$ s.t. for $t \in \mathbf{N}^{sc}$,

$$A_\varphi(t) = L(\varphi \otimes \chi_0^{-1}\chi_t, \frac{k-1}{2})\varepsilon(\chi_0^{-1}\chi_t, \frac{1}{2}).$$

**Proof:** Cf.[Explicit application of Waldspurger’s theorem]. □
6 Eulerian Integrals on \(GL(2) \times GL(1)\)

Main references are [Cog00] and [Bum98].

**Def. (16.2.6.1) [Unramified Places].** Let \((\pi, V)\) be an irreducible cuspidal representation, given a pure cuspidal form \(\varphi \in V\) and a Hecke character \(\xi\) of \(F\), we call a place \(v\) of \(F\) **unramified** iff \(v \in \Sigma^\text{fin}_F\), the conductor of \(\psi_v\) is \(O_v\) and the conductor of \(\xi_v\) is \(O_v^*\), \(\pi_v\) is a spherical principal series.

This condition is true for a.e. \(v\) by (15.10.4.2) and (15.10.4.3).

**Def. (16.2.6.2) [Zeta Functions for \(GL(2) \times GL(1)\)].** Given \((\pi, V) \in \text{Irr}^{\text{auto}}(GL(2)/F, \omega), \xi\) a Hecke character, for any \(\Phi \in V\), consider the zeta integral

\[
\zeta(\Phi, \xi; s) = \int_{C_F} \Phi\left(\begin{bmatrix} y & 0 \\ 1 & 1 \end{bmatrix}\right) |y|^{s-1/2} \xi(y) d^\times y
\]

It is absolutely convergent by (15.10.4.5) and (12.2.5.25).

If \(\Phi = \otimes \Phi_v\) is a pure tensor, the zeta integral equals

\[
\int_{I_F} W_\Phi\left(\begin{bmatrix} y & 0 \\ 1 & 1 \end{bmatrix}\right) |y|^{s-1/2} \xi(y) d^\times y = \prod_v \int_{F_v^\times} W_{\Phi_v}\left(\begin{bmatrix} y_v & 0 \\ 1 & 1 \end{bmatrix}\right) |y_v|^{s-1/2} \xi_v(y_v) d^\times y_v = \prod_v \zeta_v(\Phi_v, \xi_v; s)
\]

where each **local zeta functions** \(\zeta_v(s, \Phi_v, \xi_v)\) converges absolutely to a holomorphic function for \(\text{Re}(s) > 1/2\), and the integral is absolutely convergent when \(\text{Re}(s) > 3/2\), using (10.9.1.38).

**Proof:** We analyze the integrand for the local zeta integrals:

For non-Archimedean case, the integrand is compactly supported on (15.8.3.19), and because \(\pi_v\) is unitary, use (15.8.4.23) and (15.8.6.10) to analyze the Kirillov model of \(\pi_v\), we see the integral converges absolutely for \(\text{Re}(s) > 1/2\).

For Archimedean case, the \(W_\varphi\) decays rapidly for \(|y| \to \infty\), and for \(|y| \to 0\), by (15.7.4.2), it is bounded by \(|y|^{-1/2}\), thus it also converges absolutely for \(\text{Re}(s) > 1/2\).

By (16.2.6.3), the local factor is the same as the local L-factor a.e. \(v\), and \(|\alpha_i| < |v|^{1/2}\) by (15.8.6.10), thus it converges for \(\text{Re}(s) > 3/2\) by comparison with the Dedekind Zeta function (16.2.2.1).

**Prop. (16.2.6.3) [Unramified Factors].** If \(v\) is unramified in the sense of (16.2.6.1) and \(\Phi_v\) is the spherical function in \(\pi_v\) normalized s.t. \(W_{\Phi_v}(1) = 1\), then for \(\text{Re}(s) > 1/2\)(thus all, as they are both meromorphic),

\[
\zeta_v(\Phi_v, \xi_v; s) = L(\pi_v, \xi_v; s)(16.2.6.10).
\]

**Proof:** With the unramified hypothesis, there is an explicit formula for \(W_v\) in terms of the Satake parameters \(\alpha_1, \alpha_2\) (15.8.5.15): if \(\text{ord}_v(y) = m\), then

\[
W_v\left(\begin{bmatrix} y & 0 \\ 1 & 1 \end{bmatrix}\right) = \begin{cases} \frac{|v|^{-m/2} \alpha_1^{m+1} - \alpha_2^{m+1}}{\alpha_1 - \alpha_2} & m \geq 0 \\ 0 & \text{otherwise} \end{cases}
\]

\[
\zeta_v(W_v, \xi_v; s) = \sum_{m=0}^{\infty} |v|^{-m/2} \frac{\alpha_1^{m+1} - \alpha_2^{m+1}}{\alpha_1 - \alpha_2} |v|^{m/2 - ms} \xi(v) = \frac{1}{(1 - \alpha_1 \xi(v)|v|^{-s})(1 - \alpha_2 \xi(v)|v|^{-s})} = L(\pi_v, \chi_v; s)
\]

\(\square\)
Prop. (16.2.6.4) [Global Functional Equation]. In spite of the convergence problem of the product of local zeta integrals, the global zeta integral is absolutely convergent for any $s$ as $W_\Phi$ decay rapidly. Moreover, because $\Phi$ is automorphic, we have
\[
\zeta(\Phi, \xi; s) = \int_{C(F)} \Phi(w_1 \begin{bmatrix} y \\ 1 \end{bmatrix}) |y|^{s-1/2} \xi(y) d^\times y
\]
\[
= \int_{C(F)} \Phi(\begin{bmatrix} 1 \\ y \end{bmatrix} w_1) |y|^{s-1/2} \xi(y) d^\times y
\]
\[
= \int_{C(F)} (\pi(w_1) \Phi)(\begin{bmatrix} y \\ 1 \end{bmatrix}) |y|^{-s+1/2} (\xi \omega)^{-1}(y) d^\times y
\]
\[
= \zeta(\pi(w_1) \Phi, \xi^{-1} \omega^{-1} ; 1 - s)
\]

Local Functional Equation

Prop. (16.2.6.5) [Local Zeta Function]. Let $K$ be a $p$-adic local field and $(\pi, V) \in \text{Irr}_{\text{adm, generic}}(GL(2, K))$, if we identify $V$ with its Kirillov model, then for any $\varphi \in V$, quasi-character $\xi$ of $K^\times$, the local zeta integral $\zeta(\Phi, \xi; s)(16.2.6.2)$ is absolutely convergent for $\text{Re}(s)$ sufficiently large, and defines a holomorphic function there. And it has a meromorphic continuation to all $s$. In fact,
\[
\zeta(\Phi, \xi; s) = p_{\varphi, \xi}(q^{-s}) L(\pi, \xi; s), \quad p_{\varphi, \xi} \in \mathbb{C}[X, X^{-1}].
\]
Moreover, $\Phi$ can be chosen s.t. $p_{\varphi, \xi} = 1$.

Proof: This is by direct calculation: If $V$ is cuspidal, then $V = C_0^\infty(K^\times)$ by (15.8.3.20). If $V$ is not cuspidal, then by (15.8.4.20) it is $\pi(\chi_1, \chi_2)$ or $\sigma(\chi_1, \chi_2)$, whose elements are known (15.8.4.22) (15.8.4.23). For $\text{Re}(s)$ sufficiently large, the $|t| > q^{-k}$ part can contribute to any $p(q^{-s})$ for $p \in \mathbb{C}[q^s, q^{-s}]$ with degree $\leq k - 1$, and the $|t| \leq q^{-k}$ part is of the form
\[
\int_{p^k \setminus \{0\}} (\chi_i \xi)(y)|y|^s d^\times y = \sum_{n \geq k} (((\chi_i \xi)(\varpi) q^{-s})^n \int_{O^*} (\chi_i \xi)(y) d^\times y = C \frac{\alpha_k^s q^{-ks}}{1 - \alpha_i q^{-s}},
\]
where $C \neq 0$ iff $\chi_i \xi$ is unramified, or of the form
\[
\int_{p^k \setminus \{0\}} v(y)(\chi_i \xi)(y)|y|^s d^\times y = \sum_{n \geq k} n((\chi_i \xi)(\varpi) q^{-s})^n \int_{O^*} (\chi_i \xi)(y) d^\times y = C \frac{\alpha_k^s q^{-ks}}{(1 - \alpha_i q^{-s})^2},
\]
where $C \neq 0$ iff $\chi_i \xi$ is unramified.

Clearly $p_{\varphi, \xi}$ can be chosen to be 1 if we choose the compactly supported part of $\varphi$ suitably. □

Prop. (16.2.6.6) [Local Functional Equations]. The local zeta integral $\zeta_v(\Phi_v, \xi_v; s)$, defined in (16.2.6.2) has a meromorphic continuation to all $s$, and there exists a meromorphic function $\gamma_v(x, \pi_v, \xi_v, \psi_v)$ s.t.
\[
\zeta_v(\pi_v(w_1) \Phi_v, \xi_v^{-1} \omega_v^{-1} ; 1 - s) = \gamma_v(\pi_v, \xi_v, \psi_v; s) \zeta_v(\Phi_v, \xi_v; s).
\]

Proof: This follows by similar method as the proof of (16.2.2.8) and by evaluating $\gamma_v(\pi_v, \xi_v, \psi_v; s)$ explicitly, using methods of Weil representation parallel to the proof of (16.2.6.8), Cf.[Jacquet-Langlands(1970), P37].
There are easier way to prove this when \( v \in \Sigma_{\text{fin}}^\text{er} \). We show that both sides are linear functionals on \( \Phi \in V \) that satisfies
\[
L(\pi(\begin{bmatrix} y \\ 1 \end{bmatrix})\varphi) = \xi^{-1}(y)|y|^{-s+1/2}L(\varphi).
\]
This is true for RHS by a change of variable and analytic continuation \((16.2.6.5)\), and then also true for LHS.

Thus for general \( s \), \((15.8.3.22)\) shows two sides differ by a scalar \( \gamma(s, \pi, \xi, \psi) \). By \((16.2.6.5)\), for general \( s \), both sides can be non-zero, thus \( \gamma(s, \pi, \xi, \psi) \) is non-zero, and thus a meromorphic function of \( s \). \( \square \)

**Prop.\((16.2.6.7)\) [Gamma Factor Determines Representations]**. For \( (\pi_1, V_1), (\pi_2, V_2) \in \text{Irr}^{\text{adm, generic}}(GL(2, K)) \), if \( \gamma(s, \pi_1, \xi, \psi) = \gamma(s, \pi_2, \xi, \psi) \) for any quasi-character \( \xi \) of \( K^\times \), then \( \pi_1 \cong \pi_2 \).

**Proof**: Identify \( V_i \) with their Kirillov models, and let \( V_0 = V_1 \cap V_2 \). Then it suffices to show that \( \pi_1(w_1), \pi_2(w_1) \) acts the same on \( V_0 \): This is because \( V_0 \) contains \( \mathcal{C}_*^\infty(K^\times) \), and \( B(K) \) action on \( V_1, V_2 \) are the same by \((15.8.3.15)\), and \( GL(2, F) \) is generated by \( B(F) \) and \( w_1 \). Then \( V_0 = V_1 = V_2 \) as they are irreducible representations.

For \( \varphi \in V \), let \( \varphi_i = \pi_i(w_1)\varphi \), then it suffices to show \( \varphi_1(1) = \varphi_2(1) \): For other \( a \),
\[
\varphi_i(a) = (\pi_i(\begin{bmatrix} a \\ 1 \end{bmatrix} \begin{bmatrix} 1 \\ -1 \end{bmatrix})\varphi)(1) = (\pi_i(\begin{bmatrix} 1 \\ -1 \end{bmatrix} \begin{bmatrix} 1 \\ a \end{bmatrix})\varphi)(1)
\]
and
\[
\pi_1(\begin{bmatrix} 1 \\ a \end{bmatrix})\varphi = \pi_2(\begin{bmatrix} 1 \\ a \end{bmatrix})\varphi.
\]

For \( n \in \mathbb{Z} \), let
\[
F_\xi(n) = \int_{\mathbb{Q}_1 \backslash \mathbb{A}_{\mathbb{Q}} \mathbb{A}_{\mathbb{Q}}} (\varphi_1(y) - \varphi_2(y))\xi(y)d^\times y,
\]
then \( F_\xi(0) \) only depends on the restriction of \( \xi \) to \( \mathcal{O}^* \), and \( F_\xi(0) = 0 \) for all but f.m. characters \( \xi \) of \( \mathcal{O}^* \): \( \varphi_1 - \varphi_2 \) is a locally constant function that is fixed by \( U \subset \mathcal{O}^* \), so in order \( F_\xi(0) \neq 0 \), at least \( \xi \) should be trivial on \( U \), and there are f.m. such characters. Thus the hypothesis of Fourier transform on \( \mathcal{O}^* \) is satisfied \((10.9.3.24)\) and
\[
\varphi_1(1) - \varphi_2(1) = \sum_{\xi \in (\mathcal{O}^*)^\wedge} F_\xi(0).
\]

The hypothesis and the functional equation \((16.2.6.6)\) shows \( Z(s, \varphi_1, \xi) = Z(s, \varphi_2, \xi) \) for any quasi-character \( \xi \) of \( F^* \), so
\[
\sum_{n} F_\xi(n)q^{-sn} = Z(s, \varphi_1, \xi) - Z(s, \varphi_2, \xi) = 0
\]
and \( F_\xi(n) = 0 \) for \( n \) sufficiently small, thus \( F_\xi(n) = 0 \) for all \( n \). In particular, \( F_\xi(0) = 0 \), for any \( \xi \). \( \square \)

**Prop.\((16.2.6.8)\) [Gamma Factor Commutes with Parabolic Induction]**. If \( (\pi, V) = B(\chi_1, \chi_2) \) is irreducible, then
\[
\gamma(s, \mathcal{B}(\chi_1, \chi_2), \xi, \psi) = \gamma(s, \xi \chi_1, \psi)\gamma(s, \xi \chi_2, \psi).
\]

Proof: Cf. [Bump, P548].? This uses the concrete realization of the Whittaker model of \( \mathcal{B}(\chi_1, \chi_2) \) as a quotient of the Weil representation in the split case. \( \square \)

Jacquet-Langlands L-Functions (GL(2) × GL(1) Case)

Def. (16.2.6.10)[Local L-Factors for \( \text{GL}(2) \)]. Given \( \pi \in \text{Irr}^{\text{auto}}(\text{GL}(2)/F, \omega) \), for \( v \in \Sigma^\text{fin}_F \), the local L-factor is defined to be

\[
L(\pi_v; s) = \begin{cases} 
1 & , v \in S_{\text{cusp}}(\pi) \\
\frac{1}{(1-\alpha_1 q^{-s})(1-\alpha_2 q^{-s})} & , \pi_v = \pi(\chi_1, \chi_2) \\
\frac{1}{1-\alpha q^{-s}} & , \pi_v = \sigma(\chi_1, \chi_2), \quad \chi_1 \chi_2^{-1} = | \cdot |^{-1}
\end{cases}
\]

It follows from (15.8.4.20) and (15.8.4.2) that any irreducible representation of \( \text{GL}(2, F_v) \) is one of the form above. Also when \( \xi \) is a quasi-character of \( F^\times \), define

\[
L(\pi_v, \xi_v; s) = L(\pi_v(\xi_v); s).
\]

Prop. (16.2.6.11) [L-Factors as the Common Divisors]. Situation as in (16.2.6.6), \( \frac{\zeta_v(\Phi_v, \xi_v; s)}{L_v(\pi_v, \xi_v; s)} \) is entire for any \( \Phi_v, \xi_v \), and if \( v \in \Sigma^\text{fin}_F \), then it is a rational function of \( ||v||^{-s} \).

Moreover, for each \( (\pi_v, V_v) \), we can take specific \( \Phi_v \in V_v \) s.t. \( \frac{\zeta_v(\Phi_v, \xi_v; s)}{L_v(\pi_v, \xi_v; s)} \) is of the form \( ab^s \) for \( a \in \mathbb{C}^\times, b \in \mathbb{R}_+ \).

Proof: Cf. [Jacquet-Langlands, GL(2)]. \( \square \)

Prop. (16.2.6.12) [Local \( \varepsilon \)-Factors]. Situation as in (16.2.6.6), there exists a non-vanishing holomorphic function \( \varepsilon_v(\pi_v, \xi_v, \psi_v; s) \) s.t.

\[
\frac{\zeta(\pi(w_1)\Phi_v, \xi_v^{-1}; 1-s)}{L_v(\pi_v, \xi_v^{-1}; s)} = \varepsilon_v(\pi_v, \xi_v, \psi_v; s) \frac{\zeta(\Phi_v, \xi_v; s)}{L_v(\pi_v, \xi_v; s)}
\]

and \( \frac{Z(s, \Phi, \xi)}{L_v(s, \pi_v, \xi_v)} \) is holomorphic. Moreover, \( \varepsilon_v(s, \pi_v, \xi_v, \psi_v) \) is of the form \( ab^s \) for \( a \in \mathbb{C}^\times, b \in \mathbb{R} \). And \( \varepsilon_v(s, \pi_v, \xi_v, \psi_v) = 1 \) if \( v \) is unramified in the sense of (16.2.6.1).

Proof: Such a meromorphic \( \varepsilon_v(\pi_v, \xi_v, \psi_v; s) \) exists by (16.2.6.6). It is holomorphic and non-vanishing by the same reason as in (16.2.3.3) as both \( \frac{\zeta(\Phi_v, \xi_v; s)}{L_v(\pi_v, \xi_v; s)} \) and \( \frac{\zeta(\pi(w_1)\Phi_v, \xi_v^{-1}; 1-s)}{L_v(\pi_v, \xi_v^{-1}; s)} \) are holomorphic by (16.2.6.11) and for any given \( s_0 \in \mathbb{C}, \Phi_v \) can be chosen to make either one of them non-zero at \( s_0 \).

To show it is of the form \( ab^s \): If \( v \in \Sigma^\text{fin}_F \), it is a rational function in \( ||v||^{-s} \) with no zeros or poles, so it must be of the form \( ab^s \). And if \( v \) is unramified, then we can let \( \Phi_v \) be the spherical function in \( \pi_v \) normalized s.t. \( W_{v, \nu}(1) = 1 \), then \( \pi(w_1)\Phi_v \) is the normalized spherical function of \( \pi_v \). Then by (12.2.6.5), both sides are 1 by (12.2.6.3).

If \( v \in \Sigma^\text{inf}_F \), then we can take \( \Phi_v, \xi_v \) defined (16.2.3.2) to do the calculation to show it directly, Cf. [Jacquet-Langlands, GL(2)].? 

\( \square \)
Prop. (16.2.6.13) [Global L-Functions for $GL(2) \times GL(1)$]. Define

$$L(\pi, \xi; s) = \prod_v L_v(\pi_v, \xi_v; s), \quad \varepsilon(\pi, \xi; s) = \prod_v \varepsilon_v(\pi_v, \xi_v, \psi_v; s)$$

Then $\varepsilon(\pi, \xi; s)$ is independent of $\psi$, and $L(s, \pi, \xi)$ satisfies a functional equation

$$L(\pi, \xi; s) = \varepsilon(\pi, \xi; s)L(\overline{\pi}, \xi^{-1}; s)$$

**Proof:** This follows from (16.2.6.12) and (16.2.6.4). \hfill $\square$

Prop. (16.2.6.14) [Non-Vanishing on Re$(s) = 1$]. For $\pi \in \text{Irr}^{\text{cusp}}(GL(n)/F)$, $L(s; \pi) \neq 0$ on the line Re$(s) = 1$.

**Proof:** Cf. [A Non-Vanishing Theorem for Zeta Functions of $GL(n)$, Jacquet-Shalika (1976)]. \hfill $\square$

### Modular Forms

Prop. (16.2.6.15) [Trivial Bound]. If $f \in S_k(\Gamma(N))$, suppose $f(z) = \sum_{n \geq 0} a_n e^{2\pi inz/N}$, then $|a_n| = O(n^{k/2})$.

**Proof:** $a_n = \int_0^N f(x + iy)e^{-2\pi in(x+iy)/N} \, dx$ for any $y$, so let $y = N/n$, then $a_n = \int_0^N f(x + iN/n)e^{-2\pi inx/N} \, dx$. As $f$ is a cusp modular form, $(\text{Im}(z))^{k/2}|f(z)|$ is cuspidal automorphic function, thus bounded on $\mathcal{H}$, thus $|a_n| \leq C(N/n)^{k/2}$. \hfill $\square$

Thm. (16.2.6.16) [Ramanujan-Petersson Conjecture]. Let $f$ be a cuspidal Hecke eigenform of weight $k$ for $\Gamma(1)$, then for any prime $p$, $|a_p(f)| \leq 2p^{(k-1)/2}$.

**Proof:** By (15.11.3.12) this means the eigenvalue $\lambda_p$ of $f$ w.r.t. $T_p$ satisfies $|\lambda_p| \leq 2p^{1/2}$. This is a consequence of Weil conjecture and modularity?. \hfill $\square$

Def. (16.2.6.17) [L-functions associated to Modular Forms]. Each $f \in M_k(\Gamma_1(N))$ has an associated L-functions: if $f = \sum_{n=0}^\infty a_n q^n$, define

$$L(s, f) = \sum_{n=1}^\infty a_n n^{-s}.$$ 

Prop. (16.2.6.18) [Functional Equations of Modular Forms, Hecke]. Let $a_0, a_1, \ldots$ be a sequence of complex numbers s.t. $a_n = O(n^M)$ for some integer $M$. Given $\lambda > 0, k > 0, C = \pm 1$, write

$$\varphi(s) = \sum_{n=1}^\infty a_n n^{-s}, \quad \Phi(s) = \left(\frac{2\pi}{\lambda}\right)^{-s} \Gamma(s) \varphi(s), \quad f(z) = \sum_{n=0}^\infty a_n e^{2\pi inz/\lambda}.$$ 

Then the following conditions are equivalent:

- The function $\Delta(s) = \Phi(s) + \frac{a_0}{n} + \frac{C a_0}{k-\lambda}$ can be analytically continued to a holomorphic function of the whole plane which is bounded on vertical strips, and it satisfies the functional equation

  $$\Phi(s) = C \Phi(k - s).$$

- In the upper half plane, $f$ satisfies the functional equation

  $$f(-1/z) = C(z/i)^k f(z).$$
Thus for \( \text{Re}(s) \) large,
\[
\Phi(s) = \int_0^\infty (f(it) - a_0)t^s dt = \int_1^\infty (f(it) - a_0)t^s dt + \int_1^\infty (f\left(\frac{i}{t}\right) - a_0)t^{-s} dt.
\]

If \( 2 \) holds, then \( f\left(\frac{i}{t}\right) = Ct^k f(it) \), and
\[
\Phi(s) = \int_1^\infty (f(it) - a_0)t^s dt + \int_1^\infty (Ct^k f(it) - a_0)t^{-s} dt = \int_1^\infty (f(it) - a_0)t^s dt + C \int_1^\infty (f(it) - a_0)t^{k-s} dt + \int_1^\infty (Ct^{k-s}a_0 - t^{-s}a_0) dt.
\]

The first two integrals are absolutely convergent for any \( s \) and then can be extended to an analytic function of the whole plane, and the final term equals
\[
-(\frac{a_0}{s} + \frac{Ca_0}{k-s})
\]
when \( \text{Re}(s) \) is large, so it can be extended to a meromorphic function on the whole plane. And \( \Phi(s) = \Phi(k-s) \) follows easily from the equation above. Also it is bounded on vertical strips because it attain maximum at the real axis.

Conversely, first notice it suffices to prove for real \( y > 0 \),
\[
f\left(\frac{i}{y}\right) = Cy^k f(iy)
\]

because this implies these two holomorphic functions on \( \mathcal{H} \) coincide on the imaginary axis, so they must be equal. Notice
\[
\int_0^\infty (f(iy) - a_0)y^s \frac{dy}{y} = \Phi(s)
\]
converges absolutely for \( \text{Re}(s) \) sufficiently large, so for \( \sigma > 0 \) sufficiently large, Mellin inversion formula (10.10.2.16) shows
\[
f(iy) - a_0 = \frac{1}{2\pi i} \int_{\sigma - i\infty}^{\sigma + i\infty} \Phi(s)y^{-s} ds = \frac{C}{2\pi i} \int_{\sigma - i\infty}^{\sigma + i\infty} \Phi(k-s)y^{-s} ds = \frac{C}{2\pi i} \int_{\sigma - i\infty}^{\sigma + i\infty} (\Lambda(k-s) - \frac{Ca_0}{s} - \frac{a_0}{k-s})y^{-s} ds
\]

Notice \( \Phi(\sigma + it) \) decays exponentially for fixed \( \sigma = \alpha \) sufficiently large, because of the Stirling formula (10.5.8.8), and for \( \sigma = \beta \) sufficiently small, \( \Phi(s) = C\Phi(k-s) \) also shows \( \Phi(\sigma + it) \) decays exponentially. And also \( \frac{Ca_0}{\sigma + it} + \frac{a_0}{k - \sigma - it} = O(t^{-1}) \) for \( \sigma = \alpha \) or \( \beta \), so \( \Lambda(\sigma + it) = O(t^{-1}) \) for \( \sigma \) large or small, and also the hypothesis shows \( \Lambda \) is bounded on the strip \( \alpha < \text{Re}(z) < \beta \), thus by (10.5.5.9), \( \Lambda(\sigma + it) \to 0 \) for \( t \to 0 \) and \( \sigma \) in any compact set. So we can move the integration of \( \Lambda(s) \) to the left or to the right. Then
\[
f(iy) - a_0 = \frac{C}{2\pi i} \int_{\sigma - i\infty}^{\sigma + i\infty} (\Lambda(k-s) - \frac{Ca_0}{s} - \frac{a_0}{k-s})y^{-s} ds
\]
\[
= \frac{C}{2\pi i} \int_{\sigma-i\infty}^{\sigma+i\infty} y^{-k} \Lambda(s)y^s ds - \frac{1}{2\pi i} \int_{\sigma-i\infty}^{\sigma+i\infty} (\frac{a_0}{s} + \frac{Ca_0}{k-s})y^{-s} ds \\
= Cy^{-k} \int_{\sigma-i\infty}^{\sigma+i\infty} \Phi(s)y^s ds + \frac{Cy^{-k}}{2\pi i} \int_{\sigma-i\infty}^{\sigma+i\infty} (\frac{a_0}{s} + \frac{Ca_0}{k-s})y^s ds + \frac{1}{2\pi i} \int_{k-s-i\infty}^{k-s+i\infty} (\frac{a_0}{s} + \frac{Ca_0}{k-s})y^{-k} ds \\
= Cy^{-k}(f(\frac{i}{y}) - a_0) + \frac{y^{-k}}{2\pi i} \int_{\gamma} (\frac{Ca_0}{s} + \frac{a_0}{k-s})y^s ds \\
= Cy^{-k}(f(\frac{i}{y}) - Ca_0y^{-k} + y^{-k}(Ca_0 - a_0y^k)) = Cy^{-k}f(\frac{i}{y}) - a_0
\]

So we are done. \(\square\)

**Def. (16.2.6.19) [L-Functions of Modular Forms].** Let \(a_1, a_2, \ldots\) be a sequence of complex numbers such that \(a_n = O(n^M)\) for some \(M > 0\). Let

\[
L(s) = \sum a_n n^{-s}, \quad \Lambda(s) = (2\pi)^{-s} \Gamma(s)L(s), \quad f(z) = \sum a_n e^{-2\pi i nz}.
\]

More generally, let \(m > 0\) and \(\chi\) a primitive character mod \(m\), then we define **twisted L-function** as

\[
L(f, \chi; s) = \sum a_n \chi(n)n^{-s}, \quad \Lambda(f, \chi; s) = L_C(s)L(f, \chi; s)
\]

Notice if \(f(x) = \in S_k(\Gamma(1))\), and \(\pi_f \in \text{Irr}^{\text{auto}}(\text{GL}(2)/\mathbb{Q})\) corresponding to \(f\) via(15.10.3.12), then

\[
L(f, \chi; s) = L(\pi_f, \chi; s).
\]

**Prop. (16.2.6.20) [Converse Theorem (Correspondence for \(\Gamma(1)\)).]** If \(f \neq 0 \in S_k(\Gamma(1))(\text{so } k \text{ is even}), \) then \(\Lambda(s, f) = (2\pi)^{-s} \Gamma(s)L(s, f)\) has analytic continuation to all \(s\), is bounded on vertical strips, and satisfies a functional equation

\[
\Lambda(s, f) = (-1)^{k/2}\Lambda(k-s, f).
\]

Conversely, let \(a_0, a_1, \ldots\) be a sequence of complex numbers that \(a_n = O(n^M)\) for some \(M > 0\). Let \(f(s), L(s), \Lambda(s)\) be defined in(16.2.6.19) and \(\Lambda(s)\) has analytic continuation to all \(s\) and satisfies the above functional equation then \(f(z) \in S_k(\Gamma(1))\).

Moreover, in this case, \(f\) is a normalized Hecke eigenform(15.11.3.12) iff \(L(s, f)\) has as Euler product formula

\[
L(s) = \prod_p (1 - a_p p^{-s} + p^{k-1-2s})^{-1}
\]

for \(s\) sufficiently large, where \(1 - a_sX + p^{k-1}X^2 = (1 - aX)(1 - \overline{a}X), \text{ where } |a| = p^{\frac{k-1}{2}}\).

**Proof:** The first part is a direct consequence of(16.2.6.18). Notice \(a_n\) is bounded by polynomials in \(n\) by(16.2.6.15).

When \(s\) is large, the Euler product is absolutely convergent, thus it suffices to compare the coefficients. By(15.11.3.12) and(15.11.3.10), \(f\) being a normalized Hecke eigenform is equivalent to

\[
\begin{cases}
    c_mc_n = c_{mn}, & (m, n) = 1 \\
    c_pc_p = c_{p^{n+1}} + p^{2k-1}c_{p^{k-1}}
\end{cases}
\]

which is equivalent to

\[
(1 - a_pX + p^{k-1}X^2)(\sum_{r=0}^{\infty} a_{pr}X^r) = 1.
\]

\(\square\)
Prop. (16.2.6.21) [Functional Equation associated to $S_k(N, \psi)$]. Notation as in (16.2.6.19). If $f(z) \in S_k(N, \psi)(15.11.1.10)$. Denote $w_N = \begin{bmatrix} 0 & -1 \\ N & 0 \end{bmatrix}$, then $w_N$ stabilizes $\Gamma_0(N)$ because
\[ w_N \begin{bmatrix} a & b \\ c & d \end{bmatrix} w_N^{-1} = \begin{bmatrix} d & -c/N \\ bN & a \end{bmatrix} \]
Also notice $\psi(a_\gamma) = \overline{\psi(d_\gamma)}$, so
\[ f[w_N]_k[\gamma]_k = f[w_N \gamma w_N^{-1}]_k[w_N]_k = \overline{\psi(d)} f[w_N]_k. \]
So $g = f[w_N]_k \in S_k(N, \overline{\psi})$.

Now if
\[ f(z) = \sum a_n e^{2 \pi i n z/N}, g(z) = \sum b_n e^{2 \pi i z/N}, \]
and $\chi$ is a primitive character mod $D$, define $L(s, f, \chi), L(s, g, \overline{\chi}), \Lambda(s, f, \chi), \Lambda(s, g, \overline{\chi})$ as in (16.2.6.19), then $\Lambda(s, f, \chi)$ extends to an analytic function for all $s \in \mathbb{C}$, and there are functional equations
\[ \Lambda(s, f, \chi) = i^k \chi(N) \psi(D) \frac{\tau(\chi)^2}{D} (D^2 N)^{-s+k/2} \Lambda(k - s, g, \overline{\chi}), \quad (16.1) \]
where $\tau(\chi)$ is the Gauss sum of $\chi(16.2.3.7)$.

In particular, if $D = 1$, then
\[ \Lambda(s, f) = i^k N^{-s+k/2} \Lambda(k - s, g). \quad (16.2) \]

Proof: Let
\[ f_\chi(z) = \sum \chi(n) a_n q^n, \quad g_\overline{\chi}(z) = \sum \overline{\chi(n)} b_n q^n. \]

Use (16.2.3.11) on $f_\chi(z)$, we get
\[ f_\chi = \frac{\chi(-1) \tau(\chi)}{D} \sum_{m \in (\mathbb{Z}/D^2 \mathbb{Z})^\times} \overline{\chi(m)} f[\begin{bmatrix} D \\ m \end{bmatrix}]_k. \]

Now
\[ f_\chi[\begin{bmatrix} D^2 N \\ -1 \end{bmatrix}]_k = f_\chi[\begin{bmatrix} D \\ -1/DN \end{bmatrix}]_k = \frac{\chi(-1) \tau(\chi)}{D} \sum_{m \in (\mathbb{Z}/D^2 \mathbb{Z})^\times} \overline{\chi(m)} g[w_N^{-1}]_k[\begin{bmatrix} D \\ m \end{bmatrix}]_k[\begin{bmatrix} -1/DN \\ D \end{bmatrix}]_k = \frac{\chi(-1) \tau(\chi)}{D} \sum_{m \in (\mathbb{Z}/D^2 \mathbb{Z})^\times} \overline{\chi(m)} g[\begin{bmatrix} D \\ -Nm \end{bmatrix}]_k[\begin{bmatrix} r \\ s \end{bmatrix}]_k \]
where $(r, s)$ are integers chosen that $D s - r N m = 1$. Thus $\overline{\chi(m)} = \chi(-N) \chi(r)$, and because $g \in M_k(N, \overline{\psi})$,
\[ f_\chi[\begin{bmatrix} D^2 N \\ -1 \end{bmatrix}]_k = \frac{\chi(N) \tau(\chi)}{D} \sum_{r \in (\mathbb{Z}/D^2 \mathbb{Z})^\times} \chi(r) \psi(D) g[\begin{bmatrix} D \\ r \end{bmatrix}]_k. \]

Compare this with the formula
\[ g_\overline{\chi} = \frac{\chi(-1) \tau(\overline{\chi})}{D} \sum_{m \in (\mathbb{Z}/D^2 \mathbb{Z})^\times} \chi(m) g[\begin{bmatrix} D \\ m \end{bmatrix}]_k, \]
we get
\[
f_{\chi} \left[ D^2 N \begin{bmatrix} -1 \\ D N \end{bmatrix} \right] = \chi(-N) \psi(D) \frac{\tau(\chi)}{\tau(\chi)} \gamma_\chi = \chi(N) \psi(D) \frac{\tau(\chi)^2}{D} g_\chi. \tag{16.2.3.8}(16.2.3.10)
\]

Now similar to the proof of (16.2.6.18),
\[
\Lambda(s, f, \chi) = \int_0^\infty f_\chi(iy) y^s dy.
\]

So when \(\text{Re}(s)\) is large,
\[
\chi(N) \psi(D) \frac{\tau(\chi)^2}{D} \Lambda(s, g, \chi) = \chi(N) \psi(D) \frac{\tau(\chi)^2}{D} \int_0^\infty g_\chi(iy)y^s dy
\]
\[
= \int_{D^{\sqrt{N}}} (D^2 N)^{-k/2}(iy)^{-k} f_\chi \left( \frac{1}{D^2 N iy} \right) y^s dy + \chi(N) \psi(D) \frac{\tau(\chi)^2}{D} \int_{D^{\sqrt{N}}} g_\chi(iy) y^s dy
\]
\[
= \int_{D^{\sqrt{N}}} (D^2 N)^{k/2} t^k \chi(it) (D^2 N t)^{-s} dt + \chi(N) \psi(D) \frac{\tau(\chi)^2}{D} \int_{D^{\sqrt{N}}} g_\chi(iy) y^s dy
\]
\[
= i^{-k} (D^2 N)^{k/2-s} \int_{D^{\sqrt{N}}} \chi(it) t^k \frac{dt}{t} + \chi(N) \psi(D) \frac{\tau(\chi)^2}{D} \int_{D^{\sqrt{N}}} g_\chi(iy) y^s dy
\]

Both integrals are absolutely convergent for any \(s\). And similarly when \(\text{Re}(s)\) is small,
\[
i^{-k} (D^2 N)^{k/2-s} \Lambda(k - s, f, \chi) = i^{-k} (D^2 N)^{k/2-s} \int_{D^{\sqrt{N}}} \chi(it) t^k \frac{dt}{t}
\]
\[
= i^{-k} (D^2 N)^{k/2-s} \int_{D^{\sqrt{N}}} \chi(it) t^k \frac{dt}{t} + \chi(N) \psi(D) \frac{\tau(\chi)^2}{D} \int_{D^{\sqrt{N}}} g_\chi(iy) y^s dy
\]

Thus we get the desired result. \(\square\)

**Cor. (16.2.6.22).** As \(f([w^2_N])_k = (-1)^k f\), if \(f \in S_k(\Gamma_1(N))\) satisfies \(f[w_N]_k = cf\), \(c = \varepsilon i^k\), \(\varepsilon = \pm 1\), then
\[
N^{s/2} \Lambda(s, f, \chi) = \varepsilon (-1)^k (N^{k-s}/2) \Lambda(k - s, f, \chi).
\]

so \(\text{ord}_{1/2}(L(s, f))\) is even if \(\varepsilon = (-1)^k\) and odd if \(\varepsilon = (-1)^{k+1}\).

In particular, if \(N = 1\) and \(k \equiv 2 \text{ mod } 4\), \(L(1/2, f) = 0\).

It is conjectured that \(L(1/2, f) \neq 0\) if \(4 | k\). Cf.[Modular Forms, Ribet] P148.

**Prop. (16.2.6.23)[Converse Theorem, Weil].** Let \(N > 0\) and \(\psi\) a character mod \(N\). Suppose \(a_n, b_n\) are two sequence of complex numbers that \(|a_n|, |b_n| = O(n^M)\) for some positive integer \(M\). If \((D, N) = 1\) and \(\chi\) is a primitive character mod \(D\), let
\[
L_1(s, \chi) = \sum \chi(n)a_n n^{-s}, \quad L_2(s, \chi) = \sum \overline{\chi(n)}b_n n^{-s},
\]
and \(\Lambda_i(s, \chi_i) = (2\pi)^{-s} \Gamma(s)L_i(s, \chi_i)\).

Now if for \(D\) equals to a.e. \(p\) and any primitive character mod \(D\), \(\Lambda_i(s, \chi)\) has analytic continuation to all \(s\), are bounded on vertical strips, and satisfy the functional equation
\[
\Lambda_1(s, \chi) = i^k \chi(N) \psi(D) \frac{\tau(\chi)^2}{D} (D^2 N)^{-s+k/2} \Lambda_2(k - s, \chi),
\]
where \(\tau(\chi)\) is the Gauss sum of \(\chi(16.2.3.7)\), then \(f(z) = \sum a_n e^{2\pi i n z} \in M_k(N, \psi)\).
Proof: Let 

\[ f_\chi(z) = \sum \chi(n) a_n q^n, \quad g_\chi(z) = \sum \chi(n) b_n q^n. \]

We first show equation 16.3 holds. As in the proof of (16.2.6.18), it suffices to show the functional equation it is true on the positive imaginary axis. If \( \sigma = \text{Re}(s) \) is sufficiently large, then

\[ \int_0^\infty f_\chi(iy) y^s \frac{dy}{y} = \Lambda_1(s, \chi) \]

so by Mellin inversion formula

\[ f_\chi(iy) = \frac{1}{2\pi i} \int_{s-i\infty}^{s+i\infty} \Lambda_1(s, \chi) y^{-s} ds = i^k \chi(N) \psi(-D) \frac{\tau(\chi)^2}{D} \frac{1}{2\pi i} \int_{s-i\infty}^{s+i\infty} (D^2 N)^{-s+k/2} \Lambda_2(k - s, \chi) ds \]

Same argument of Phragmén-Lindelöf principle as in proof of (16.2.6.18) shows \( \Lambda_2(\sigma + it, \chi) \) converges to 0 for \( t \to \infty \), uniformly on any compact subset, so we can move the integral horizontally and make a change of variable \( s \mapsto k - s \) to get

\[ f_\chi(iy) = i^k \chi(N) \psi(-D) \frac{\tau(\chi)^2}{D} (D^2 N)^{-k/2} y^{-k} \frac{1}{2\pi i} \int_{s-i\infty}^{s+i\infty} \Lambda_2(k - s, \chi)(D^2 N y)^s ds \]

which is equivalent to 16.3.

The rest is to manipulate \( 2 \times 2 \) matrices and use (15.7.1.15) to show that \( g \in M_k(N, \psi) \), Cf.[Bump, P62].

Remark (16.2.6.24). For \( \Gamma(1) \), the function only requires one functional equation, and we used the fact \( \Gamma(1) \) is generated by \( S \) and \( T \). But \( \Gamma_0(N) \) is not generated by two elements, so we must assume functional equations for the twists \( L(s, f, \chi) \) also.

Maass Forms

See Wei’s notes.

7 Langlands-Shahidi Method

8 Triple Product

Cf.[Bump]
16.3 L-Functions Attached to Galois Representations

1 Artin L-Functions


Def. (16.3.1.1) [Local Artin L-Factors]. For a Galois extension of global fields \( L/F \) and \( \rho \in \text{Rep}(\text{Gal}(L/F)) \),

\[
L_v(F, \rho; s) = \begin{cases} 
  (\det(1 - (Np)^{-s}\rho(\varphi_{\mathfrak{q}/p})|V^f_{\mathfrak{q}}))^{-1}, & v \in \Sigma^{\text{fin}}_F \\
  L_C(s)\chi(1), & v \in \Sigma^c_F \\
  L_R(s)^n + L_R(s + 1)^n, & v \in \Sigma^R_F 
\end{cases} \quad (16.2.3.1)
\]

where in the case \( v \in \Sigma^{\text{fin}}_F \), \( \mathfrak{q} \) is a prime over \( p = \mathfrak{p}_v \), and in the case \( v \in \Sigma^c_F \), let \( p = \mathfrak{p}_v \). \( \mathfrak{q} \) be any place of \( L \) over \( p \), and let \( \varphi_{\mathfrak{q}} \) be the generator of \( \text{Gal}(L_{\mathfrak{q}}/F_p) \), then

\[
   n_+ = \frac{\chi(1) + \chi(\varphi_{\mathfrak{q}})}{2}, \quad n_- = \frac{\chi(1) - \chi(\varphi_{\mathfrak{q}})}{2}.
\]

Prop. (16.3.1.2) [Functoriality of Artin L-Factors]. For a Galois extension of global fields \( L/F \) and \( (\rho, V) \in \text{Rep}(\text{Gal}(L/F)) \), \( v = \mathfrak{p}_v \in \Sigma_F \), The Artin L-factors (16.3.1.1) satisfy the following functorial properties:

- \( L_v(F, \mathbb{1}; s) = L_v(\mathbb{1}; s) \).
- For \( \rho, \rho' \in \text{Rep}(\text{Gal}(L/F)) \), \( L_v(F, \rho \oplus \rho'; s) = L_v(F, \rho; s)L_v(F, \rho'; s) \).
- For Galois extensions \( L'/L/K \) and \( p \in \text{Rep}(\text{Gal}(L/F)) \), \( L(L'/F, \rho; s) = L(L/F, \rho; s) \).
- If \( F \subset M \subset L \), \( \rho \in \text{Rep}(\text{Gal}(L/M)) \), then \( L_p(F, \text{Ind}_{\text{Gal}(L/M)}^{\text{Gal}(L/F)}(\rho); s) = \prod_{q|p} L_q(M, \rho; s) \).

Proof: 1, 2, 3 are clear.

For 4: Let \( G = \text{Gal}(L/F), H = \text{Gal}(L/M) \), for any \( p \in \Sigma^{\text{fin}}_F \), let \( \{q_1, \ldots, q_r\} = S(p) \subset \Sigma^{\text{fin}}_M \), and take \( \mathfrak{q}_i \in \Sigma^{\text{fin}}_L \) over \( q_i \). Let \( G_i, I_i \) be the decomposition and inertia groups of \( \mathfrak{q}_i/p \), then \( H_i = G_i \cap H, I_i' = I_i \cap H \) are the decomposition and inertia groups of \( \mathfrak{q}_i/q_i \). Denote \( f_i \) the inertia degree of \( q_i/p \). Let \( (\rho, W) \in \text{Rep}(\text{Gal}(L/M)) \), \( (\rho', V) = \text{Ind}_{\text{Gal}(L/M)}^{\text{Gal}(L/F)}(\rho) \in \text{Rep}(\text{Gal}(L/F)) \), then it suffices to show that

\[
\det(1 - \varphi_{\mathfrak{q}_i/p} T f_i |V^f_{\mathfrak{q}_i}) = \prod_{i=1}^r \det(1 - \varphi_{\mathfrak{q}_i/p} T f_i |W^f_{\mathfrak{q}_i}).
\]

If \( \mathfrak{q}_i = \tau_i^{-1} \mathfrak{q}_i \), then we can take \( \varphi_{\mathfrak{q}_i/p} = \tau_i^{-1} \varphi_{\mathfrak{q}_i/p} \tau_i, I_i = \tau_i^{-1} I \tau_i, \) then

\[
\det(1 - \varphi_{\mathfrak{q}_i/p} T f_i |W^f_{\mathfrak{q}_i}) = \det(1 - \varphi_{\mathfrak{q}_i/p} T f_i |W^f_{\mathfrak{q}_i \cap I \tau_i^{-1}}),
\]

and \( f_i = (G : H_i I_i) = (G_1 : (G_1 \cap \tau_i H \tau_i^{-1}) I_i) \).

Let \( \sigma_{ij} \) be a representative of \( G_1/(G_1 \cap \tau_i H \tau_i^{-1}) \), then because \( G/H = \cup_i G_i/H_i, \{\sigma_{ij} \tau_i\}_{ij} \) is a representative of \( G/H \). Then

\[
   V = \oplus_i \bigoplus_j \sigma_{ij} \tau_i W,
\]
and \( V_i = \bigoplus_j \sigma_j \tau_i W = \text{Ind}_{G_1 \cap \tau_i H_{r_i}^{-1}}^{G_1} \tau_i W \) is a \( G_1 \)-module. So
\[
\det(1 - \varphi_{\mathbb{F}_p} T | V_i^{f_i}) = \prod_{i=1}^{r} \det(1 - \varphi_{\mathbb{F}_p} T | V_i^{f_i})
\]
Then it suffices to prove for each \( i \),
\[
\det(1 - \varphi_{\mathbb{F}_p} T | V_i^{f_i}) = \det(1 - \varphi_{\mathbb{F}_p} T | W_i^{f_i}).
\]
Notice
\[
V_i^{f_i} = \left( \text{Ind}_{G_1 \cap \tau_i H_{r_i}^{-1}}^{G_1} \tau_i W \right)^{f_i} = \text{Ind}_{H_i}^{G_1} W_i^{\tau_i}(15.1.4.47) = \bigoplus_{i=0}^{f_i-1} \varphi_{\mathbb{F}_p} W_i^{f_i},
\]
so the assertion follow easily from this.

**Def. (16.3.1.3) [Artin L-Functions].** For a Galois extension of global fields \( L/F \) and \((\rho, V) \in \text{Rep}(\text{Gal}(L/F))\), the Artin L-function of \( \rho \) is defined to be the Euler product
\[
L(F, \rho; s) = \prod_{v \in \Sigma_F} L_v(F, \rho; s).
\]
This L-function also only depends on \( F \) but not \( L \), as we will see in (16.3.1.4).

And also define the completed Artin L-function as the function
\[
\Lambda(F, \rho; s) = \prod_{v \in \Sigma_F} L_v(F, \rho; s).
\]

**Prop. (16.3.1.4) [Functoriality of Artin L-Functions].** For a Galois extension of global fields \( L/F \) and \((\rho, V) \in \text{Rep}(\text{Gal}(L/F))\), The L-functions satisfy the following functorial properties:

- \( L(F, \mathds{1}; s) = \zeta(F; s)(16.2.3.20) \).
- For \( \rho, \rho' \in \text{Rep}(\text{Gal}(L/F)) \), \( L(F, \rho \oplus \rho'; s) = L(F, \rho; s)L(F, \rho'; s) \).
- For Galois extensions \( L'/L/K \) and \( \rho \in \text{Rep}(\text{Gal}(L/F)) \), \( L(L'/F, \rho; s) = L(L/F, \rho; s) \).
- If \( F \subset M \subset L \), \( \rho \in \text{Rep}(\text{Gal}(L/M)) \), then \( L(F, \text{Ind}_{\text{Gal}(L/M)}^{\text{Gal}(L/F)}(\rho); s) = L(M, \rho; s) \).

**Proof:** These follow from (16.3.1.2). \( \square \)

**Cor. (16.3.1.5).** For a finite Galois extension \( L/F \),
\[
\zeta(L; s) = \zeta(F; s) \cdot \left( \prod_{\rho \neq 1 \in \text{Irr}(\text{Gal}(L/F))} L(F, \rho; s)^{\chi_{\rho}(1)} \right)
\]

**Prop. (16.3.1.6) [Artin L-Functions and Weber L-Functions].** For an Abelian extension of global fields \( L/F \) with conductor \( \mathfrak{f} \) and a character \( \chi : \text{Gal}(L/F) \to \mathbb{C}^\times \), composing with the Artin symbols (12.4.5.25), we get a character \( \overline{\chi} : C_F/C_{\mathfrak{f}} \cong \mathbb{J}_{\mathfrak{f}}/P_{\mathfrak{f}} \to \text{Gal}(L/F) \xrightarrow{\overline{\chi}} \mathbb{C}^\times \), which is a Dirichlet character. Then we have
\[
L(F, \chi; s) = \prod_{p \in S} \frac{1}{1 - \chi(\mathfrak{p}/p)(Np)^{-s}} L(F, \overline{\chi}; s)(16.2.3.16),
\]
where \( S = \{ p \in S_f(\mathfrak{f}) | \chi(I_p) = 1 \} \). Moreover, if \( \chi \) is injective, then \( S = \emptyset \).

**Proof:** \( S \) are the primes that are ramified in \( L/F \) and \( \mathbb{C}(\chi)^{I_p} \neq 0 \). \( \square \)
2 Artin Conductors

Def. (16.3.2.1) [Artin Conductors]. Let $L/F$ be a Galois extension of global fields and $(\rho, V) \in \text{Rep}(\text{Gal}(L/F))$, for $v \in \Sigma_F^{\text{fin}}$, let $G_v = G_{v,0} \supset G_{v,1} \supset \ldots \supset G_{v,m} = 0$ be higher ramification groups at $v$, then the Artin conductor of $\rho$ is defined to be the ideal in $O_F$:

$$f(F, \rho) = \prod_{v \in \Sigma_F^{\text{fin}}} p_v^{a_v}, \quad a_v = \sum_{i \geq 0} \dim(V/V^{G_v,i}) \frac{\#G_v,i}{\#G_v,0}.$$  

And we also define the Swan conductor

$$b(F, \rho) = \prod_{v \in \Sigma_F^{\text{fin}}} p_v^{b_v}, \quad b_v = \sum_{i \geq 1} \dim(V/V^{G_v,i}) \frac{\#G_v,i}{\#G_v,0}.$$  

Prop. (16.3.2.2) [Conductor-Discriminant-Formula]. For any Galois extension of global fields $L/F$,

$$b_{L/F} = \prod_{\rho \in \text{Irr}(\text{Gal}(L/F))} f(F, \rho)^{\chi_\rho(1)}.$$  

Proof: Cf.[Neu99]P534. □

3 Functional Equations

Prop. (16.3.3.1) [Functional Equations, Brauer]. By Brauer theorem(15.1.2.33) and(15.1.2.33), the Artin L-functions can be written as products and inverses of Weber L-functions(16.2.3.16) and f.m. L-factors. In particular, they can be extended meromorphically to all $s \in \mathbb{C}$ and satisfies a functional equation(16.2.3.18). But the $\varepsilon$-factor remains mysterious?.

More explicitly, for a Galois extension of global fields $L/F$ and $(\rho, V) \in \text{Rep}(\text{Gal}(L/F))$, the completed Artin L-function satisfies a functional equation

$$\Lambda(F, \rho; s) = \varepsilon(\rho; s)\Lambda(\rho^\vee; 1-s),$$  

where

$$\varepsilon(\rho) = w(\rho) \left( |d_F|^\chi_\rho(1) ||f(F, \rho)|| \right)^{1/2-s} (16.3.2.1)$$  

and $w(\rho)$ is a root number, which satisfies $|w(\rho)| = 1$.

Proof: Cf.[Algebraic Number Theory, Neukirch]. □

Def. (16.3.3.2) [Completed Artin L-Functions]. For a Galois extension of global fields $L/F$, for $\rho \in \text{Rep}(\text{Gal}(L/F))$, the completed L-function is defined to be

Conj. (16.3.3.3) [Artin]. If $F$ is a global field and $(\rho, V) \in \text{Rep}(\text{Gal}_F)$ satisfies $V^{\text{Gal}_F} = 0$, then $L(F, \rho; s)$ is an entire function on $\mathbb{C}$.

Proof: □

Remark (16.3.3.4). The Artin conjecture is true for $\rho$ factoring through a solvable quotient, as we can reduce to Abelian case, and use(16.3.1.6) and(16.2.3.18).

4 Artin-Weil L-Functions

Cf.[On the Functional Equation of the Artin L-Functions, Langlands].
16.4 $p$-adic L-Functions

1 $p$-Adic L-Functions

Main references are [Fontaine’s rings and $p$-adic L-functions, Colmez].

Prop.(16.4.1.1)[Kummer’s Theorem]. Let $a \geq n$ be coprime to $p$ and $k \geq 1$. If $n_1, n_2 \geq k$ that
\[ n_1 \equiv n_2 \mod \varphi(p), \]
then
\[ (1 - a^{n_1})\frac{B_{n_1}}{n_1} \equiv (1 - a^{n_2})\frac{B_{n_2}}{n_2} \mod p^k. \]


Remark(16.4.1.2). This has vast generalizations in Iwasawa theory, Cf.[Iwasawa, On $p$-adic L-functions].

2 Iwasawa Main Conjectures

Thm.(16.4.2.1)[Herbrand]. Let $p \in \mathbf{P}$, $Y = \text{Cl}(Q(\mu_p))[p]$, then $\text{Gal}(Q(\mu_p)/Q) = (Z/(p))^\times$ acts on $Y$ as a $\mathbb{F}_p$-space by conjugation. Let $Y^j$ be the subspace of $Y$ that $(Z/(p))^\times$ acts by character $a \mapsto a^j$. Then for $1 < j < p - 1$ an odd integer, if $Y^j \neq 1$, then the Bernoulli number $B_{p-j}$ has numerator divisible by $p$.

Proof: Cf.[Eisenstein Ideals, Mazur, P52].

3 Iwasawa Main Conjectures for GL(2)

Main references are [the Iwasawa Main Conjectures for GL(2), Skinner, Urban].
16.5 Heegner Points


1 Heegner Points

Def.(16.5.1.1)[Heegner Conditions]. Let $E \in Ell/\mathbb{Q}$ and $F/\mathbb{Q}$ an imaginary quadratic extension with $(d_F, N) = 1$ and associated quadratic character $\eta_F : (\mathbb{Z}/d_F)^\times \to \{\pm 1\}$. Then the Heegner condition is the hypothesis that every prime factor of $N$ splits in $F$.

Prop.(16.5.1.2). In the Heegner situation (16.5.1.1), the sign of functional equation for $E(16.8.1.1)$ $w_E = -1$?, thus rank$_{an}(E/\mathbb{Q})$ is odd and the BSD conjecture (16.8.1.2) predicts rank($E/\mathbb{Q}$) is odd, so at least it has a non-torsion rational point.

Def.(16.5.1.3)[Heegner Points]. In the Heegner situation (16.5.1.1), there exists an ideal $\mathcal{N} \subset \mathcal{O}_F$ of conductor $N$. Then for any $n \in \mathbb{Z}_+$, $\mathcal{O}_n = \mathbb{Z} + n\mathcal{O}_F$ is an order of $\mathcal{O}_F$ of conductor $n$. Thus for $(n, N) = 1$,

$$C/\mathcal{O}_F \to C/(\mathcal{O}_F \cap \mathcal{N})^{-1}$$

is an isogeny of degree $N$, thus defines a point $x_n \in X_0(N)$, by moduli characterization?, called a Heegner point. Then by theory of complex multiplication?, $x_n$ is defined over the ring class field $F_n$ corresponding to the open compact subgroup $(\mathcal{O}_n \otimes \hat{\mathbb{Z}})^\times \subset A^\times_F$.

Proof:

Def.(16.5.1.4)[Heegner Points]. In the Heegner situation (16.5.1.1), using the modular parametrization $\varphi_E : X_0(N) \to E$ over $Q(16.9.1.6)$, $y_n = \varphi_E(x_n) \in E(K_n)$. In particular, define $y_F = \text{tr}_{F_1/F}(y_1) \in E(F)$, called the (principal) Heegner point of $E$.

Prop.(16.5.1.5). The Heegner point $y_F \in E(F)$ is uniquely defined up to sign and torsion.

Proof:

2 Gross-Zagier Formula

Thm.(16.5.2.1)[Gross-Zagier]. In the Heegner situation (16.5.1.1),

$$L'(E/F; 1) = \frac{\int_{\mathbb{C}} \varphi \wedge \overline{\varphi}}{|d_F|^{1/2}} \cdot \frac{1}{c^2} \cdot \langle y_F, y_F \rangle_{NT}$$

Proof:

Cor.(16.5.2.2). If rank$_{an}(E/F) = 1$, then the Heegner point $y_F$ is non-torsion, by (13.5.12.6). And if rank$_{an}(E/F) = 1$, $y_F$ is torsion.
3 Kolyvagin’s Work

Main references are [Kolyvagin’s Work on Modular Elliptic Curves, Gross], [Finiteness of $E(\mathbb{Q})$ and $\text{III}(E/\mathbb{Q})$ for a subclass of Weil curves, Kolyvagin].

Def. (16.5.3.1) [Kolyvagin Primes]. In the Heegner situation (16.5.1.1), let $p \in \mathcal{P}$, a Kolyvagin prime $\ell$ for $E$ is a prime $\ell \in \mathcal{P} \setminus S(Npd_F)$ s.t. $\ell$ is inert in $F$ and $p|\ell + 1, p|a_{\ell,E}$. Equivalently, $\text{Frob}_\ell$ is in the conjugacy class of $c \in \text{Gal}(F(E[p])/F)$?. So by Chebotarev density theorem, the set of Kolyvagin primes has positive Dirichlet density.

For a Kolyvagin prime $\ell$, $M(\ell) = \min\{v_p(\ell + 1), v_p(a_{\ell,E})\}$ is called the Kolyvagin index of $\ell$.

A product of distinct Kolyvagin primes is called a Kolyvagin number for $E$. The set of Kolyvagin numbers is denoted by $\Lambda_E$. For a Kolyvagin number $n$, define the Kolyvagin index of $n$ as $M(n) = \min_{\ell|n}\{M(\ell)\}$.

Prop. (16.5.3.2). In the Heegner situation (16.5.1.1), let $\ell$ be a Kolyvagin prime for $E$, then

$$\text{Gal}(F_\ell/F_1) \cong \text{Pic}(\mathcal{O}_\ell)/\text{Pic}(\mathcal{O}_F) \cong \mathbb{Z}/(\ell + 1) = \langle \sigma \rangle.$$

Proof: \[\square\]

Def. (16.5.3.3) [Kolyvagin Derivative]. In the situation (16.5.3.1), let $\ell$ be a Kolyvagin prime for $E$, define the Kolyvagin derivative $D_\ell = \sum_{i=1}^\ell i\sigma^i \in \mathbb{Z}[\text{Gal}(F_\ell/F_1)]$. Then $(\sigma - 1)D_\ell = \ell + 1 - \text{tr}_\ell$.

Prop. (16.5.3.4). In the situation (16.5.3.1), for $\ell \in \Lambda_E \cap \mathcal{P}$ and Heegner point $y_\ell \in E(F_\ell)$, $D_\ell y_\ell \in E(F_\ell)/p^M E(F_\ell) \subset H^1(F_\ell, E[p^M])$ is invariant under the action of $\text{Gal}(F_\ell/F_1)$.

Thus for any $n \in \Lambda_E$ and $M \leq M(n)$, $D_n y_n \in H^1(F_n, E[p^M])$ is invariant under the action of $\text{Gal}(F_\ell/F_1) \cong \prod_{\ell|n} G_\ell$, thus descends to an element in $H^1(F_1, E[p^M]) \cong H^1(F_n, E[p^M])^{\text{Gal}(F_n/F_1)}$ by Hochschild-Serre spectral sequence (10.1.1.13) and the fact $E[p^M](K_n) = 0$?!?

Proof: By (16.5.3.3), it suffices to show that $(\sigma - 1)D_\ell y_\ell = (\ell + 1 - \text{tr}_\ell)y_\ell \in p^M E(F_1)$: This follows from the definition (16.5.3.1) and the fact $\text{tr}_\ell y_\ell$ is just the Hecke operator action $T_\ell$ on $y_1$, which maps to $a_{\ell y_1} \in E(F_1)$?!?

Def. (16.5.3.5) [Kolyvagin Systems]. In the situation (16.5.3.1), for $n \in \Lambda_E$, define the Kolyvagin cohomology classes

$$c_M(n) = \sum_{s \in \text{Gal}(F_1/F)} sD_n y_n \in H^1(F, E[p^M]), \quad M \leq M(n).$$

The collection of cohomology classes

$$\kappa = \{c_M(n) \in H^1(F, E[p^M])|n \in \Lambda_E, M \in \mathbb{Z}_+, M \leq M(n)\}$$

is called a Kolyvagin system of $E$.

Def. (16.5.3.6) [$p$-Divisibility]. In the situation (16.5.3.1), for $r \in \mathbb{N}$, denote $\Lambda_r$ to be the subset of $\Lambda_E$ consisting of numbers with exactly $r$ prime factors, and define $\mathcal{M}_r \in [0, \infty]$ to be the maximal integer s.t. $p^{\mathcal{M}_r}c_M(n)$ for any $n \in \Lambda_r, M \leq M(n)$.

Prop. (16.5.3.7) [Order of Kolyvagin Systems]. In the situation (16.5.3.1), $\mathcal{M}_0 \geq \mathcal{M}_1 \geq \ldots \geq 0$.

In particular, we can define $\mathcal{M}_\infty = \lim_{r \to \infty} \mathcal{M}_r$. Clearly, $\mathcal{M}_\infty = \infty$ iff $\kappa = 0$. The vanishing order of $\kappa$ is the minimal $r$ s.t. $\mathcal{M}_r \neq \infty$, denoted by $\text{ord } \kappa$. 

1638 CHAPTER 16. L-FUNCTIONS
Proof:

Prop.(16.5.3.8). $\mathcal{M}_0$ is just the $p$-divisibility of the Heegner point $y_F$. In particular, $\mathcal{M}_0 < \infty$ if $y_F$ is non-torsion.

Thm.(16.5.3.9)[Kolyvagin]. Let $\text{ord } \kappa < \infty$, then

- $\text{Sel}^{\infty}(E/F)$ is contained in the subgroup of $H^1(F,E[p^{\infty}])$ generated by $\kappa$.
- $\text{rank}_{p}(E/F)^{\infty}(E/F) = \text{ord } \kappa + 1$, $\text{rank}_{p}(E/F)_{\infty}^{\infty}= \text{ord } \kappa - d$ and $d \in 2\mathbb{N}$.
- Let
  $$\tilde{\Pi}(E/F)[p^{\infty}]^{\text{ord } \kappa +1} = (\oplus_{i \geq 1} \mathbb{Z}/(p^{a_i}))^2, \quad \tilde{\Pi}(E/F)[p^{\infty}]^{\text{ord } \kappa} = (\oplus_{i \geq 1} \mathbb{Z}/(p^{b_i}))^2,$$
  where $(a_i), (b_i)$ is non-increasing, then
  $$a_i = \mathcal{M}_{\text{ord } \kappa + 2i - 1} - \mathcal{M}_{\text{ord } \kappa + 2i}, \quad b_{d+i} = \mathcal{M}_{\text{ord } \kappa + 2i - 2} - \mathcal{M}_{\text{ord } \kappa + 2i - 1}.$$

In particular, $\# \tilde{\Pi}(E/F)[p^{\infty}]^{\text{ord } \kappa +1} \geq p^{\mathcal{M}_{\text{ord } \kappa} - \mathcal{M}_\infty}$, with equality iff $d = 0$.

Proof:

Cor.(16.5.3.10). If $\text{ord } \kappa = 0$, i.e. $y_F$ is non-torsion(16.5.3.8), then $d = 0$, and $r(E/Q) = 1, \# \tilde{\Pi}(E/K) < \infty$.

Kolyvagin’s Conjecture

Conj.(16.5.3.11)[Kolyvagin]. Let $p \in \mathbf{P}\setminus\{2\}$ s.t. $\overline{\rho}_{E,p}$ is surjective, then $\kappa \neq \{0\}$. Equivalently, $\mathcal{M}_\infty < \infty$.

Thm.(16.5.3.12)[Zhang]. Let $E \in \mathcal{E}$ with conductor $N$ and $p \geq 5$ is good ordinary and $\overline{\rho}_{E,p}$ is surjective and ramifies at every prime $\ell \in \mathbf{P}$ s.t. $v_{\ell}(N) = 1$, then $\mathcal{M}_\infty = 0$. In particular, Kolyvagin’s conjecture(16.5.3.11) is true.

Remark(16.5.3.13). There are results that generalize this.

Cor.(16.5.3.14). Under the hypothesis of(16.5.3.12), if $\text{rank}_{p}(E/Q) = 1$, then $r_{\text{an}}(E/Q) = r(E/Q) = 1$, and $\# \tilde{\Pi}(E/Q) < \infty$.

Proof: Cf.[Wei Zhang].

4 p-adic Gross-Zagier Formula

References are [Heegner points and a p-adic Gross-Zagier formula].

5 Waldspurger’s Period Formula

6 Gan-Gross-Prasad Conjecture

7 Kudla’s Program

8 Higher Gross-Zagier over Function Fields, Yun-Zhang

Remark(16.5.8.1). The formula relates arbitrary order central derivative of the base change L-function of an unramified automorphic representation of $PGL(2)$ over a function field to the self-intersection number of a certain algebraic cycle on the moduli stack of Shtukas.
16.6 Gan-Gross-Prasad Conjecture

References are [Wei, More Arithmetic Fundamental Lemma Conjectures: The Case Of Bessel Subgroups].

1 Introduction

The GGP conjecture is a generalization of the the Gross-Zagier formula to higher dimensional varieties. It concerns the central derivative of the L-function and special cycles of Shimura varieties. AGGP conjecture has applications to the Beilinson-Bloch conjecture, which is a generalization of the BSD conjecture.

2 restriction Problems

Conj.(16.6.2.1) [Local Restriction Problems]. Let $K$ be a local field with an involution $\sigma$, $K_0 = K^\sigma$. Let $V \in \text{Vect}/K$ with a non-degenerate sesqui-linear form. Let $G(V)$ be the identity component of the subgroup of $GL(V_{k_0})$ preserving this form.

There are natural non-degenerate subspace $W \subset V$, there will be a subgroup $H \subset G(W) \times G(V)$ containing the diagonally embedded subgroup $G(W)$, and a unitary representation $\nu$ of $H$.

The local restriction problem is to determine for each $\pi \in \text{Irr}(G)$, the number

$$d(\pi) = \dim \text{Hom}_H(\pi|_H \otimes \nu, 1).$$

Def.(16.6.2.2)[Arithmetic Periods]. Let $F$ be a global field and $G$ a reductive group over $F$, $H \subset G$ an algebraic subgroup, $Z = Z(G) \cap H$. Denote $[H] = Z(A_F)H(F)\backslash H(A_F)$. For $\chi \in \tilde{H}(A_F)$, denote the (twisted) automorphic L-period map:

$$l_{H,\chi} : \mathcal{A}_0(G/F) \to \mathbb{C} : \varphi \mapsto \int_{[H]} \chi(h)\varphi(h)dh.$$ (Convergence).

3 Statements

References are [Symplectic Local Root Numbers, Central Critical L-Values, And Restriction Problems In The Representation Theory Of Classical Groups, Gan-Gross-Prasad].

Conj.(16.6.3.1).

4 Arithmetic Fundamental Lemma

Jacquet–Rallis proposed an approach using relative trace formula to attack the unitary case of Gan–Gross–Prasad conjecture. The fundamental lemma is proved by Yun.

Later Wei Zhang proposed an analogous approach using the arithmetic fundamental lemma, equality between certain intersection numbers and the first derivatives of some relative orbital integrals, and is not proved yet.
16.7 Colmez Conjecture

References are [On Faltings heights of abelian varieties with complex multiplication, Xinyi Yuan].

1 Averaged Colmez Conjecture
16.8 BSD Conjecture

References are [Lectures on the Conjecture of Birch and Swinnerton-Dyer, Gross], [Sil99], 

1 Statements

Elliptic Curves

Thm.(16.8.1.1) [Analytic Continuation]. Let $E$ be an elliptic curve over a global field $K$, the $L$-function $L(E, s)$ defined as in(16.1.5.2) has an analytic continuation an entire function on $s \in \mathbb{C}$, and satisfies a functional equation relating its value at $s$ and $2 - s$.

If $K = \mathbb{Q}$ and the zeta function $Z(E, s) = N_{E/Q}^{s/2}(2\pi)^{-s}\Gamma(s)L(E, s)$, where $N_{E/Q}$ is the conductor, the functional equation writes:

$$Z(E, s) = w_E Z(E, 2 - s)$$

where $w_E = \pm 1$ is called the **sign of functional equation of $E$**.

**Proof:** This is a consequence of the Breuil-Conrad-Diamond-Taylor theorem(16.9.1.6), Cf.[Introduction to the Theory of Automorphic Forms, Shimura]. \hfill \Box

Conj.(16.8.1.2)[Birch-S.Dyer]. Let $K$ be a number field, $E \in \text{Ell} / K$, let $L(E, s)$ be the L-function of $E(16.1.5.2)$, then

- $\#\text{III}(E) < \infty$, $\text{rank}(E/K) = \text{rank}_{\text{an}}(E/K) = r$, and

$$L^{(r)}(E, s) = \frac{2^{r_2}\Omega(\prod_{v \in \Sigma_K^0} c_v)\prod_{v \in \Sigma_K^\infty} |\omega/\omega_{E,v}|_v}{\sqrt{|d_K|}} \cdot \#\text{III}(E/K) \cdot \frac{\text{Reg}(E/K)}{(#E(K)_{\text{tor}})^2},$$

where

- $r_2$ is the number of complex places of $K$,
- $\text{Reg}(E/K)$ the regulator of $E(K)/E(K)_{\text{tor}}$ w.r.t the Neron-Tate height pairing on $E(K)(13.5.12.8)$,
- $c_v$ the local Tamagawa numbers,
- $\omega$ a non-zero global exterior differential form,
- $\Omega = \prod_{v \in \Sigma_K^\infty} \int_{E(K_v)} |\omega|_v$,
- $\omega_{E,v}$ is a Néron differential on $E_v$.

**Proof:** \hfill \Box

Conj.(16.8.1.3)[$p$-Parts of the Birch-S.Dyer Conjecture].

Prop.(16.8.1.4)[Nekovar]. The parity conjecture holds for elliptic curves over a totally real number field $K$ if $\text{III}(E/K)$ is finite.

**Proof:** \hfill \Box
Abelian Varieties

Conj. (16.8.1.5) [Functional Equation Conjecture]. Let $F$ be a number field, $A \in \text{AbVar}^g/F$, then

- the zeta function $Z(A, s)$ extends to an entire function on $s \in \mathbb{C}$, and satisfies the functional equation
  \[ Z(A, s) = w_A Z(A, 2 - s), \]
  where $w_A = \pm 1$ is called the sign of functional equation of $A$, and
- $w_A = w = \prod_{v \in \Sigma_F} w_v$, where $w_v$ is the local root number of $A/K$ at $v$.

Proof: □

Conj. (16.8.1.6) [Birch-S.Dyer-Tate]. Let $F \in \mathbb{NField}, A \in \text{AbVar}^g/K$, let $L(A, s)$ be the $L$-function of $A(16.1.5.2)$, then

- $L(A, s)$ extends to an entire function on $s \in \mathbb{C}$, #\text{III}(A) < \infty, \text{rank}(A/F) = \text{rank}_{an}(A/F) = r$,
- \[
\frac{L^{(r)}(A, s)}{r!} = \frac{2^{gr} \Omega_A \left( \prod_{v \in \Sigma_F} c_v \right) \left( \prod_{v \in \Sigma_K} |\omega/\omega_{A,v}|_v \right)}{\sqrt{|d_K|}} \cdot \text{#III}(A/K) \cdot \frac{\text{Reg}(A/K)}{\#(A)_{tor} \#(A(K))_{tor}},
\]
  where
  - $r_2$ is the number of complex places of $F$,
  - $\text{Reg}(A/F)$ the regulator of the Neron-Tate height pairing $A(K)/A(K)_{tor} \times \hat{A}(K)/\hat{A}(K)_{tor} \to \mathbb{R}(13.5.12.8)$,
  - $c_v$ the local Tamagawa numbers,
  - $\omega$ a non-zero global $g$-form,
  - $\Omega_A = \prod_{v \in \Sigma_F} \int_{A(F_v)} |\omega|_v$,
  - $\omega_{A,v}$ is a Néron differential on $A_v$.

Proof: □

Remark (16.8.1.7).
- The BSDT conjecture has been verified numerically for some elliptic curves over number fields, some Jacobians of genus 2 curves and (up to square) a few Jacobians of higher genus curves.
- BSDT conjecture implies BSD conjecture (16.8.1.2), as any $E \in \text{Ell}/K$ is an Abelian variety of dimension 1, and $E \cong \hat{E}$ canonically.

Prop. (16.8.1.8). If the BSDT conjecture holds for all Abelian varieties over $\mathbb{Q}$, then it holds for all Abelian varieties over any number fields.

Proof: Cf.[The Arithmetic of Abelian Varieties, Milne]. □

Conj. (16.8.1.9) [Parity Conjecture]. Let $K$ be a number field and $A \in \text{AbVar}/K$, then $\text{rank}_{an}(A/K) \equiv \text{rank}(A/K) \mod 2$. This is a consequence of BSDT conjecture (16.8.1.6).
2 Low Rank Cases


We use notations in 11.

Thm. (16.8.2.1) [Rank 0 Case]. For $E \in \mathcal{E}_{\ell}/\mathbb{Q}$ and $\ell \in \mathcal{P}$, there are implications:

- $\operatorname{rank}(E/\mathbb{Q}) = 0$, $\#\mathbb{I}^\mathcal{I}[\ell^\infty] < \infty \Rightarrow \operatorname{rank}_\ell(E/\mathbb{Q}) = 0$.
- $\operatorname{rank}_{\text{an}} (E/\mathbb{Q}) = 0 \Rightarrow \operatorname{rank}(E/\mathbb{Q}) = 0$, $\#\mathbb{I}^\mathcal{I}[\ell^\infty] < \infty$.
- $\operatorname{rank}_\ell(E/\mathbb{Q}) = 0 \Rightarrow \operatorname{rank}_{\text{an}}(E/\mathbb{Q}) = 0$ if $\ell \geq 3$ is good ordinary for $E$ and $\overline{\rho}_{E,\ell}: \text{Gal}_\mathbb{Q} \rightarrow \text{Aut}(E[\ell])$ surjective.

Proof: 1 is trivial.

2 is the work of Gross-Zagier and Kolyvagin.

3 is the work of Skinner-Urban (2000s).

Prop. (16.8.2.2). If $\operatorname{rank}_{\text{an}}(E/\mathbb{Q}) = 0$, the $p$-part of the BSD formula (16.8.1.3) is known for $p \geq 3$ under similar hypotheses by work of Kato (2000s) and Skinner-Urban on the Iwasawa main conjecture for elliptic curves.

Rank 1 Case

References are [Weil Zhang, Selmer groups and the divisibility of Heegner points (2013)] and [the Birch and Swinnerton-Dyer Formula for Elliptic Curves of Analytic Rank One].

Thm. (16.8.2.3) [Rank 1 Case]. For $E \in \mathcal{E}_{\ell}/\mathbb{Q}$ and $\ell \in \mathcal{P}$, there are implications:

- $\operatorname{rank}(E/\mathbb{Q}) = 1$, $\#\mathbb{I}^\mathcal{I}[\ell^\infty] < \infty \Rightarrow \operatorname{rank}_\ell(E/\mathbb{Q}) = 1$.
- $\operatorname{rank}_{\text{an}} (E/\mathbb{Q}) = 1 \Rightarrow \operatorname{rank}(E/\mathbb{Q}) = 1$, $\#\mathbb{I}^\mathcal{I}[\ell^\infty] < \infty$.
- $\operatorname{rank}_\ell(E/\mathbb{Q}) = 1 \Rightarrow \operatorname{rank}_{\text{an}}(E/\mathbb{Q}) = 1$ if $\ell \geq 5$ is good ordinary for $E$ and $\overline{\rho}_{E,\ell}: \text{Gal}_\mathbb{Q} \rightarrow \text{Aut}(E[\ell])$ surjective with some mild ramification conditions.

Proof: 1 is trivial.

2 is the work of Gross-Zagier (16.5.2.2) and Kolyvagin (16.5.3.10).

3 follows from (16.5.3.14).

Cor. (16.8.2.4). As a corollary of (16.8.2.1) and (16.8.2.3), [Bhargava-Skinner-Zhang] proved that at least 66% of Elliptic curves over $\mathbb{Q}$ satisfy the rank part of the BSD conjecture (16.8.1.2)?

Prop. (16.8.2.5). Under the hypothesis of (16.5.3.12), if $\operatorname{rank}_p(E/\mathbb{Q}) = 1$, then the $p$-part of the

Prop. (16.8.2.6). If $E \in \mathcal{E}_{\ell}/\mathbb{Q}$ with conductor $N$ satisfies $\operatorname{rank}_{\text{an}}(E/\mathbb{Q}) = 1$, $p \in \mathcal{P}\setminus\{2, 3\}$ and $\rho_{E,p}$ is surjective and ramifies at any $\ell \in \mathcal{P}$ s.t. $v_\ell(N) = 1$, then the $p$-part of the BSD formula (16.8.1.3) holds.

3 over Function Fields

**Prop. (16.8.3.1)**[Artin-Tate]. The BSD conjecture hold for an elliptic curve over a function field $F$ iff $\text{III}(E/F)$ is finite.

*Proof:* □

4 Motivic BSD Conjectures

**Prop. (16.8.4.1)**[Motivic BSD conjectures]. For $E \in \text{Ell}/\mathbb{Q}$, consider the motive $h^1(E)$, then

$$L(E, s) = Z(h^1(E), s).$$

More generally, if we consider $L$-functions of the form

$$L_3(E, s) = \prod_p L(E_{F_p^3}, s).$$

Then there exists a motive $M \in M_{\text{num}}(\mathbb{Q})$ s.t.

$$h^1(E) \otimes h^1(E) \otimes h^1(E) = 3h^1E(-1) \oplus M,$$

and

$$L_3(E, s) = Z(M, s).$$

*Proof:* □
16.9 Shimura-Taniyama-Weil Conjecture

References are [Ring-theoretic properties of certain Hecke algebras, Taylor-Wiles], http://virtualmath1.stanford.edu/~conrad/modseminar/.

1 Modularity

Thm. (16.9.1.1) [Eichler-Shimura]. If \( f \in S_2(\Gamma_0(N)) \) be a Hecke eigenform with integral coefficients, then there exists an elliptic curve \( E/\mathbb{Q} \) s.t. \( L(E,s) = L(f,s) \).

Proof: □

Def. (16.9.1.2) [Modular Elliptic Curves]. Let \( E \in \mathbb{Ell}/\mathbb{Q} \), then \( E \) is called a modular elliptic curve if there exists a normalized Hecke eigenform \( f \) with integral coefficients s.t. \( L(E,s) = L(f,s) \).

E is called a modular elliptic curve if for some odd prime \( \ell \in P \setminus 2 \), the representation of \( \text{Gal}_{\mathbb{Q}} \) on \( T_\ell \) is isomorphic to \( \rho_{f,\lambda} \) for some \( f \in S_2(\Gamma_0(N)) \).

E is called a modular elliptic curve if there is a non-constant map \( X_0(N) \to E \) over \( \mathbb{Q} \) for some \( N \in \mathbb{Z}_+ \).

Lemma (16.9.1.3). For \( E \in \mathbb{Ell}/\mathbb{Q} \) and \( N \in \mathbb{Z}_+ \), there is a surjection \( X_0(N) \to E \) iff there is a surjection \( J_0(N) \to E \).

Proof: If \( \varphi : X_0(N) \to E \) is non-zero, then \( \varphi_* : J_0(N) \to \text{Jac}(E) \cong E \) is nonzero, by (13.5.13.9). If \( \Phi : J_0(N) \to E \) is surjective, then \( X_0(N) \xrightarrow{\text{Abel}} J_0(N) \to E \) is also surjective, by looking at the Tate module.

Lemma (16.9.1.4) [Langland-Tunnell]. If \( E \in \mathbb{Ell}/\mathbb{Q} \) is semistable and \( E[\ell] \) is irreducible for some odd prime \( \ell \), then \( E[\ell] \) is modular.

Lemma (16.9.1.5) [Taylor-Wiles]. If \( E \in \mathbb{Ell}/\mathbb{Q} \) is semistable and \( \ell \) is an odd prime s.t. \( E[\ell] \) is irreducible and modular, then \( T_\ell \) is modular.

Proof: □

Thm. (16.9.1.6) [Taylor-Wiles/Breuil-Conrad-Diamond-Taylor]. The modularity conjecture (16.9.1.2) is true for any \( E \in \mathbb{Ell}/\mathbb{Q} \).

Proof: □

Prop. (16.9.1.7). For any elliptic curve \( E \) over \( \mathbb{Q} \), there exists some \( N > 0 \) and a surjective morphism \( X_0(N) \to E \) over \( \mathbb{Q} \).

Proof: Cf.[On the modularity of elliptic curves over \( \mathbb{Q} \): wild 3-adic exercises, C. Breuil, B. Conrad, F. Diamond, and R. Taylor]. □

Cor. (16.9.1.8). Let \( a, b, c \in \mathbb{Q} \) be distinct, then the elliptic curve \( E \in \mathbb{Ell}/\mathbb{Q} \) defined by

\[
y^2 = (x-a)(x-b)(x-c)
\]

is modular.

Prop. (16.9.1.9). Let \( a, b, c \in \mathbb{Q} \) be distinct, then the elliptic curve \( E \in \mathbb{Ell}/\mathbb{Q} \) defined by

\[
y^2 = (x-a)(x-b)(x-c)
\]

has a
2 L-Functions

Conj. (16.9.2.1) [Shimura-Taniyama]. For any \( E \in \mathcal{E} \setminus / \mathbb{Q} \), \( L(E,s) = L(f_E,s) \) for some normalized eigenform \( f_E \in S_2(\Gamma_0(N)) \), where \( N \) is the conductor of \( E \).

Prop. (16.9.2.2) [Elliptic Curves and Modular Forms]. Let \( E \) be an elliptic curve over \( \mathbb{Q} \) of conductor \( N \) and sign of functional equation \( w_E \), and has L-function \( L(E,s) = \sum c_n n^{-s} \). Let \( f_E(\tau) = \sum c_n e^{2\pi i n \tau} \) be the Mellin transform of \( L(E,s) \), then
- \( f_E \) is a cuspidal modular form on \( S_k(\Gamma_0(N)) \).
- \( f_E \) is a normalized Hecke eigenfunction, and satisfies \( f(-1/N\tau) = w_E f(\tau) \).
- Let \( \omega \) be an invariant differential form on \( E \), then there exists a finite morphism \( \varphi : X_0(N) \to E \) over \( \mathbb{Q} \) s.t. \( \varphi^*(\omega) \) is a multiple of the differential form on \( X_0(N) \) represented by \( f(\tau) d\tau \).

Proof: \( \square \)

Def. (16.9.2.3) [Manin Constant]. Let \( E \in \mathcal{E} \setminus / \mathbb{Q} \) and \( \omega \in K_{E/\mathbb{Q}} \), the Manin constant is defined to be the constant \( c \in \mathbb{C} \) s.t. \( f^* \omega = c \cdot 2\pi i f_E dz \).

3 Fermat’s Last Theorem

Def. (16.9.3.1) [Frey’s Curve]. Let \( a, b, c \in \mathbb{Z} \) satisfy \( a^n + b^n = c^n, n \geq 2, abc \neq 0 \), the Frey curve for \( a, b, c \) is the elliptic curve define by
\[
E_{a,b,c} : y^2 = x(x+a^n)(x-b^n).
\]
The discriminant of this Weierstrass equation is \( \Delta_{a,b,c} = 16a^{2n}b^{2n}(a^n+b^n)^2 = 16(abc)^{2n} \). The minimal discriminant of a Frey’s curve \( E_{a,b,c} \) satisfies \( \Delta_{a,b,c}^{\min} \geq \frac{|abc|^{2n}}{2^8} \) by (13.8.4.25).

Thm. (16.9.3.2) [Fermat’s Last Theorem, Ribet/Wiles-Taylor]. If \( l \geq 5 \), then there are no integral solution to the equation \( a^l + b^l = c^l \).

Proof:

Step 1 : Frey’s Curve : \( y^2 = x(x-a^l)(x+b^l) \). It defines an elliptic curve, has semistable reduction with discriminant \( \Delta = 16(abc)^l \).

The Galois representation : \( \rho_{E,l} : \text{Gal}(\mathbb{Q}) \to \text{Aut}(E[l]) \cong GL(2, \mathbb{F}_l) \) is unramified.

Step 2: Taniyama-Shimura-Weil Conjecture: \( E \) is associated with a cuspidal modular eigenform \( f_E(q) = \sum a_n q^n, a_n \in \mathbb{Q} \) of level \( \Gamma_0(N) \) and weight 2.

This is defined by \( a_1 = 1 \), and \( a_p = p + 1 - [E(\mathbb{F}_p)] \) for \( p \) not divisible by \( N \).

By Eichler-Shimura, weight 2 cusp eigenform over \( \mathbb{Q} \) can always associated to a Galois representation \( \rho_f : G(\mathbb{Q}) \to GL_2(\mathbb{Q}_l) \), Weil did the converse.

Step 3: Serre+Ribet’s Level-Lowering: there should be a cuspidal modular eigenform \( f' \) of level \( \Gamma_0(2) \) and weight 2. s.t. \( a_n(f') \equiv a_n(f) \mod l, \forall (n,N) = 1 \).
Step 4: But there is no cuspidal form of level $\Gamma_0(2)$ and weight $2$, because there $X_0(2) = \mathbb{P}^1$, and $H^0(\mathbb{P}^1, \Omega^1_{\mathbb{P}^1}) = 0$. \hfill \Box

Prop. (16.9.3.3) [Szpiro’s Conjecture and Fermat’s Last Theorem]. The Szpiro’s conjecture (13.5.10.12) implies Fermat’s last theorem for sufficiently large $n$(depending on the effectiveness of Szpiro’s conjecture).

Proof: Let $a, b, c \in \mathbb{Z}$ satisfy $a^n + b^n = c^n$, $n \geq 2, abc \neq 0$, the conductor $N_{a,b,c}$ of the Frey’s curve (16.9.3.1) $E_{a,b,c}$ satisfies $N_{a,b,c} \leq 2^8(abc)$ by (13.8.4.25). Szpiro’s conjecture implies

$$\frac{|abc|^{2n}}{2^8} \leq |\Delta_{a,b,c}^{\min}| \leq \kappa_1 N_E^7 \leq 2^{56}\kappa_1 |abc|^7,$$

so $|abc|^{2n-7} \leq 2^{64}\kappa$. As $|abc| \geq 2$, this gives an upper bound for $n$. \hfill \Box

Prop. (16.9.3.4) [Modular Lifting Theorem]. The main tool.

Prop. (16.9.3.5) [Weil’s Theorem], modular deformation ring $T$ is isomorphic to the Galois deformation ring $R_T$. 

16.10 Special Values of L-Functions

1 Deligne Conjecture

Main references are [Del79], [Conrad BSD notes], [Remarks on special values of L-functions, Scholl].

Conj.(16.10.1.1) [Deligne-Beilinson-Scholl]. Let $L(s)$ be a motivic L-function, $m \in \mathbb{Z}$, $r = \text{ord}_{s=m} L(s)$, then $L^{(r)}(m) \in \hat{\mathbb{P}}$.

Proof: □

2 Beilinson-Bloch Conjecture

References are [Blo00], [Beilinsen, Higher regulators of modular curves, Applications of algebraic $K$-theory to algebraic geometry and number theory, Part I, II], [Iwasawa theory for the symmetric square of an elliptic curve], [Beilinson’s Conjecture, in Motives, 537-570], [Algebraic K-Theory and Special Values of L-Functions: Beilinson’s Conjecture]

Regulator Maps

Def.(16.10.2.1)[Polylogarithm]. For $s \in \mathbb{Z}_+$, the power series

$$\text{Li}_s(z) = \sum_{n \geq 1} \frac{z^n}{n^s}$$

converges absolutely for $|z| < 1$ and can be analytically continued to a multi-valued function on $\mathbb{C}\setminus\{1\}$, called the Polylogarithm function.

Proof: In fact, $\text{Li}_1(z) = -\log(1-z)$, and $\text{Li}_{s+1}(z) = \int_0^z \text{Li}_s(t) \frac{dt}{t}$. □

Def.(16.10.2.2)[Bloch-Wigner Dilogarithm]. The function

$$D(z) = \text{Im} \left( \text{Li}_2(z) + \log|z| \log(1-z) \right), \quad z \in \mathbb{C}(16.10.2.1)$$

is a real-valued function on $\mathbb{C}$, called the Bloch-Wigner dilogarithm.

Proof: Cf.[Blo00]P44. □

$A^1$ Case

Conj.(16.10.2.3)[Bloch Conjecture for Fields]. For a number field $F$, mapping the higher K-groups $K_{2i-1}(F)$ to a lattice with covolume $\zeta_F(m)$ via higher regulator maps. And the regular maps are made from $m$-th polylogarithm functions(16.10.2.1), so $\zeta_F(m)$ can be expressed by combinations of $m$-th polylogarithm functions of elements in $F$.

For example:

$$\zeta_{\mathbb{Q}(\sqrt{5})}(3) = \frac{24}{25\sqrt{5}} \text{Li}_3(1)[\text{Li}_3(\alpha) + \text{Li}_3(-\alpha) + \frac{1}{2}(\log(\alpha))^3 - \frac{\pi^2}{6} \log(\alpha)], \alpha = \frac{\sqrt{5} - 1}{2}.$$

This makes the numerical calculation of higher K-groups possible.

Proof: □

Remark(16.10.2.4). $m = 2$ case is proved by Bloch-Suslin-Merkuriev, $m = 3$ case is proved by Goncharov.
Elliptic Curve Case

Def. (16.10.2.5) [Elliptic Dilogarithm]. Let $E \in \mathcal{E}_{/ \mathbb{C}}$ with complex parametrization $\mathbb{C}^\times / \mathbb{Q}^\times$, define the elliptic dilogarithm:

$$D_q : \mathbb{C}^\times / \mathbb{Q}^\times \to \mathbb{R} : z \mapsto \sum_{n \in \mathbb{Z}} D(q^n z)(16.10.2.2).$$

And it extends linearly to a map $Z_1(E) \to \mathbb{R}$.

Prop. (16.10.2.6) [Bloch]. Let $E \in \mathcal{E}_{/ \mathbb{C}}$, define

$$F : R(E)\times \otimes R(E)\times \to \mathbb{R} : f \otimes g \mapsto D_q(\sum m_i n_j [b_j - a_i]),$$

where $f, g \in R(E)^\times$ with divisor $(f) = \sum m_i a_i, (g) = \sum n_j b_j$. Then $F$ is additive, and

$$D(f \otimes (1 - f)) = 0.$$

In particular, $F$ factors through $R(E)^\times \otimes R(E)^\times / \{f \otimes (1 - f)\} = K_2(R(E))$.

Thus, there is a composition $r_E : K_2(E) \to K_2(R(E)) \to \mathbb{R}$, called the (higher) regulator map.

Thm. (16.10.2.7) [Beilinson-Bloch]. Let $E \in \mathcal{E}_{/ \mathbb{Q}}$ with complex parametrization $E(\mathbb{C}) \cong \mathbb{C}^\times / \mathbb{Q}^\times$, then there exists a Gal$_\mathbb{Q}$-invariant divisor $P$ on $E$ s.t. $D_q(P) \sim_{\mathbb{Q}^\times} L(E, 2)/\pi(16.10.2.5)$.

Proof: Cf.[Beilinson, Higher regulators of modular curves].

3 Bloch-Kato Conjecture

4 Height Pairings
16.11 Riemann Conjecture

1 Hilbert-Pólya Conjecture

References are [Rudnick-Sarnak, Zeros of Principal $L$-functions and Random Matrix Theory], [Trace formula in noncommutative geometry and the zeros of the Riemann zeta function].
17  Arakelov Geometry

17.1  Arithmetic Intersection Theory

1  Arithmetic Riemann-Roch
17.2 Arakelov Geometry

1 Metrized Line Bundles

Def. (17.2.1.1)[Metrized Line Bundles]. Let $F$ be a number field, a metrized line bundle $(\mathcal{L}, |\cdot|)$ is a line bundle on $\mathcal{O}_F$ together with norms $|| \cdot ||_v$ on the free $F_v$-module $M \otimes_R F_v$ of rank 1 for $v \in \Sigma_F^\infty$.

Def. (17.2.1.2)[Heights and Degree of Metrized Line Bundles]. Let $F$ be a number field and $(\mathcal{L}, |\cdot|)$ be a metrized line bundle on $\mathcal{O}_F(17.2.1.1)$, for each $v \in \Sigma_F^0$, $\mathcal{L}_v = \mathcal{O}_{F,v} m_v$ for some $m_v \in \mathcal{L}_v$, so we define $||m||_v = |m/m_v|_v$ for $m \in \mathcal{L}_v$, and define the height of $\mathcal{L}$ to be

$$H((\mathcal{L}, |\cdot|)) = \prod_{v \in \Sigma_F} ||m||_v^{-1}, \quad m \neq 0 \in M$$

which is independent of $m$ by product formula. Also we define

$$h(M) = \frac{1}{[F:Q]} \log H(M),$$

called the degree of $\mathcal{L}$. $h((\mathcal{L}, |\cdot|))$ is invariant under change of number fields.
18 | Theoretical Physics

18.1 Quantum Mechanics

Basic References are [Nap].

1 Basics

Axiom (18.1.1.1) [Axioms for Quantum Mechanics]. The Schrödinger equation can be derived from the Dirac-von Neumann axioms:

- The states of particles is a countable dimensional Hilbert space, and
- The observables of a quantum system are defined to be the (possibly unbounded) Hermitian operators $A$ on $\mathbb{H}$. Then any continuous observable is unitarily diagonalizable, with real eigenvalues by Hilbert-Schimidt (10.8.4.16).
- The state $\varphi$ of the quantum system is a unit vector of $\mathbb{H}$, up to scalar multiples.
- The expectation value of an observable $A$ for a system in a state $\varphi$ is given by the inner product $\langle \varphi, A\varphi \rangle$.
- (Unitarity) The time evolution of a quantum state according to the Schrödinger equation is mathematically represented by a unitary operator $U(t)$ (depends only on the state an relative time) (one-parameter subgroup).

Now that $\varphi(t) = \hat{U}(t)\varphi(t_0)$, so $\hat{U}(t)\varphi(t_0) = e^{-i\hat{H}t}$, $\hat{H}$ hermitian.

So now take derivative w.r.t $t$, we get $i\frac{d\varphi}{dt} = \hat{H}\varphi$. By quantum correspondence principle, it is possible to derive the expression of $\hat{H}$ by classical methods.

Def. (18.1.1.2) [Qubits]. A qubit is a state that is complex combination of 0 and 1, i.e. $|\varphi\rangle = \alpha|0\rangle + \beta|1\rangle$. Notice I very dislike the 'bra-ket’ notation, I prefer to think of state just as an element in the Hilbert space, and use any notation I like.

Def. (18.1.1.3) [Pauli Observables]. The observables on a two dimensional Hilbert space, i.e. a qubit state space, are all combinations of Pauli Observables or Pauli matrixes plus $I$:

$$\sigma_z = \begin{bmatrix} 1 & 0 \\ 0 & -1 \end{bmatrix}, \quad \sigma_x = \begin{bmatrix} 0 & 1 \\ 1 & 0 \end{bmatrix}, \quad \sigma_y = \begin{bmatrix} 0 & -i \\ i & 0 \end{bmatrix}$$

Their corresponding eigenvalues are denoted by

$$\uparrow = \begin{bmatrix} 1 \\ 0 \end{bmatrix}, \quad \downarrow = \begin{bmatrix} 0 \\ 1 \end{bmatrix}, \quad \rightarrow = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ 1 \end{bmatrix}, \quad \leftarrow = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -1 \end{bmatrix}, \quad \otimes = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ i \end{bmatrix}, \quad \odot = \frac{1}{\sqrt{2}} \begin{bmatrix} 1 \\ -i \end{bmatrix}$$
Remark (18.1.1.4). The solution of a Schrödinger equation for a non-Relativistic particle is assumed to be a Schwartz function (Vanish fast enough at infinity). The coefficients are assumed smooth enough to guarantee at least uniqueness and existence locally.

Prop. (18.1.1.5). The wave function on the \((p, t)\) coordinates is the Fourier Transform of the wave function on the \((x, t)\) coordinates, because the eigenstate of the \(p\)-operator \(i\hbar \frac{\partial}{\partial x}\) is \(e^{ikx}\), the coefficients of which is the value (probability) of the wave function of the \((p, t)\) coordinates.

Prop. (18.1.1.6) [Schrödinger Uncertainty Principle]. Set \(\sigma_A = \sqrt{\langle \hat{A}^2 \rangle - \langle \hat{A} \rangle^2}\), then:
\[
\sigma_A^2 \sigma_B^2 \geq \left| \frac{1}{2} \langle \hat{A} \hat{B} + \hat{B} \hat{A} \rangle - \langle \hat{A} \rangle \langle \hat{B} \rangle \right|^2 + \left| \frac{1}{2i} \langle [\hat{A}, \hat{B}] \rangle \right|^2.
\]
Proof: Derived from definition and Schwarz inequality, Cf. [Wiki]. □

Cor. (18.1.1.7) [Heisenberg Uncertainty Principle]. \(\sigma_x \sigma_p \geq \frac{\hbar}{2}\).
Proof:
\[
[x, i\hbar \frac{\partial}{\partial x}] = i\hbar.
\] □

Prop. (18.1.1.8) [Spectral Decomposition]. In Quantum physics, one need to use spectral decomposition of the Hamiltonian operator. But at most cases, there are only countably many eigenstate and the eigenvalue has a lower bound and tends to infinity. In this case, \((\hat{H} + A)^{-1}\) is a compact operator thus by spectral theorem (10.8.4.15) the eigenstate of \(\hat{H}\) forms a set of complete basis.

Prop. (18.1.1.9) [No-Cloning Theorem].

Calculations

Prop. (18.1.1.10) [Virial Theorem]. For a system that \(V(r) \sim r^n\), the average kinetic energy and the average potential energy has the relation:
\[
2\langle T \rangle = n \langle V \rangle.
\]

Spin

2 Quantum Computations

Classical Logic Gates

Def. (18.1.2.1) [Boolean Functions]. A Boolean function is a function \(f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2\).

Def. (18.1.2.2) [Classical Logic Gates]. There are four classical logic gates, if we let \(0, 1 \in \mathbb{F}_2\), then:
- AND gate: \((a, b) \mapsto ab\).
- OR gate: \((a, b) \mapsto ab + a + b\).
- NOT gate: \(a \mapsto a + 1\).
- COPY gate: \(a \mapsto (a, a)\).

Def. (18.1.2.3) [Reversible Gates]. A gate is called reversible iff it is a bijection from \(\mathbb{F}_2^n\) to \(\mathbb{F}_2^n\).
**Def. (18.1.2.4) [Stimulation]**. A set of gates is said to be able to **stimulate** a boolean function \( f \) iff there is a composition of these gates that maps:

\[
(x_1, \ldots, x_{m+n}) \mapsto (g_1(x_1, \ldots, x_{m+n}), \ldots, g_k(x_1, \ldots, x_{m+n}))
\]

that if we let \( x_{i_1} = a_1, x_{i_2} = a_2, \ldots, x_{i_m} = a_m \) be fixed, where \( \{0, 1 \ldots, m + n\} - \{i_1, \ldots, i_m\} = \{j_1, \ldots, j_n\} \) (in some order), then \( g_1(x_1, \ldots, x_{m+n}) = f(x_{j_1}, \ldots, x_{j_n}) \).

A set of gates is called **universal** iff they can stimulate all Boolean function \( f : \mathbb{F}_2^n \mapsto \mathbb{F}_2 \).

**Prop. (18.1.2.5) [Classical Gates Universal]**. The four classical gates are universal. In fact, \( \text{AND}(x, y) = \text{OR}(\text{NOT}(x), \text{NOT}(y)) \), so even AND is disposable, and COPY is not used as well.

*Proof:* Just use OR gate to juxtapose all possible combinations that are mapped to 1. \( \square \)

**Def. (18.1.2.6) [Examples of Reversible Gates].**

- The **CNOT gate** is defined to be \( \text{CNOT} : (a, b) \mapsto (a, a + b) \).
- The **Toffoli gate** is defined to be \( \text{CCNOT} : (a, b, c) \mapsto (a, b, c + ab) \).

**Prop. (18.1.2.7).** CNOT gate cannot stimulate AND. In particular, CNOT is not universal.

*Proof:* It can be shown that any Boolean function that can be stimulated by CNOT gate is of the form \( (x_1, \ldots, x_n) \mapsto \sum a_i x_i + b \). But AND is of the form \( (a, b) \mapsto ab \), which is not of the form, so it is not stimulated by CNOT. \( \square \)

**Prop. (18.1.2.8).** Toffoli gate is universal.

*Proof:* It suffices to show it can stimulate AND and NOT, then it can stimulate OR because \( \text{OR}(x, y) = \text{NOT}(\text{NOT}(x), \text{NOT}(y)) \).

AND is outputted in the third bit with \( c = 0, a = x, b = y \), NOT is outputted in the third bit with \( a = 1 = c, b = x \). \( \square \)

**Quantum Logic Gates**

**Def. (18.1.2.9) [Quantum Logic Gates].** A **quantum logic gate** is a unitary matrix. So a quantum logic gate is always reversible.

**Prop. (18.1.2.10) [Examples of Quantum Gates].**

- The **Hadamard gate** \( H \) is a rotation on one single qubit given by the matrix

\[
\begin{bmatrix}
\frac{1}{\sqrt{2}} & \frac{1}{\sqrt{2}} \\
\frac{1}{\sqrt{2}} & -\frac{1}{\sqrt{2}}
\end{bmatrix}
\]

- If a classical gate is reversible and its matrix is unitary, then the same matrix will give out a quantum gate with all entries 0 and 1, called the **quantization** of the classical gate.
- The **Fredkin gate** or CSWAP gate is a three-bit gate defined as the quantization of the gate given by:

\( (a, b, c) \mapsto (a, a(b + c) + b, a(b + c) + c) \).
3 Quantum Algorithms

Deutsch-Jozsa Algorithm

Prop. (18.1.3.1) [Deutsch-Jozsa Algorithm]. The Deutsch-Jozsa problem is that: given a function \( f : \mathbb{F}_2^n \rightarrow \mathbb{F}_2 \), which is either a constant function or a function that takes half value 0 and half value 1, If we have a box that maps: \((x_1, \ldots, x_n, x) \mapsto (x_1, \ldots, x_n, x + f(x_1, \ldots, x_n))\).

Now there is a Deutsch-Jozsa algorithm that can determine if \( f \) is a constant function just using the box one time.

Proof: Cf. [Napkin P270]. The circuit is

\[
(0, 0, \ldots, 0, 1) \mapsto (H(0), H(0), \ldots, H(0), H(1)) \mapsto (H(0), H(0), \ldots, H(0), H(1) + f(H(0), H(0), \ldots, H(0)))
\]

\[
\mapsto (H(H(0)), H(H(0)), \ldots, H(H(0)), H(1) + f(H(0), H(0), \ldots, H(0))).
\]

Then we measure all the first \( n \) bits in the \( |0 \rangle/|1 \rangle \)-basis.

Notice if \( f \) is constant, then the first \( n \) bits must be all \( \pm |00\ldots0 \rangle \), so the measure is all 0. And if \( f \) is not constant, then the first \( n \) bits are entangled, equals the image of

\[
\frac{1}{\sqrt{2^n}} \sum_{(a_1, \ldots, a_n) \in \mathbb{F}_2^n} (-1)^{f(a_1 \ldots a_n)} |a_1 \ldots a_n \rangle.
\]

after the action of \( H \otimes^n \), then its coefficient of \( |0 \ldots 0 \rangle \) is just 0, so the measure cannot be all 0. □

Quantum Fourier Transform

Def. (18.1.3.2) [Discrete Fourier Transform]. The inverse Fourier transform is defined to be:

\[
(x_0, \ldots, x_{n-1}) \mapsto (y_0, \ldots, y_{n-1}),
\]

where

\[
y_k = \frac{1}{N} \sum_{j=0}^{N-1} \omega_N^{jk} x_k.
\]

This is in fact represented by a van der Waerden matrix of \( \omega_N \) times \( \frac{1}{N} \).

Prop. (18.1.3.3) [Fast Fourier Transform]. There is a fast Fourier transform algorithm that can calculate the Fourier transform in \( O(N \log N) \) times.

Proof: □

Def. (18.1.3.4) [Quantum Fourier Transform]. The quantum Fourier transform is a gate represented by a matrix \( U_{QFT} \) which is the van der Waerden matrix of \( \omega_N \) times \( \frac{1}{\sqrt{N}} \).

Proof: It suffices to prove this matrix is truly unitary. □

Prop. (18.1.3.5) [Tensor Representation]. The trick of the quantum Fourier transform lies in its connection with the 2-adic decimal representation:

\[
U_{QFT}(|x_n x_{n-1} \ldots x_1 \rangle) = \frac{1}{\sqrt{N}}(|0 \rangle + \exp(2\pi i \cdot 0.x_1)|1 \rangle)
\]

\[
\otimes(|0 \rangle + \exp(2\pi i \cdot 0.x_2 x_1)|1 \rangle)
\]

\[
\otimes \ldots
\]

\[
\otimes(|0 \rangle + \exp(2\pi i \cdot 0.x_n x_{n-1} \ldots x_1)|1 \rangle)
\]
Proof: Direct calculation. □

Prop. (18.1.3.6). Now by the above tensor representation, the thing seems to be beautiful, and it seems the Fourier transform for $2^n$ data can be done in $n^2$ steps. And this is true, $QFT_n$ is inductively define, Cf.[Napkin P273].

Shor’s Algorithm

Def. (18.1.3.7). For a number $M = pq$, where $p, q$ are different odd prime numbers. Then an $x \mod M$ is called good iff: $(x, M) = 1$, $r = \text{ord}(x)$ is even, and neither of $x^{r/2} \pm 1$ is divisible by $M$.

Then at least half of $(\mathbb{Z}/M\mathbb{Z})^*$ is good.

Proof: It suffices to consider a fixed order $2a$, and this is additive in $\mathbb{Z}/(2a, p - 1)\mathbb{Z} \times \mathbb{Z}/(2a, q - 1)\mathbb{Z}$. □

Remark (18.1.3.8). If we find a good $x$ for $M$, then $x^{r/2} \pm 1$ contains separately a prime $p$ or $q$, so we can use Euclidean algorithm to extract a prime of $M$. This is just the ideal of Shor’s Algorithm.

Prop. (18.1.3.9)[Shor’s Algorithm]. For $M = pq$, we can factor $p, q$ out in $O((\log M)^2)$ time.

Proof: Cf.[Napkin P274]. □

Grover’s Algorithm

Prop. (18.1.3.10).

Prop. (18.1.3.11)[Grover’s Algorithm]. If there are $n$ items labeled $\{0, \ldots, n - 1\}$, and there is a marked item $w$. then there is a quantum algorithm that find $w$ in $O(\sqrt{n})$ times.

Proof: Cf.[Quantum Algorithm MIT P33,35]. □
18.2 Quantum Field Theory

Main references are [Witten, Super-symmetry and Morse Theory], [Witten, Topological Quantum Field Theory, 1988], [Witten, Elliptic Genera and Quantum Field Theory], [Quantum Field Theory and the Jones Polynomial, Witten], [Supersymmetry and Morse Theory, Witten].

1 Supersymmetric Quantum Field Theory

Main references are [Supersymmetry and Morse Theory, Witten].

2 Topological Quantum Field Theory

Main references are [Ati88], [On the Classification of Topological Field Theories, Lurie].

Remark (18.2.2.1). It now seems clear that the way to investigate the subtleties of low-dimensional manifolds is to associate to them suitable infinite-dimensional manifolds (e.g. spaces of connections) and to study these by standard linear methods (homology, etc.). In other words we use quantum field theory as a refined tool to study low-dimensional manifolds. ——Atiyah.

Def. (18.2.2.2) [Topological Quantum Field Theory]. A topological quantum field theory or TQFT in dimension $d$ defined over a ground ring $\Lambda \in \mathcal{C}Alg$ consists of the following data:

- For any $\Sigma \in \text{Diff}_{\text{ornt,cpct}}$, there is a finite $\Lambda$-module $Z(\Sigma)$, called the states of particles of $\Sigma$.

- For any $M \in \text{Diff}_{\text{ornt,\partial}}^{d+1}$, there is an element $Z(M) \in Z(\partial M)$, called the vacuum state defined by $M$.

s.t.

- $Z$ are functorial in orientation-preserving diffeomorphisms of $\Sigma$ or $M$.

- $Z$ are involutary, i.e. $Z(\Sigma^*) = Z(\Sigma)^*$, where $\Sigma^*$ is $\Sigma$ with the dual orientation and $Z(\Sigma)^*$ is the dual module of $Z(\Sigma)$.

- $Z$ is multiplicative, i.e. $Z(\Sigma_1 \coprod \Sigma_2) = Z(\Sigma_1) \otimes Z(\Sigma_2)$, and if $\partial M_1 = \Sigma_1 \coprod \Sigma_3$, $\partial M_2 = \Sigma_3 \coprod \Sigma_2$, $M = M_1 \coprod M_2$, then
  $$Z(M) = \langle Z(M_1), Z(M_2) \rangle$$

  where the pairing is the natural pairing $Z(\Sigma_3) \times Z(\Sigma_3)^* \to \Lambda$.

- $Z(\emptyset^d) = \Lambda$, and $Z(\emptyset^{d+1}) = 1 \subset \Lambda = Z(\emptyset^d)$.

Prop. (18.2.2.3) [Cobordisms]. If For $M \in \text{Diff}_{\text{ornt,\partial}}^{d+1}$, if $\partial M = \Sigma_1^* \coprod \Sigma_2$, then $Z(M) \in Z(\Sigma_1)^* \otimes Z(\Sigma_2)$ can be regarded as a homomorphism $Z(M) : Z(\Sigma_1) \to Z(\Sigma_2)$, and this is compatible with composition of cobordisms. In particular, if $\Sigma \in \text{Diff}_{\text{ornt,cpct}}^d$, $M = \Sigma \times [0,1]$, then $Z(M) = \text{id} \in \text{End}(Z(\Sigma))$.

In particular, the states of particles and vacuum states can be calculated by cut-and-paste.

Def. (18.2.2.4) [Vacuum-Vacuum Expectation Values]. For $M \in \text{Diff}_{\text{ornt,cpct}}^{d+1}$, $Z(M) \in Z(\partial M = \emptyset) = \Lambda$ is an element, called the vacuum-vacuum expectation value of $M$.

Prop. (18.2.2.5) [Homotopy Invariance]. Let $\Sigma, \Sigma' \in \text{Diff}_{\text{ornt,cpct}}^d$, $M = \Sigma \times [0,1], M' = \Sigma' \times [0,1]$, and $F : M \to M'$ is a homotopy of morphisms between $f_1, f_2 : \Sigma \to \Sigma'$, then $Z(f) = Z(f') : Z(\Sigma') \to Z(\Sigma)$, by (18.2.2.3).
Examples of Topological Quantum Field Theory

Remark (18.2.2.6). For $d = 1$, there are Floer/Gromov theory and holomorphic conformal field theories.

Remark (18.2.2.7). For $d = 2$, there are Jones/Witten theory, Casson theory, Johnson theory, and “Thurston” theory.

Remark (18.2.2.8). For $d = 3$, there are Floer/Donaldson theory.
19  |  Combinatorics

19.1  Combinatorics

1  Graph Theory

Def. (19.1.1.1) [Graphs]. A graph $X$ is a CW-complex of dimension $\leq 1$ with a given presentation $(X^0, X^1 = X)(3.9.3.1)$. The elements in the set of $X^0$ are called vertices of $X$, and the 1-cells are called edges of $X$.

For a graph $X$, a subgraph is a sub CW-complex of $X$.

Def. (19.1.1.2) [Trees]. A tree is a graph $T$ s.t. $H_1(T) = 0$. A tree in a graph $X$ is called a maximal tree if it contains all vertices of $X$. A forest is a graph that is a disjoint union of trees.

Prop. (19.1.1.3). Any tree $T$ is contractible, and any vertex $v$ is a deformation retract of $T$.

Proof: □

Prop. (19.1.1.4) [Maximal Trees]. Every connected graph contains a maximal tree, and any tree in such a graph is contained in a maximal tree.

A tree $T$ in a graph $X$ is maximal iff $X^0 \subset T$.

Proof: Cf. [Hat02]P84. □

Prop. (19.1.1.5) [π1 of Graphs]. For a connected graph $X$ with a maximal tree $T$, $\pi_1(X)$ is a free group with basis the classes $[f_\alpha]$ corresponding to the edges $e_\alpha \in X \setminus T$.

Proof: The quotient map $X \to X/T$ is a homotopy equivalence by (3.9.6.7). And the quotient space $X/T$ has only one vertex, thus is a wedge sum of circles corresponding to $e_\alpha \in X \setminus T$. So we are done by (3.9.4.28). □

Prop. (19.1.1.6) [Covering Spaces of Graphs]. Every covering space $\pi : \tilde{X} \to X$ of a graph is also a graph, with vertices and edges lifts of vertices and edges of $X$.

Proof: Let the sets $\pi^{-1}(v)$ be vertices of $\tilde{X}$, where $v$ are vertices of $X$. And if we write $X$ as a quotient space of $X^0 \cup_\alpha I_\alpha$, each $I_\alpha$ can be lifted to maps to $\tilde{X}$, and we let these be edges of $\tilde{X}$. The topology of $\tilde{X}$ coming from quotient topology of this is the same as the original topology, because they has the same basis open sets, because $\pi$ is a local homeomorphism. □

Prop. (19.1.1.7) [Spencer’s Lemma]. If there is a triangulation of a plane polygon $P$, for arbitrary 3-color numbering($\{0, 1, 2\}$) of the vertices, if the number of edges on the boundary with color $(0, 1)$ is odd, then there is a triangle with vertices of pairwise different colors.
Proof: In fact the number of those triangles with vertices of pairwise different colors is odd. In fact, the number of \((0,1)\)-edges on a triangle is odd iff its vertices has pairwise different colors. But the sum of numbers of \((0,1)\)-edges on the triangles are odd, by hypothesis, thus the result. □

Prop.(19.1.1.8)[Plane Graphs]. When can a graph be embedded in \(\mathbb{R}^2\)?

Proof: □

Applications

Thm.(19.1.1.9)[Monsky]. A square cannot be divided into \(m\) triangles of the same area, where \(m\) is odd.

Proof: Choose a 3-coloring on \(\mathbb{R}^2\): By\((12.1.3.4)\) there can be an extended 2-adic valuation \(|\cdot|_2\) on \(\mathbb{R}\) that extends the 2-adic valuation on \(\mathbb{Q}\), then color a point \((x,y)\)

- 0 if \(|x|_2 < 1, |y|_2 < 1,
- 1 if \(|x|_2 \geq 1\) and \(|x|_2 \geq |y|_2,
- 2 if \(|y|_2 \geq 1\) and \(|y|_2 > |x|_2.

Then there are two things:

1. The coloring is invariant under translation by vectors represented by a point of color 0.
2. The valuation of the area of a triangle with vertices of 3 different colors is bigger than 1, because we can assume one vertex is the origin, and then its area is \(\frac{1}{2}|x_1y_2 - x_2y_1|\), which, because the coloring, must have 2-adic valuation bigger than 1.

Now back to the question, let the square be placed as a unit square, then its area is 1, and it has exactly one \((0,1)\)-edge, so by Spencer’s lemma\((19.1.1.7)\), it has a triangle with vertices of pairwise different colors, so its area \(A\) has valuation\(> 1\), but the total area is \(mA = 1\) that has valuation 1, so \(|m| < 1\), which means that \(m\) is even. □

Prop.(19.1.1.10)[Hindman’s Theorem]. Whenever \(\mathbb{N}\) is colored with f.m. colors, one can find an infinite subset \(A \subset \mathbb{N}\) and a color \(c\) that whenever \(F \subset A\) is finite, the color of the sum of numbers in \(F\) is colored \(c\).


2 Ramsey’s Theory

Prop.(19.1.2.1)[Finite Ramsey’s Theorem]. For any positive natural number \(k, r, s\), there is a \(n\) that if we color the \(r\)-subsets of a set with cardinality \(n\) into \(s\) groups, then there is a subset of cardinal \(k\) that all its \(r\)-subsets are colored the same.

Proof: Cf.[Set Theory P218]. □

3 Polytopes

Def.(19.1.3.1)[Polytopes]. A \(n\)-\textbf{polytope} is a compact subset of \(\mathbb{R}^n\) for some \(n \in \mathbb{Z}\) with boundaries given by polytopes of smaller dimensions. A \textbf{polygon} is a 2-polytope. A \textbf{polyhedron} is a 3-polytope.
Def. (19.1.3.2) [Tetrahedra]. A **tetrahedron** is an 3-simplex in \( \mathbb{R}^3 \).

Def. (19.1.3.3) [Orthohedra]. An **orthohedron** is a tetrahedron isomorphic to the convex hull of the four points 
\[
\{(0,0,0), (x,0,0), (x,y,0), (x,y,z)\} \in \mathbb{R}^3.
\]

Prop. (19.1.3.4) [Dihedral Angles of Orthohedra].
- Each orthohedron has dihedral angles \((\alpha, \beta, \gamma, \pi/2, \pi/2, \pi/2)\).
- A rectangular solid can be cut into 6 orthohedra sharing a common diagonal. And for any \(\alpha, \beta, \gamma \in (0, \pi)\), \(\alpha + \beta + \gamma = \pi\), there is a rectangular solid that can be cut into 6 orthohedra s.t. the dihedral angles along the diagonal are \((\alpha, \beta, \gamma, \alpha, \beta, \gamma)\).

**Proof:** Only 2 needs a proof, and this is verified by brutal force calculations. \(\square\)

4 Hilbert’s 3rd Problem

Cf. [Sch13b].

Def. (19.1.4.1) [Scissors Congruence]. A **dissection of a polytope** \(P\) is an expression \(P = \bigcup_i^n P_i\) s.t. the interiors of \(P_i\) are disjoint.

Two polytopes \(P, Q\) are called **scissors-congruent** if there are dissections \(P = \bigcup_i^n P_i, Q = \bigcup_i^n Q_i\) s.t. \(P_i \cong Q_i\) for \(1 \leq i \leq n\). Scissors congruence relations are denoted by \(\sim_s\).

Thm. (19.1.4.2) [Wallace-Bolyai-Gerwien]. Any two polygons \(P, Q\) in \(\mathbb{R}^2\) are scissors-congruent.

**Proof:** Find a line \(l\) that is not parallel to any line generated by vertices of \(P\) and \(Q\), cut \(P, Q\) through lines parallel to \(l\) and passing through some vertices of \(O, Q\). Then we get some trapezoids. Then we cut them into right triangles.

Now we transform any right triangle \(P\) with vertices \(\{A = (-0,0), B = (0,2b), C = (0,c)\}\) to a triangle triangle of height 2: Now consider another right triangle with vertices \(\{A = (-0,0), X = (0,2), Y = (0, bc)\}\). Then \(BY/\parallel CX\), thus \(BYC\) and \(BYX\) are triangles of the same base and height.

Then \(BYC \sim_s BYX\): cut them into parallelograms with the same base and height, then it is easy to see any two such parallelograms are scissors-congruent.

Now all the triangles has a side of length 2, we can transform them into rectangles with a side of length 1. Then clearly \(P, Q\) are transformed together. \(\square\)

Thm. (19.1.4.3) [Zylev]. If \(P, A, B\) are polytopes, \(A \subset P, B \subset P, P \setminus A \sim_s P \setminus B\), then \(A \sim_s B\).

**Proof:** Let
\[
F = A \bigcup_{k=1}^n P_k = B \bigcup_{k=1}^n Q_k, P_k \sim_s Q_k
\]

We can dissect them even further s.t. \(\text{Vol}(P_k) < \frac{1}{2} \text{Vol}(A)\). Then we use induction on \(n\) to show that \(A \sim_s B\): \(n = 0\) is trivial. For \(n > 0\), because of the volume bound, \(\text{Vol}(A \setminus Q_n) > \text{Vol}(Q_n)\), thus we can find disjoint \(T_1, \ldots, T_n \subset A \setminus Q_n\) s.t. \(T_k \sim_s P_k \cap Q_n\). Now define
\[
F' = F \setminus Q, P'_k = (P_k \setminus Q_n) \cup T_k \sim_s P_k, \quad A' = F' \bigcup_{k=1}^{n-1} P'_k = (A \setminus \bigcup_{k=1}^{n-1} T_k) \bigcup Q_k
\]

Then by induction, \(A' \sim_s B' = B\). But \(A' \sim_s A\) by changing \(T_k\) with \(Q_k\). \(\square\)
Dehn-Sydler Theorem

Prop. (19.1.4.4) [Tetrahedra]. Any polyhedron has a dissection into tetrahedra.

Proof: By choose a sufficiently small lattice dissection of \( \mathbb{R}^3 \), it suffices to consider three cases:
- A cube.
- A cube cut by one hypersurfaces.
- A cube cut by two hypersurfaces.
- A cube containing a single vertex.
All cases are straightforward. \( \Box \)

Def. (19.1.4.5) [Dehn Invariants]. For a polyhedron \( P \), define the Dehn invariant of \( P \) as
\[
\Delta(P) = \sum_i l_i[\alpha_i] \in \mathbb{R} \otimes (\mathbb{R}/\mathbb{Z}\pi)
\]
where the sum is over all edges \( e_i \), of \( P \), \( l_i = l(e_i) \), and \( \alpha_i \) is the dihedral angles of \( e_i \).

Thm. (19.1.4.6) [Dehn]. If two polyhedra in \( \mathbb{R}^3 \) are scissors-congruent, then they have the same volume and Dehn invariants.

Proof: The volumes are the same by the invariance properties of Lebesgue measure. To show the Dehn invariants are the same, notice the dissections of a polytope \( P \) may create new edges, but the sum of angles around a new edge is \( 2\pi \) for if it is contained in the interior of \( P \), or \( \pi \) if it is in the surface of \( P \). \( \Box \)

Def. (19.1.4.7) [Simple Prisms]. A simple prism is a polyhedron that is isomorphic to an affine translate of \( T \times I \subset \mathbb{R}^2 \times \mathbb{R} \), where \( T \subset \mathbb{R}^2 \) is a triangle.

Prop. (19.1.4.8). A simple prism \( P \) is scissors-congruent to \([0,1]^2 \times [0, \text{Vol}(P)]\).

Proof: Place the three edges \( P_1Q_1, P_2Q_1, P_3Q_3 \) that is the image of Vertices(\( T \)) \times \( I \) vertically, and they have length \( l \). Then we can talk about the heights of \( P, Q_i \). Suppose \( h(P_1) \geq h(P_2) \geq h(P_3) \). If \( h(P_3) \geq h(Q_1) \), then we can cut \( P \) along height \( h(Q_1) \) make \( P \) scissors-congruent to a perfect simple prism \( P' = T' \times I' \). If \( h(P_3) < h(Q_1) \), then we can cut \( P \) along the plane \( P_2P_3Q_1 \) to make \( P \sim_s P' \), where for \( P', h(P'_3) - h(Q'_1) \) is larger. And if this process goes on, every 2 transform makes \( h(P_3) - h(Q_1) \) bigger by at least \( l \), so eventually \( h(P_3) \geq h(Q_1) \), and we can transform it to a perfect simple prism.

Now if \( P = T \times I \) is a perfect simple prism, (19.1.4.2) shows \( T \) is scissors equivalent to \([0,1] \times [0, \text{Vol}(T)]\), and then it suffices to show \([0, \text{Vol}(T)] \times I \) is scissors equivalent to \([0, \text{Vol}(P)]\), which is by (19.1.4.2) again. \( \Box \)

Def. (19.1.4.9) [pseudo-prisms]. A pseudo-prisms is a convex polyhedra \( (OPQRS) \), where
- \( OPQ \) is an isosceles with \( OP = PQ \),
- \( PR, QS \) is orthogonal to the plane \( OPQ \),
- \( l(QS) = 2l(PR) \).
Notice a pseudo-prism \( (OPQRS) \) is scissors-congruent to the perfect simple prism \( OPQ \times PR \).

Def. (19.1.4.10). Denote
\( \mathcal{P} \) the free Abelian group generated by isomorphism classes of all polyhedra.

- \( \mathcal{E} \) the subgroup of \( \mathcal{P} \) generated by the dissection relations.
- \( \mathcal{F} \) is the subgroup of \( \mathcal{P} \) generated by \( \mathcal{E} \) and all the simple prisms (19.1.4.7).
- \( \mathcal{V} = \mathcal{P}/\mathcal{F} \).

Then clearly two polyhedra \( P, Q \) are scissors-congruent iff \([P] = [Q] \in \mathcal{P}/\mathcal{E} \).

**Prop. (19.1.4.11) [R-Structures].** \( \mathbb{R} \) acts on the set of polyhedra by scaling, and this action is additive and multiplicative, and stabilizes \( \mathcal{F} \), thus inducing an \( \mathbb{R} \)-structure on \( \mathcal{V} \).

**Proof:** By (19.1.4.4), \( \mathcal{P} \) is generated by tetrahedra. So it suffices to show that for \( \lambda_1, \lambda_2 \in \mathbb{R}_+ \) and a tetrahedron \( T, [\lambda_1 T]+[\lambda_2 T]−[(\lambda_1+\lambda_2)T] \in \mathcal{F} \). For this, use geometry, notice \((\lambda_1+\lambda_2)T \setminus (\lambda_1 T \cup \lambda_2 T)\) consists of two simple prisms, where these two smaller tetrahedra aligned along an edge of \( T \). \( \square \)

**Prop. (19.1.4.12) [Orthohedra].** \( \mathcal{V} \) is generated by orthohedra (19.1.3.3).

**Proof:** By (19.1.4.4), it suffices to show that for any tetrahedron \( T, [T] \) is a linear combinations of orthohedra. For this, take the center \( I \) of the inscribed circle of \( T \), and take its projections \( I_1, I_2, I_3, I_4 \) to the faces of \( T \), then they form 24 orthohedra (may be degenerate ones). Thus \( T \) is a linear combinations of those non-degenerate orthohedra. \( \square \)

**Prop. (19.1.4.13).** A simple primes \( P \) has Dehn invariant \( \Delta(P) = 0 \) (19.1.4.14) and (19.1.4.8), so by (19.1.4.8) again, \( \Delta \) factors through \( \mathcal{V} : \mathbb{R} \to \mathbb{R} \otimes (\mathbb{R}/\mathbb{Z}\pi) \), which is \( \mathbb{R} \)-linear with \( \mathbb{R} \)-structure on \( \mathcal{V} \) given in (19.1.4.11).

**Thm. (19.1.4.14) [Dehn-Sydler].** Two polyhedra in \( \mathbb{R}^3 \) are scissors-congruent iff they have the same volume and Dehn invariants.

**Proof:** One direction is shown in (19.1.4.6). For the other, it suffices to show this map \( \Delta : \mathcal{V} = \mathcal{P}/\mathcal{F} \to \mathbb{R} \otimes (\mathbb{R}/\mathbb{Z}\pi)(19.1.4.13) \) is injective, because in this way, if two polyhedra has the same volume and Dehn invariants, then they are scissors equivalent to two prisms with the same volume, hence scissors-congruent, by (19.1.4.8).

Take a good function \( \varphi : \mathbb{R} \to \mathcal{V}(19.1.4.24) \). \( \varphi \) vanishes on \( \mathbb{Z}\pi \), thus extends to an \( \mathbb{R} \)-linear map \( \Phi : \mathbb{R} \otimes (\mathbb{R}/\mathbb{Z}\pi) \to \mathcal{V} \), and for an orthohedron \( T \), \( \Phi(\Delta([T])) = [T] \) by (19.1.4.15), and orthohedra generate \( \mathcal{V} \) by (19.1.4.12), so \( \Phi \circ \Delta = \text{id}_\mathcal{V} \). Thus \( \Delta \) is injective. \( \square \)

**Homological Arguments**

**Def. (19.1.4.15) [Good Functions].** A map \( \varphi : \mathbb{R} \to \mathcal{V} \) is called a good function if

- \( \varphi \) is additive and \( \varphi(\pi) = 0 \).
- For any orthohedron \( T, [T] = \sum_{i=1}^6 l_i \varphi(\alpha_i) \), where the notation is the same as in (19.1.4.5).

**Def. (19.1.4.16) [T(a, b)].** For \( a, b \in (0, 1) \), define \( a' = \sqrt{a^{-1}−1}, b' = \sqrt{b^{-1}−1} \), and define \( T(a, b) \) to be the orthohedron with vertices

\[ \{(0, 0, 0), (a', 0, 0), (a', a'b', 0), (a', a'b', b')\} \in \mathbb{R}^3. \]

Notice \( T(a, b) \cong T(b, a) \).

The order of the vertices is also important. It is always assumed to be written in this order.
Prop. (19.1.4.17). For $\alpha, \beta \in \mathbb{R}$, $T(\sin^2(\alpha), \sin^2(\beta))$ has three edges with dihedral angle $\pi/2$, and three edges with lengths $\cot(\alpha), \cot(\beta), \cot(\gamma)$ and dihedral angles $(\alpha, \beta, \pi/2 - \gamma)$ resp., where $\sin^2(\gamma) = ab, \gamma \in (0, \pi/2)$. In particular,
\[
\Delta(T(\sin^2(\alpha), \sin^2(\beta))) = \cot(\alpha) \otimes \alpha + \cot(\beta) \otimes \beta + \cot(\gamma) \otimes (\pi/2 - \gamma).
\]
Proof: Brutal force calculation.

Prop. (19.1.4.18). For $a, b, c \in \mathbb{R}_+$,
\[
\begin{align*}
  a[T(\frac{a+b}{a+b+c}, \frac{a}{a+b})] + b[T(\frac{a+b}{a+b+c}, \frac{b}{a+b})] &= a[T(\frac{a+c}{a+b+c}, \frac{a}{a+b+c})] + c[T(\frac{a+c}{a+b+c}, \frac{c}{a+c})]
\end{align*}
\]
Proof: This follows from the different ways of cutting the tetrahedron with vertices
\[
\{O = (0, 0, 0), X = (\sqrt{bc}, 0, 0), Y = (0, \sqrt{ac}, 0), Z = (0, 0, \sqrt{ab})\} \in \mathbb{R}^3.
\]
In fact, for this tetrahedron, the plane orthogonal to $YZ$ passing through $X$ cut this to two orthohedra, and similar does the plane orthogonal to $XZ$ passing through $Y$. These two cutting give the assertion above.

Def. (19.1.4.19) [Homological Functions]. A **homological function** is a function $h : (0, 1) \to \mathcal{V}$ s.t.
- For $a, b \in (0, 1), [T(a, b)] = h(a) + h(b) - h(ab)$.
- If $a, b \in (0, 1), a + b = 1$, then $ah(a) + bh(b) = 0$.

Prop. (19.1.4.20). For $V \in \text{Vect}/\mathbb{R}$, if $g : \mathbb{R}_+ \to V$, define $\delta(g)(a, b) = g(a) + g(b) - g(ab)$. And if $F : \mathbb{R}_+^2 \to V$, define $\delta(F)(a, b, c) = F(a, b) - F(a, c) + F(ab, c) - F(ac, b)$.

Then if $F : (0, 1) \to \mathcal{V}$ is symmetric and $\delta(F) = 0$, then $F = \delta(f)$ for some $f : (0, 1) \to \mathcal{V}$.

Proof: Cf.[Sch13b].

Prop. (19.1.4.21). Let $G : \mathbb{R}_+^2 \to V$ be a symmetric function satisfying
- $G(\lambda a, \lambda b) = \lambda G(a, b), \lambda, a, b \in \mathbb{R}_+$,
- $G(a, b) + G(a + b, c) = G(a, c) + G(a + c, b)$.
Then there exists a homomorphism $g : \mathbb{R}_+^2 \to \mathcal{V}$ s.t. when $a + b = 1$,
\[
G(a, b) = ag(a) + bg(b).
\]
Proof: Cf.[Sch13b].

Prop. (19.1.4.22) [Sydler]. Let $F : (0, 1)^2 \to \mathcal{V} : (a, b) \mapsto [T(a, b)]$, then $F$ is symmetric, and $\delta(F) = 0$.

Proof: We check that $[T(a, b)] + [T(ab, c)] = [T(a, c)] + [T(ac, b)]$. This is done by geometry:
Put $T(a, b), T(a, c)$ together: $T(a, b) \cong ABCD, T(a, c) \cong ABEF$, where $BDE$ is collinear. Let $H$ be the center of the sphere $S$ passing through $ACDE$, and the projection of $H$ on the planes $ABC, ABD$ is denoted by $I, J$ resp. Let $K, L, M$ be the intersection of $AH, AI, AJ$ with the sphere $S$ resp.
Then it can be verified that $T(ab,c) \cong ANMK, T(ac,b) \cong AFLK$. Let $P = ABDFHI + ADHJ$, then

$$P - \text{(AICHD)} - \text{(FICHD)} + \text{(DJMHK)} = T(a,b) + T(ab,c).$$

$$P + \text{(DJEHF)} - \text{(AJEHF)} + \text{(FILHK)} = T(a,c) + T(ac,b).$$

\[ \square \]

**Cor. (19.1.4.23).** Homological functions(19.1.4.19) exist.

**Proof:** By(19.1.4.20), there exists $f : (0,1) \to V$ s.t. $F(a,b) = [T(a,b)] = f(a) + f(b) - f(ab)$. Then we want to find $h = f - g$, where $g : (0,1) \to V$ is a homomorphism s.t. when $a + b = 1$, $ah(a) + bh(b) = 1$, which is equivalent to

$$ag(a) + bg(b) = af(a) + bf(b).$$

Let

$$G : \mathbb{R}_+^2 \to V : (a,b) \mapsto af\left(\frac{a}{a+b}\right) + bf\left(\frac{b}{a+b}\right),$$

then $G(\lambda a, \lambda b) = \lambda G(a,b), \lambda, a, b \in \mathbb{R}_+$, and $G(a,b) + G(a+b, c) = G(a, c) + G(a + c, b)$. In fact, this boils down to(19.1.4.18). Thus by(19.1.4.21), we truly can find such a function $g$. \[ \square \]

**Prop. (19.1.4.24).** Good functions(19.1.4.15) exist.

**Proof:** Take a homological function $h(19.1.4.23)$, define $\varphi : \mathbb{R} \to V$:

$$\varphi\left(\frac{n\pi}{2}\right) = 0, \quad n \in \mathbb{Z}, \quad \varphi(\alpha) = \tan(\alpha) h(\sin^2(\alpha)).$$

We show this is a good function:

Firstly we show:

**Lemma (19.1.4.25).** $\varphi(\pi/2 - \alpha) = -\varphi(\alpha), \varphi(\alpha + \pi/2) = \varphi(\alpha)$. 

Proof: If $\alpha = n\pi/2$, the assertion holds. So we assume $\alpha \neq n\pi/2$ and let $\beta = \pi/2 - \alpha$, $a = \sin^2(\alpha)$, $b = \sin^2(\beta)$, then $a + b = 1$, so by definition (19.1.4.19),

$$0 = 2ah(a) + abh(b) = 2\sin^2(\alpha) \cot(\alpha)\varphi(\alpha) + 2\sin^2(\beta) \cot(\beta)\varphi(\beta)$$

$$= \sin(2\alpha)\varphi(\alpha) + \sin(2\beta)\varphi(\beta) = \sin(2\alpha)(\varphi(\alpha) + \varphi(\beta))$$

So the assertion holds as $\sin(2\alpha) \neq 0$.

The second equality follows from the first. \qed

Next, we show $[T] = \sum_{i=1}^6 l_i\varphi(\alpha_i)$ for an orthohedron $T$: By scaling, it suffices to prove for $T$ of the form $T(\sin^2(\alpha), \sin^2(\beta))(19.1.4.16)$. Thus by (19.1.4.19) and (19.1.4.17),

$$[T(\sin^2(\alpha), \sin^2(\beta))] = h(\sin^2(\alpha)) + h(\sin^2(\beta)) - h(\sin^2(\alpha) \sin^2(\beta))$$

$$= \cot(\alpha)\varphi(\alpha) + \cot(\beta)\varphi(\beta) + \cot(\gamma)\varphi(\pi/2 - \gamma) = \sum_{i=1}^6 l_i\varphi_i(\alpha_i)$$

Finally, to show additivity of $\varphi$, notice by the lemma above, it suffices to show $\varphi(\alpha) + \varphi(\beta) = \varphi(\alpha + \beta)$ for $\alpha, \beta \in (0, \pi/2)$. In this case, let $\gamma = \pi - \alpha - \beta \in (0, 2\pi)$, then use (19.1.3.4) to find a rectangular solid that cuts along a diagonal to 6 orthohedra $T_i$ s.t. the dihedral angles along the diagonals are $(\alpha, \beta, \gamma, \alpha, \beta, \gamma)$. Then

$$0 = [R] = \sum_{k=1}^6 [T_i] = 2l(\varphi(\alpha) + \varphi(\beta)) + \sum_{k=1}^6 l_k(\varphi(\theta_{k1}) + \varphi(\theta_{k2}))$$

where $l$ is the length of the diagonal, $\theta_{k1}$ are the dihedral angles along the edges of the rectangular solid that is connected to the diagonal, and $\theta_{k1} + \theta_{k2} = \pi/2$. Thus by the lemma above, $\varphi(\alpha) + \varphi(\beta) = -\varphi(\gamma) = \varphi(\alpha + \beta)$. \qed
20 Elementary Mathematics

1 Algebra

Prop. (20.1.1.1). If \((a_n)_{n \geq n_0, n \in \mathbb{N}}\) is a series of real numbers and \(C \in \mathbb{R}\) s.t. \(a_{m+n} \geq a_m + a_n + C\) for any \(m, n \geq n_0 \in \mathbb{N}\), then \(a_m/m\) converges to \(\lim_{n \to \infty} a_n/n \in (-\infty, \infty)\).

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

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

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

2 Number Theory

Def. (20.1.2.1) [Prime Numbers]. \(p \in \mathbb{Z}_+\) is called a (rational) prime number if for any \(d \in \mathbb{Z}_+\), \(d/p\) implies \(d = 1\) or \(d = p\). The set of prime numbers is denoted by \(\mathbb{P}\).

Prop. (20.1.2.2) [\(p\)-Power in Product]. \(v_p(n!) = \frac{n-c(n)}{p-1}\), where \(c(n)\) is the sum of the presentation of \(n\) in the \(p\)-adic base.

Cor. (20.1.2.3). \(v_p\left(\binom{a+b}{a}\right)\) equals the number of carries when adding \(a\) and \(b\) in base \(p\).

Def. (20.1.2.4) [Integral Part]. For any number \(\alpha \in \mathbb{R}\), let \([\alpha]\) be the maximal integer \(n\) that \(n \leq \alpha\), called the integral part of \(\alpha\) and \(\{\alpha\} = \alpha - [\alpha]\), called the fractional part of \(\alpha\).

Prop. (20.1.2.5) [Approximation of Irrational Numbers]. Let \(\alpha\) be an irrational number, then for any integer \(N\), there exists an integer \(n \in \mathbb{N}\) that \(\{n\alpha\} < 1/N\) or \(\{n\alpha\} > 1 - 1/N\).

Proof: Consider the sequence

\[\{\alpha\}, \{2\alpha\}, \ldots, \{(N+1)\alpha\},\]

where \(\{x\}\) is the fractional part of \(x\), then this sequence sits in the \(N\) intervals

\[\{(0, 1/N), (1/N, 2/N), \ldots, ((N-1)/N, 1)\},\]
thus there are two that are in the same interval. If \( v_1 < v_2 \) satisfies \( \{v_1 \alpha \} \) and \( \{v_2 \alpha \} \) are in the
same interval, then \( n = v_2 - v_1 \) satisfies the desired property. □

**Prop. (20.1.2.6) [Cauchy-Davenport].** If \( A, B \) are two nonempty subsets of \( \mathbb{F}_p \), then \( |A + B| \geq \min\{p, |A| + |B| - 1\}. \)

**Proof:** If \( |A| + |B| > p \), then this is trivial, because \( A \cap (B - x) \neq \emptyset \) for all \( x \).

Now if \( |A| + |B| \leq p \), and if \( A + B \subset C \) with \( |C| = |A| + |B| - 2 \), define \( f = \prod_{x \in C}(x + y - c) \),
then \( f(a, b) = 0 \) for all \( a, b \in B \), but the coefficient of the highest degree term \( x^{|A| - 1}y^{|B| - 1} \) is \( C^{|A| - 1}_{|A| + |B| - 2} \neq 0 \), so this
contradicts combinatorial Nullstellensatz (2.2.2.6). □

**Cor. (20.1.2.7).** Any element of \( \mathbb{F}_p \) is a sum of two squares, as there are \( \frac{p + 1}{2} \) squares.

**Prop. (20.1.2.8) [Power Lifting].** If \( a \equiv b \mod p \), then \( a^p \equiv b^p \mod p^{n+1} \) for all \( n > 0 \).

**Proof:** Prove by induction, if \( a^p = b^p + p^{n+1}c \) for some \( c \), then \( a^{p+1} = b^{p+1} + p^{n+2}d + p(n+1)cp \), so we are done.

**Lemma (20.1.2.9).** \( \sum_{x=0}^{p-1} x^k \equiv -1 \mod p \) iff \( p - 1 \mid k \), and \( \equiv 0 \mod p \) otherwise.

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

**Prop. (20.1.2.10) [Quadratic Legendre Symbol Sum].** For add prime \( p \),
\[
\sum (\frac{x^2 + 1}{p}) = -1.
\]

**Proof:** The sum is equivalent modulo \( p \) to \( \sum_{x=0}^{p-1}(x^2 + ax + b)^{\frac{p-1}{2}} \), which by the lemma (20.1.2.9) above equivalent to \( -1 \) modulo \( p \). Now it can not be \( p - 1 \), because otherwise there is a solution for \( p \mid x^2 + 1 \), and then it can be calculated directly. □

**Prop. (20.1.2.11).** The multiplicative group of \( \mathbb{Z}/2^n \) is \( \mathbb{Z}/2 \times \mathbb{Z}/2^{n-2} \) for \( n \geq 2 \).

**Proof:** it suffices to show \( 3^{2^{n-3}} \not\equiv \pm 1 \mod 2^n \), and \( 3^{2^{n-2}} \equiv 1 \mod 2^n \). □

**Lemma (20.1.2.12).** If \( P(x) = a_nx^n + a_{n-1}x^{n-1} + \ldots + a_0 \) satisfies \( a_n \geq 1, a_{n-1} \geq 0 \), and \( |a_i| \leq H \) for \( i \leq n - 2 \), then for any root \( \alpha \) of \( P \), either \( \text{Re} \alpha \leq 0 \), or \( |\alpha| < \frac{1+\sqrt{1 + 4H}}{2} \).

**Proof:** □

**Prop. (20.1.2.13) [\( b \)-adic Decompositions and Irreducibility].** If \( b > 2 \) and \( p \) is a prime, consider the \( b \)-adic expansion \( p = \sum a_n b^n \), then the polynomial
\[
\sum a_nX^n
\]
is irreducible over \( \mathbb{Z} \).

**Proof:** If \( p(x) = h(x)r(x) \), use the lemma (20.1.2.12) to show that \( r(b) \) and \( h(b) \) cannot be 1, thus \( h(b)r(b) = p \) cannot happen. □
Def. (20.1.2.14) [Numerical Polynomials]. A function \( f : \mathbb{Z} \rightarrow \mathbb{Z} \) is called a numerical polynomial if it there exists \( a_1, \ldots, a_r \in \mathbb{Z} \) that

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

for \( n \) sufficiently large.

Prop. (20.1.2.15). Suppose that \( f : \mathbb{Z} \rightarrow \mathbb{Z} \) is defined for \( n \) sufficiently large and \( g(n) = f(n) - f(n-1) \) is a numerical polynomial, then \( f \) is a numerical polynomial.

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

Cor. (20.1.2.16). Any polynomial function with coefficients in \( \mathbb{Q} \) maps any integer sufficiently large into \( \mathbb{Z} \) iff it is a numerical function.

Def. (20.1.2.17) [Euler Function]. The Euler function is defined to be

\[
\varphi : \mathbb{Z}_+ \rightarrow \mathbb{Z}_+ : n \mapsto \sum_{d|n} a.
\]

Def. (20.1.2.18) [Möbius Functions]. The Möbius function is defined to be

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

Prop. (20.1.2.19) [Möbius Identities]. For \( n \in \mathbb{Z}_+ \),

- If \( m \in \mathbb{Z}_+ \) is prime to \( n \), then \( \mu(mn) = \mu(m) \mu(n) \).

\[
\sum_{d|n} \mu(d) = \begin{cases} 1 & n = 1 \\ 0 & n > 1 \end{cases}.
\]

- If \( p \in \mathbb{P} \),

\[
\sum_{d|n, p|d} \mu(d) = \begin{cases} 1 & n = p^k, \exists k \in \mathbb{N} \\ 0 & \text{otherwise} \end{cases}.
\]

Proof: 1: This is clear.

2: By item 1, it suffices to prove for \( d = p^k \) for some \( p \in \mathbb{P} \), then this is clear.

3: By item 1, it suffices to prove for \( d = p^k \) for some \( p \in \mathbb{P} \), then this is clear. \( \square \)

Continued Fractions

Def. (20.1.2.20). A finite continued fraction \([a_1, \ldots, a_n]\) is an abbreviation of

\[
\frac{1}{a_1 + \frac{1}{a_2 + \cdots + \frac{1}{a_n}}} , \quad a_i \in \mathbb{Z}_+.
\]

A continued fraction \([a_1, a_2, \ldots]\) is an abbreviation of

\[
\frac{1}{a_1 + \frac{1}{a_2 + \cdots}} , \quad a_i \in \mathbb{Z}_+.
\]
Def. (20.1.2.21) [Gauss Transformation]. The Gauss transformation is the function \( \varphi : \mathbb{R} \to [0, 1] : \)

\[
\varphi(x) = \begin{cases} 
1/x - \lfloor 1/x \rfloor & x \neq 0 \\
0 & x = 0 
\end{cases}
\]

Prop. (20.1.2.22). For any sequence of positive numbers \( \{a_1, \ldots, a_n, \ldots\} \), \( [a_1, \ldots, a_n] \) converges. In particular, \( \lim_{n \to \infty} [\varphi(x), \varphi^2(x), \ldots, \varphi^n(x)] = \{x\} \) for \( x \in \mathbb{R} \).

Proof: We may assume the sequence is infinite. Then we notice for any \( a \in \mathbb{Z}_+ \) and \( t \) varying in an interval in \( (0, 1] \) of length \( l \), the value of \( \frac{1}{a+t} \) is in an interval of length \( l/a(a+l) \leq l/(l+1) \). So clearly the length of possible values of \( [a_1, \ldots, a_n, t] \) for \( t \) in an interval of length \( l \) is in an interval of length \( l_n \) that \( \lim_{n \to \infty} l_n = 0 \).

Then we conclude \( [a_1, \ldots, a_n] \) is a Cauchy sequence for \( n \), thus it converges. \( \square \)

Prop. (20.1.2.23). \( x \in \mathbb{R} \) is a rational number iff \( \varphi^m(x) = 0 \) for some \( m > 0 \).

Proof: If \( x \) is rational then this is Euclid division. If \( \varphi^m(x) = 0 \), then notice \( x = [x] + [\varphi(x), \varphi^2(x), \ldots, \varphi^{m-1}(x)] \) is rational. \( \square \)

Prop. (20.1.2.24). \( x \in \mathbb{R} \) has eventually periodic continued fractions \( [\varphi(x), \varphi^2(x), \ldots, \varphi^n(x), \ldots] \) iff \( [Q(x) : Q] \leq 2 \).

Proof: If the fraction is finite, then \( Q(x) = Q \), by (20.1.2.23). If the fraction has periodic part \( [a_1, \ldots, a_n] \), let \( t = [a_1, \ldots, a_n, a_1, \ldots, a_n, \ldots, \ldots] \), then \[
\frac{at + b}{ct + d} = t
\]

for some \( a, b, c, d \in \mathbb{Z} \), so \( [Q(t) : Q] = 2 \), and hence \( [Q(x) : Q] = 2 \).

For the converse, \( ? \). \( \square \)
20.2 French to English Dictionary

1 A

- aide: help
- apres: after
- ans: years
- avoir: have
- aux: to the

2 B

3 C

- cas: case
- cet: this
- chaleureusement: warmly
- classifiant: classifying
- corp: field
- courbe: curve

4 D

- dans: in
- d’apres: according to
- de: of, than
- des: of
- du: of
- d’une: of a

5 E

- en: in
- enonce: state
- est: is
- et: and
- etabl: established
- etre: be

6 F

7 G

- generale: general
- grandes: large

8 H

-
• il y a: there is

• introduite: introduced

• indépendamment: independence

• Je: I

• la: the

• le: the

• les: the

• lignes: lines

• lues: read

• nous: we

• par: by, through

• pour: for, to

• peuvent: can

• preuve: proof

• principales: main

• presenterons: introduce

• prolonge: extended

• qui: who
18  R

- recement: recently  •  •  •  •  •
- remercie: thank  •  •  •  •  •
- renvoyant: returning
- reste: rest

19  S

- sa: his  •  •  •  •  •
- ses: its, his, her  •  •  •  •  •
- schema: scheme  •  •  •  •  •
- strategie: strategy
- son: his
- sont: are
- suit: follows
- sur: on, about

20  T

- texte: text  •  •  •  •  •
- theoreme: theorem
- toroidale: toroidal
- traiter: treat

21  U

- un: a  •  •  •  •  •
- une: a

22  V

- variante: variant
- vectoriel: vector

23  W

- 

24  X

- 

25  Y

- 

26  Z

- 
This chapter is a collection of definitions used often. These notations will be used without throughout this book without referring, so if you are confused about some notation, maybe you can find it here.

Sometimes in the beginning of a chapter/section/subsection/..., there are notation assignments. When they contradict (which I will try to avoid from happening), they have descending priorities, and have higher priorities than notation assignments in this chapter.

In any proposition, for any symbol appeared, there will only be two cases:
1. This symbol appear without assigned meanings. Then its meaning is defined in this chapter.
2. This symbol has been assigned meanings. Then its meaning may be different from the notations here (which I will try to avoid from happening).

## 27 General

### Notations (20.2.27.1).

- Use uppercase for names of people.
- $\in$ is an abbreviation for “in” or “be/is/are in”, depending on the syntax. So I will use this symbol more casually than usual.
- $i$ is a chosen square root of $-1$ in $\mathbb{C}$.
- s.t. is an abbreviation for “such that”.
- e.g. is an abbreviation for “for example”.
- i.e. is an abbreviation for “which means”.
- f.m. is an abbreviation for “finitely many”.
- a.e. is an abbreviation for “all but finitely many”.
- “Sufficiently large” means “is an integer greater than a given integer $N_0$ that only depends on the parameters defined before in the statement of the proposition”.

## 28 Set Theory

### Notations (20.2.28.1)[Sets]. For $X \in \text{Set}$,

- Use $\#X$ instead of $|X|$ to denote the cardinality of a set $X$.
- To avoid confusion with other structures on sets, use bijection of sets instead of isomorphism of sets to indicate an isomorphism in $\text{Set}$.
- Use $U \subset X$ to indicate $U$ is a subset of $X$. Use $U \subseteq X$ ot indicate $U$ is a proper subset of $X$. 
• Use \texttt{capital} to represent a property on a set.
• If $P$ is a property on $X$, then use $\{x \in X : P(x)\}$ or $\{x \in X | P(x)\}$ to indicate the subset of $X$ defined by the property $P$, depending on which avoids confusion better.
• If $S \subset P(X)$, we say a property $P$ holds for elements of $Y$ sufficiently large if it holds for all elements of $Y$ containing a fixed subset $S_0 \subset X$. Notice this definition is compatible with the definition of numbers being sufficiently large, by taking $X = \aleph_0$ and $Y = \mathbb{N} \subset P(\aleph_0)$.
• Use \texttt{capital} to represent a set that doesn’t form a category with good properties. For example, $G\texttt{Field}$ represents the set of global fields.
• If $f : X \to X$ is a self-map and $S \subset X$, then $f$ is said to fix $S$ or stabilizes $S$ if $f(S) \subset S$.

\textbf{Notations (20.2.28.2) [Common Sets].}
• For $n \in \mathbb{N}$, $[n]$ is the set $\{0, 1, \ldots, n\}$.
• $\mathbb{Z}$ is the ring of integers.
• $\mathbb{Z}_+ \subset \mathbb{Z}$ is the commutative multiplicative monoid of positive integers.
• $\mathbb{Z}_- \subset \mathbb{Z}$ is the commutative multiplicative monoid of negative integers.
• $\mathbb{N} \subset \mathbb{Z}$ is the commutative multiplicative monoid of non-negative integers.
• $\mathbb{Q}$ is the field of rational numbers.
• $\mathbb{R}$ is the ordered valued field of real numbers.
• $\mathbb{R}_+$ is the ordered commutative multiplicative monoid of positive real numbers.
• $\mathbb{C}$ is the complete valued field of complex numbers.

\section{29 Categories}

\textbf{Notations (20.2.29.1) [Categories].}
• Use \texttt{mathscr} capital for symbols representing a category.
• Use pr for morphisms that look like projections.

\textbf{Notations (20.2.29.2) [Common Categories].} To avoid the set-theoretical issue that the class of all sets is not a set, we fix a cardinal $\kappa$, which will be given in prior in each situation, and define
• Set to be the category of sets with cardinality $< \kappa$.
• $\mathsf{Grp}$ to be the category of groups with cardinality $< \kappa$.
• $\mathsf{Ab}$ to be the category of Abelian groups with cardinality $< \kappa$.
• $\mathsf{Grp}^{\text{fin}}$ to be the category of finite groups. $\mathsf{Ab}^{\text{fin}}$ to be the category of finite Abelian groups.
• $\mathsf{CAlg}$ to be the category of commutative unital rings with cardinality $< \kappa$.
• For $p \in \mathbb{P}$, $\mathsf{CAlg}^p$ to be the category of commutative unital rings of characteristic $p$ with cardinality $< \kappa$.
• $\mathsf{Field}$ to be the category of fields\textit{(2.2.1.3)} with cardinality $< \kappa$.
• $\mathsf{Field}^p$ to be the category of fields of characteristic $p$ with cardinality $< \kappa$, where $p \in \mathbb{P} \cup \{0\}$.
• $\mathsf{Top}$ to be the category of topological spaces with cardinality $< \kappa$.
• $\text{TopG}$ to be the category of topological groups with cardinality $< \kappa$.
• $\text{Cat}$ to be the category of categories with cardinality $< \kappa$.
• In generally, whenever we define the category of some objects, we mean the category of objects with cardinality $< \kappa$. This applies to the whole book.

Remark (20.2.29.3). If the cardinal $\kappa$ in (20.2.29.2) is chosen to be too small, some construction in the categories won’t be possible. For example, if you take $\kappa = 2$, then $\{\emptyset\} \coprod \{\emptyset\}$ is not definable in $\text{Set}$. If you take $\kappa = \aleph$, then $\coprod_{\kappa} \{\emptyset\}$ is not definable in $\text{Set}$.

So usually $\kappa$ is taken to be a large enough strongly inaccessible cardinal (whose existence depends on the large cardinal axiom). But in specific cases we can take $\kappa$ to be smaller to show some proposition is invariant of the axiom of large cardinals, for example the Weil conjecture (Deligne’s theorem).

Notations (20.2.29.4) [Categories]. For $\mathcal{C}, \mathcal{D} \in \text{Cat}$, $A \in \mathcal{C}$,
• $\mathcal{C} \ll A$ is the slice category of objects over $A$.
• $\text{Func}(\mathcal{C}, \mathcal{D})$ is the category of functors from $\mathcal{C}$ to $\mathcal{D}$.

Homological Algebra

Notations (20.2.29.5) [Homological Algebras].
• Use $\bigwedge \text{capital}$ for symbols representing a complex over an Abelian category.
• Use $K$-groups instead of $K$-groups.

30 Topology

Notations (20.2.30.1) [Topological Spaces].
• cntd is an abbreviation for “connected”.
• For a metric space $X$ and $x \in X, \delta \in \mathbb{R}_+$, denote $U(x, \delta) = \{y \in X : d(x, y) < \delta\}, \mathcal{D}(x, \delta) = \{y \in X : d(x, y) \leq \delta\}$.

Notations (20.2.30.2) [Common Spaces].
• For $n \in \mathbb{Z}_+$, $S^n$ is the unit sphere $\{x \in \mathbb{R}^n || x || = 1\}$.
• For $n \in \mathbb{Z}_+$, $D^n$ is the unit disk $\{x \in \mathbb{R}^n || x || \leq 1\}$. $D^2$ is also denoted by $D$.
• For $n \in \mathbb{Z}_+$, $I^n$ is the unit cube $\{x = (x_i) \in \mathbb{R}^n || x_i || \leq 1\}$. $I^1$ is also denoted by $I$.
• For $n \in \mathbb{Z}_+, a < b \in \mathbb{R}_{\geq 0}$, $D^n(a, b)$ is the annulus $\{x \in \mathbb{R}^n | a < ||x|| < b\}$. Similarly, we can define $D^n[a, b], D^n(a, b], D^n[a, b]$.
• For $K \in \{\mathbb{R}, \mathbb{C}, \mathbb{H}\}$, $S_K^\infty$ is the unit sphere in $K^\infty$.

31 Algebras

Notations (20.2.31.1) [Groups]. For $G \in \mathfrak{G}$,
• $G_{ab}$ is the abelianization of $G$.
• Use $H \leq G$ to indicate that $H$ is a subgroup of $G$.
• Use $H \triangleleft G$ to indicate that $H$ is a normal subgroup of $G$. 
Notations (20.2.31.2) [Free Groups].
- For \( n \in \mathbb{Z}_+ \), \( F_n \) is the free group generated by \([n-1]\).

Notations (20.2.31.3) [Abelian Groups]. For \( G \in \text{Ab} \),
- \( \hat{G} = \text{Hom}(G, \mathbb{C}^\times) \) is the dual group of \( G \).

Notations (20.2.31.4) [Linear Algebras]. For \( R \in \mathbb{C}\text{Alg}, m, n \in \mathbb{Z}_+ \),
- For \( V \in \text{Vect}_R \), \( V^* \) is the dual space of \( R \).
- \( \text{Mat}_{m \times n}(R) \) is the group of \( m \times n \)-matrices with coefficients in \( R \). \( \text{Mat}(n,R) \) denotes \( \text{Mat}_{m \times n}(R) \).
- \( GL(n, R) \) is the group of invertible elements in \( M(n, R) \).
- For \( A \in \text{Mat}_{m,n}(R) \), \( A^t \in \text{Mat}_{n \times m}(R) \) is the transpose of \( A \).
- For \( A \in GL(n, R) \), \( A^{-1} \in GL(n, R) \) is the inverse of \( A \). \( A^{-t} \) denotes \( (A^{-1})^t = (A^t)^{-1} \).

Prop. (20.2.31.5) [Algebras]. For \( R \in \mathbb{R}\text{ing} \),
- \( \text{Mod}_R \) is the category of left \( R \)-modules.
- \( \text{Alg}_R \) is the the category of \( R \)-algebras.
- \( \mathbb{R}\text{ing}_R \) is the category of associative unital \( R \)-algebras.
- \( \mathbb{C}\text{Alg}_R \) is the category of commutative unital \( R \)-algebras.

Notations (20.2.31.6) [Lie Algebras].
- Use \( \mathfrak{lowercase} \) for symbols representing a Lie algebra.

32 Commutative Algebras

Notations (20.2.32.1) [Fields]. For \( k \in \text{Field} \),
- \( \text{char} \) \( k \) is the characteristic of \( k \).
- \( \overline{k} \) is a fixed algebraic closure of \( k \).
- \( k^{sep} \) is the separable closure of \( k \) in \( \overline{k} \).
- \( k^{perf} \) is the perfect closure of \( k \) in \( \overline{k} \).
- For a Galois extension \( k'/k \), use \( \text{Gal}(k'/k) \) instead of \( \text{Gal}_{k'/k} \) or \( G(k'/k) \) or \( G_{k'/k} \) to denote the Galois group of \( k'/k \).
- \( \text{Gal}_k = \text{Gal}(k^s/k) \).
- \( e \in \text{Gal}(\mathbb{C}/\mathbb{R}) \) is the complex conjugation. For \( a \in \mathbb{C} \), \( e(a) \) is also denoted by \( \overline{a} \).
- For \( p \in \mathbb{P} \), \( \mathbb{F}_p \) is the a fixed finite field of order \( p \).
- For \( p \in \mathbb{P} \), \( \mathbb{F}_{p^r} \) is the fixed finite field of order \( p^r \) contained in \( \overline{F}_p \).
- \( \mu(k) \) is the group of roots of unity in \( k \).

Notations (20.2.32.2) [Commutative Algebras].
- Use \( \mathfrak{lowercase} \) for a first prime ideals. Use \( \mathfrak{uppercase} \) for a prime ideal that is over a given prime ideal.
Notations (20.2.32.3) [Integral Rings]. For $R \in \mathcal{CAlg}^{\text{int}}$, 
- Use "let $(R, K)$ be an integral ring to indicate that $R$ is an integral ring with fraction field $K$.
- Use \texttt{\textbackslash mathcal} uppercase for symbols representing a Dedekind domain.
- $R^\times$ is the commutative monoid of non-zero elements in $R$.
- $R^*$ is the commutative group of units of $R$.

Notations (20.2.32.4) [Local Rings].
- Use "let $(R, K, m, k)$ be an integral local ring" to indicate that $R$ is a local ring with maximal ideal $m$, $\kappa(m) = k$, and $\text{Frac}(R) = K$.
- DVR is the synonym for “discrete valuation ring”.
- CDVR is the synonym for “complete discrete valuation ring”.

Notations (20.2.32.5) [Dedekind Domains].
- Use $D$ to denote differents of extensions of Dedekind domains.
- Use $d$ instead of $\delta$ to denote discriminants of extensions of Dedekind domains.

33 Algebraic Geometry

Notations (20.2.33.1) [Sheaves].
- Use \texttt{\textbackslash mathcal} capital for symbols representing a sheaf or a complex of sheaves.

Notations (20.2.33.2) [Schemes]. Let $(X, O_X) \in \mathcal{S}ch$,
- For brevity, we can use $X$ to denote the the scheme $(X, O_X)$, and use $|X|$ to denote the underlying topological space.
- Use \texttt{\textbackslash mathbf} capital for a relative scheme.
- Use \texttt{\textbackslash mathcal} capital for symbols representing an integral model.
- Use $\kappa(x)$ to denote the residue field of a point $x \in X$ instead of $k(x)$.
- Use $R(x)$ instead of $K(X)$ to denote the function field of an integral scheme $X$.
- Use $O_X(D)$ instead of $\mathcal{L}(D)$ to denote the line bundle associated to a Cartier divisor $D$.

Notations (20.2.33.3) [Categories of Schemes]. Let $X \in \mathcal{S}ch$,
- $\mathcal{S}ch$ is the category of schemes.
- $\mathcal{S}ch'$ is the category of locally Noetherian schemes.
- For $R \in \mathcal{CAlg}$, use $\mathcal{S}ch/R$ to denote $\mathcal{S}ch/\text{Spec} R$.
- $\mathcal{S}ch_{\text{int}}$ is the category of integral schetmes.
- $\mathcal{S}ch^{\text{ft}}/X$ is the category of schemes of f.t. over $X$.
- $\mathcal{S}ch^{\text{loc.ft}}/X$ is the category of schemes locally of f.t. over $X$.
- $\mathcal{S}ch^{\text{f\text{'} et}}/X$ is the category of schemes finite étale over $X$. In general, use superscript to denote relative properties w.r.t. $X$, and superscript to denote absolute properties.
- Use \texttt{\textbackslash underline} for a functor on the category $\mathcal{S}ch/X$. 


Notations (20.2.33.4) [Morphisms of Schemes].
- Use $i$ for a closed immersion and $j$ for an open immersion.
- For $R \in \mathcal{C}\text{Alg}$, $S \in \mathcal{C}\text{Alg}_R$, $X \in \text{Sch}/R$, $X_RS$ denotes $X_{\text{Spec } R} \text{Spec } S$.

Notations (20.2.33.5) [Modules on Schemes]. Let $(X, \mathcal{O}_X) \in \text{Sch},$
- $\text{Mod}(\mathcal{O}_X)$ is the category of $\mathcal{O}_X$-modules.
- $\text{QCoh}(X)$ is the category of $\text{Qco } \mathcal{O}_X$-modules.
- $\mathcal{Coh}(X)$ is the category of coherent $\mathcal{O}_X$-modules.
- For $k \in \mathbb{N}$, $\mathcal{Coh}^{\leq k}(X)$ is the category of coherent $\mathcal{O}_X$-modules with $\text{dim Supp}(F) \leq k$.
- $D(X) = D(\mathcal{O}_X) = D(\text{Mod}(\mathcal{O}_X))$.
- $D_{\text{QCoh}}(X) = D_{\text{QCoh}}(\text{Mod}(\mathcal{O}_X))$.
- $D_{\text{Coh}}(X) = D_{\text{Coh}}(\text{Mod}(\mathcal{O}_X))$.

Notations (20.2.33.6) [Group Schemes].
- $\mu$ is the group scheme $X \mapsto \mu(\Gamma(X, \mathcal{O}_X))$.

Notations (20.2.33.7) [Formal Schemes].
- Use $\mathfrak{m}$ mathfrak capital for symbols representing a formal scheme.

34 Algebraic Number Theory

Notations (20.2.34.1) [Numbers].
- $\mathbb{P}$ is the set of rational primes.
- $\mathbb{P}$ is the algebra consisting of periods.
- Don’t use “#” as an abbreviation of “number” or “numbers”.
- $\Box$ is an abbreviation of “square” or “a square number”. This is obsolete and I strongly suggest not using this notation, for one reason it doesn’t specify square of what numbers, and for the other reason it may be confused with unrecognizable codes.

Notations (20.2.34.2) [Number Theory].
- For $n \in \mathbb{Z}^\times$, use $\mathbb{Z}/(n)$ instead of $\mathbb{Z}/n$ or $\mathbb{Z}/n\mathbb{Z}$.
- Use $p$ to denote a prime number.
- Use $\ell$ instead of $l$ or $q$ to denote a second prime number when $p$ is present.
- Use $\varpi$ instead of $\pi$ to denote a uniformizer in a valuation ring to avoid confusion with the frequently used $\pi$.
- In number theory/arithmetic geometry, try to use $F$ to denote a global field, $K$ a CDVR and $k$ a finite field or general field.
- For $p \in \mathbb{P}$, use $\overline{\mathbb{Q}}_p$ instead of $\overline{\mathbb{Q}}_p$ to denote the fixed $p$-adic completion of $\overline{\mathbb{Q}}$.
- For $p \in \mathbb{P}$, $\mathbb{Q}_p^n$ is the unique unramified extension of $\mathbb{Q}_p$ of the degree $n$ contained in $\overline{\mathbb{Q}}_p$.
- $\mathbb{Z}_{p^n} = \mathcal{O}_{\mathbb{Q}_p^n}$.
- $\{\zeta_n, n \in \mathbb{Z}_+\}$ is a compatible system of roots of unity in $\overline{\mathbb{Q}}$, and $\zeta_2 = i$. 
Notations (20.2.34.3) [Global Fields]. For a global field $F$,

- Use $\text{GField}$ to denote the set of global fields. Use $\text{FField}$ to denote the set of global function fields, use $\text{NField}$ to denote the set of global number fields. $\text{GField}/F$ is the set of global fields over $F$.
- $O_F$ is the ring of integers of $F$.
- $\Sigma_F$ is the set of places of $F$. $\Sigma^\text{fin}_F$ is the set of finite places of $F$, $\Sigma^\infty_F$ is the set of infinite places of $F$. $\Sigma^R_F$ is the set of real places of $F$, $\Sigma^C_F$ is the set of complex places of $F$.
- For a finite extension $L/F$ and $v \in \Sigma^\text{fin}_F$, $\Sigma^v_L$ is the set of finite places over $v$.
- For $x \in O_F$, let $S(x) \subset \Sigma^\text{fin}_F$ denote the set of finite places dividing $x$.
- For $v \in \Sigma^\text{fin}_F$, $(R_v, m_v, k_v)$ is the valuation ring of $v$, and $||v|| = \# k_v$.

Notations (20.2.34.4) [Local Fields].

- Use $\text{LField}$ to denote the set of local fields. Use $p - \text{LField}$ to denote the set of $p$-adic local fields. Use $p - \text{FField}$ to denote the set of $p$-adic number fields. Use $p - \text{NField}$ to denote the set of $p$-adic number fields. Use $\text{AField}$ to denote the set $\{\mathbb{R}, \mathbb{C}\}$.

35 Number Theory

Notations (20.2.35.1) [Numbers].

- $\pi$ represents the smallest $x \in \mathbb{R}_+$ s.t. $e^{ix} + 1 = 0$.

Notations (20.2.35.2) [Analysis on Adeles and Ideles].

- For a local field $K$, $V \in \text{Vect}/K$, $\mathcal{S}(V)$ is the space of Bruhat-Schwartz Functions on $V$.
- For a global field $F$, $V$ a finite free module over $A_F$, $\mathcal{S}(V)$ is the space of Bruhat-Schwartz functions on $V$.

Notations (20.2.35.3) [L-Functions].

- Use $L$-functions instead of $L$-functions.

36 Representation Theory

Notations (20.2.36.1) [Representations]. Let $G \in \text{TopGrp}$, $L \in \text{TopCAlg}$,

- $\text{Rep}_L(G)$ is the category of continuous representations of $G$ with coefficients in $L$. $\text{Rep}_C(G)$ is also denoted by $\text{Rep}(G)$.
- $\text{Irr}_L(G)$ is the category of irreducible representations of $G$ with coefficients in $L$. $\text{Irr}_C(G)$ is also denoted by $\text{Irr}(G)$.
- $\text{Rep}^{\text{alg}}_L(G)$ is the category of smooth complex representations of $G$. $\text{Irr}^{\text{alg}}_C(G)$ is the category of irreducible smooth complex representations of $G$.
- For $(\rho, V) \in \text{Rep}^{\text{alg}}_L(G)$, let $(\rho^\vee, V^\vee)$ denote the contragradient representation: $\rho^\vee(g) = \rho(g)^{-t}$.

37 Analysis

Notations (20.2.37.1) [Real Analysis].

- $\sqrt{-} : \mathbb{R}_+ \to \mathbb{R}_+$ is inverse of the function $\mathbb{R}_+ \to \mathbb{R}_+: x \mapsto x^2$. 
• For a differentiable function \( f \), write \( f' \) instead of \( f' \) to denote the derivative of \( f \). For \( p \in \mathbb{Z}_+ \) and a \( p \)-th differentiable function \( f \), write \( f^{(p)} \) to denote the \( p \)-th derivative of \( f \).

Notations (20.2.37.2) [Special Functions].

•

38 Geometry

Notations (20.2.38.1) [Manifolds].

•

39 Combinatorics

Notations (20.2.39.1) [Combinatorics Numbers].

• For \( n, m \in \mathbb{N}, m \leq n \),

\[
\begin{align*}
n! &= \begin{cases} 1, & n = 0 \\ \prod_{k=1}^{n} k, & n > 0 \end{cases}, \quad \binom{n}{m} = \frac{n!}{(n-m)!m!} \\
\end{align*}
\]

• For \( n, m \in \mathbb{N}, m \leq n \) and \( p, q \in p^{\mathbb{Z}^+} \),

\[
\begin{align*}
[n]_p &= \begin{cases} 1, & n = 0 \\ \frac{q^n - 1}{q - 1}, & n > 0 \end{cases}, \\
[n]_q &= \begin{cases} 1, & n = 0 \\ \prod_{k=1}^{n} [k]_q, & n > 0 \end{cases}, \\
\left[ \begin{array}{c} n \\ m \end{array} \right] &= \frac{[n]_q}{[n-m]!_q[m]!_q} \\
\end{align*}
\]
Bibliography


[Ahl79] Lars V. Ahlfors, Complex Analysis.


[B-Z76] I. N.Bernshtein and A. V. Zelevinskii, Representations of the Group $GL(n, F)$ where $F$ is a Non-Archimedean Local Field.


[Cog00] J. W. Cogdell, Notes on L-Functions for $GL_n$. 


[D-S16] Fred Diamond and Jerry Shurman, A first course in Modular Forms.


[Fu11] Lei Fu, Étale Cohomology Theory.


[Har77] Hartshorne, Algebraic Geometry.

[Hat02] Allen Hatcher, Algebraic Topology.


[Hum90] James Humphreys, Reflection Groups and Coxeter Groups.


[Huy05] Daniel Huybrechts, Complex Geometry, An Introduction.

[Huy16] Daniel Huybrechts, Lectures on K3 Surfaces.


[Kle05] Steven L. Kleinman, The Picard Scheme.


[Kos97] B. Kostant, Clifford Algebra Analogue of the Hopf-Koszul-Samelson Proposition, the $\rho$-Decomposition, $C(g) = \text{End}_\rho \otimes C(P)$, and the g-Module Structure of $\wedge g$, Adv. in Math., 125(1997), 275-350.

[Lam05] T.Y. Lam, Introduction to Quadratic Forms over Fields.

[Lan05] Serge Lang, Algebra.


[Mil17c] J. S. Milne, Modular Functions and Modular Forms.


[Mil20b] J. S. Milne, Complex Multiplication, Version 0.10.

[M-S74] John W. Milnor and James D. Stasheff, Characteristic Classes.

[Mor19] Sophie Morel, Adic Spaces.


[Mun00] Munkres, Topology.


[Nit05] Nitin Nitsure, Construction of Hilbert and Quot Schemes.

[Ols16] Martin Olsson, Algebraic Spaces and Stacks.


[P-R94] Vladimir Platonov and Andrei Rapinchuk, Algebraic Groups and Number Theory.


[R-V99] Dinakar Ramakrishna and Robert J. Valenza, Fourier Analysis on Number Fields.


[Sen80] Sharker Sen, Continuous Cohomology and $p$-adic Cohomologies.


[Vis08] Angelo Vistoli, Notes on Grothendieck Topologies, Fibered Categories and Descent Theory.


[Yao17] Zijian Yao, Notes on the Local Langlands Program for $GL_n$.


1694 BIBLIOGRAPHY

[Zin84] Zink, Cartier Theory of Commutative Formal Groups.

MORE TO BE ADDED

References are https://math.mit.edu/~zzyzhang/list.html.

Articles

2010-2014


M. Emerton, Completed cohomology and the p-adic Langlands program, Proceedings of the ICM 2014.


M. Harris, Automorphic Galois representations and the cohomology of Shimura varieties, Proceedings of the ICM 2014.


V. Lafforgue, Introduction to ch'toucas for reductive groups and to the global Langlands parameterization, Arxiv 2014.


R. Kottwitz, B(G) for all local and global fields, Arxiv 2014.


Y. Liu, Relative trace formulae toward Bessel and Fourier-Jacobi periods of unitary groups, Manuscripta Mathematica, 145 (2014), 1-69.


S. Lysenko, Geometric Waldspurger periods II, Arxiv 2013.


O. Lorscheid, Algebraic groups over the field with one element, Mathematische Zeitschrift volume 271, pages 117-138.

David Lawrence Roe, The local langlands correspondence for tamely ramified groups, ProQuest LLC, Ann Arbor, MI, 2011. Thesis (Ph.D.) 鈥橈rvard University. MR2898606


2000s


M. Kisin. 鈥淒rystalline representations and F-crystals-. In: Algebraic geometry and number theory. Springer, 2006, pp. 459-496.


T. Konno, A note on the Langlands classification and irreducibility of induced representations of p-adic groups, Kyushu J. Math. 57 (2003), no. 2, 383-409,


S 酵ren Have Hansen, Picard groups of Deligne-Lusztig varieties 鈥椕 ith a view toward higher codimensions, Beitr 鈥椕 age Algebra Geom. 43 (2002), no. 1, 9-26. MR1913766


T. J. Haines and Ngo Bao Chau, Alcoves associated to special fibers of local models, Amer. J. Math. 124 (2002), no. 6, 1125-1152. MR 1939783


1990s


H. Stamm, On the reduction of the Hilbert-Blumenthal moduli scheme with $\Gamma_0(p)$ level structure, Forum Mathematicum 9 (1997), 405-455.
J. P. Serre, Two letters on quaternions and modular forms (mod p), Israel J. Math. 95 (1996), 281-299.
Arxiv Mathematics (since February 1992)


1970-1980s


N. Elkies, The existence of infinitely many supersingular primes for every elliptic curve over \( \mathbb{Q} \), Inventiones Mathematicae, 89 (3) (1987), 561-567.


A. Borel, Admissible representations of a semi-simple group over a local field with vectors fixed under an Iwahori subgroup, Invent. Math. 35 (1976), 233-259.


1950-1970


Classical books

N. Chriss, V. Ginzburg, Representation theory and complex geometry, 1997.
Casselman, note on p-adic groups, 1995.
V. Platonov, A. Rapinchuk, Algebraic groups and number theory, (1994).
S. Mac Lane, I. Moerdijk, Sheaves in Geometry and Logic - A first introduction to topos theory, Springer Verlag, 1992.

D. A. Cox, Primes of the form $x^2 + ny^2$, (1989).
A. Borel, W. Casselman (Editors), Automorphic Forms, Representations and L-Functions, Parts 1 and 2, Corvallis proceedings (1979).
D. Quillen, homology of commutative rings, unpublished, MIT 1968.
Flatland: A Romance of Many Dimensions, (1884).
Index

(−1)-curve, 715, 1251
(−2)-truncated, 360
(2, 1)-category, 176
(g, K)-module, 1480
(φ, Γ)-module, 1338
(n, ε)-separated, 1038
(n, ε)-spanning, 1038
2-commutative diagram, 176
2-fibered product, 176
2-morphism of topoi, 496
A-algebra extension, 865
A-antisymmetric, 964
A-definable, 16
A-order, 401
A-torsor, 888
B-admissible, 1340, 1348
B-ring, 1137
B*-algebra, 980
E-sheaves, 735
E-valued (p, q)-forms, 1061
F-crystal, 749
G-equivariant object, 185
G-ringed K-space, 1360
G-space, 492
G-unramified, 439
G_K-regular, 1341
H-projective, 581
H-quasi-projective, 582
I-adic completion, 383
I-adically complete, 383
I-completely
   (faithfully)flat/smooth/étale/..., 469
I-completely flat, 859
I-completely regular, 859
I-torsion, 462
K-finite vectors, 1013

K-flat, 543
K/k-image, 1313
K/k-trace, 1313
K_0-group, 201
M-Koszul-regular, 432
M-bounded, 1210
M-quasi-regular sequence, 407
R-fundamental class, 305
R-invariant, 852
R-orbit, 852
R-orientation, 305
S-adeles, 1161
S-birational, 533
S-dense, 532
S-ideles, 1162
S-rational map, 533
S-torsion-free, 364
U-limit, 246
X_n-distinguished of order s, 902
X_n-distinguished of order s at x, 905
J-free, 175
$\delta$-enriched model category, 262
Γ(N)-structure, 1290
Γ_0(N)-structure, 1290
Γ_1(N)-structure, 1290
Γ_K-conjugate, 1448
Λ-formal functor, 833
Λ-formal group, 833
Λ-formal scheme, 833
Ω-Spectrum, 311
α-limit points, 1035
δ-functor, 212
δ-pairs, 454
δ-ring, 454
$\ell$-adic cohomological dimension, 727
$\ell^\infty$-Selmer group, 1240
(weakly)admissible pair, 1373
(weakly)initial, 167
etale, 1337, 1403
étale cohomology group, 720
étale cohomology with compact support, 731
étale fundamental group, 720
étale morphism, 621
étale site, 504
étale topology, 504
étale, 441, 442
Čech cohomology, 539
Čech complex, 539

Abel-Jacobi map, 1123
Abelian, 31
Abelian category, 201
Abelian scheme, 1221
Abelian variety, 1221
Abelianization, 33
absolute Frobenius, 534
absolute prismatic site, 758
absolute ramification index, 449
absolutely algebraically closed, 896
absolutely continuous, 927
absolutely unramified, 449
absorbing set, 959
abstract measure, 12
active, 350
acyclic complex of $M$, 353
Adam operators, 647
addition of ordinals, 7
additive, 197
additive category, 198
additive Herbrand quotient, 209
additive reduction, 1268
adelic group, 1161
adelic automorphic forms, 1545
adelic group of $G$, 1217
Adelic Tate module, 1231
adic completion, 895
adic morphism, 908
adic point, 1384
adic ring, 894
adic spaces, 1391
adic spectrum, 1382
adjoint group, 1089
adjoint Lie group, 1107
adjunction pair, 168
admissible, 325, 896, 1481
admissible $\mathcal{H}$-module, 103
admissible covers, 492
admissible epimorphism, 199
admissible modulus, 1195
admissible monomorphism, 199
admissible opens, 492
admissible representation, 1483, 1545
admissible rings, 1369
admissible smooth representation, 1455
admissible topology, 243
affine connection, 1063
affine formal scheme, 1369
affine local, 557
affine scheme, 529
affinoid $K$-algebra, 921
affinoid $K$-space associated to $A$, 1353
affinoid (Tate) algebras, 903
affinoid adic spaces, 1391
affinoid covering, 1355
affinoid generator, 905
affinoid perfectoid space, 1398
affinoid subdomain, 1353
Affinoid Tate ring, 908
Albanese map, 1123
Albanese variety, 1123
alephs, 8
algebra, 58
algebra of subsets, 923
algebra over a monad, 189
algebraic analytic space, 1114
algebraic closure, 61
algebraic cycle, 692
algebraic de Rham cohomology, 717
algebraic dimension, 1109
algebraic extension, 60
algebraic family of varieties parametrized by $T$, 610
algebraic function, 1201
algebraic group of EL type, 1377
algebraic group of multiplicative type, 805
algebraic group of PEL type, 1377
algebraic integer, 1157
algebraic space, 850
algebraic stack, 851
algebraically admissible, 1401
algebraically equivalent, 712
algebraically prime models, 23
almost étale, 487
almost commutative algebras, 484
almost complex manifold, 1110
almost complex structure, 1110
almost elements, 485
almost everywhere convergence, 924
almost finitely generated, 485
almost finitely presented, 485
almost flat, 485
almost integral, 379
almost modular forms, 1573
almost perfect, 485
almost periodic, 1035
almost projective, 485
almost uniform convergence, 924
almost XXX, 485
almost zero, 485
almost-simple algebraic group, 811
alteration, 580
alternating Čech complex, 540
amalgamated sum, 1138
ample holomorphism line bundle, 1127
ample invertible sheaf, 600
amplitude character, 815
amplitude function, 1029
analytic, 913, 934, 1395
analytic adic point, 1384
analytic group, 1090
analytic module, 1111
analytic Picard group, 1112
analytic point, 913, 1395
analytic space, 1111
analytic space of $\mathbb{C}^n$, 1111
analytic subvariety, 1111
analytification of $\mathcal{F}$, 1115
analytification of $X$, 1114
AND gate, 1656
André-Quillen cohomology, 862
André-Quillen homology, 862
anisotropic, 1172
annihilating ideal, 592
annihilator, 75
anodyne, 339
anti-affine algebraic group, 789
anti-symmetrized tensors, 86
antichain, 11
approaches, 230
approximate identity, 997, 1020
Arakelov heights, 1207
arc-topology, 508
Archimedean, 899
Arin-Rees category, 734
arithmetic Frobenius, 534
arithmetic genus, 631
arithmetic monodromy group, 1300
arithmetic point, 661
arithmetic subgroup, 1220
arithmetic surface, 1251
Aronszajn tree, 12
Artin conductor, 1333, 1635
Artin L-function, 1634
Artin reciprocity map, 1187, 1191
Artin symbol, 1197
Artin-Hasse exponential, 822, 1409
Artin-Rees $I$-adic, 734
Artin-Rees category of $\Lambda$-sheaves, 734
Artin-Schreier exact sequence, 725
Artin-Schreier extension, 68
Artin-Schreier sheaf, 1308
Artinian, 203, 370
Artinian Abelian category, 203
associated $G$-bundle with fiber $F$, 323
associated category fibered in groupoids, 186
associated point of $X$, 533
associated points, 587
associated primes, 391
associated to $\mathcal{F}$, 533
associative H-space, 302
associative operator, 31
atlas for the algebraic space $\mathcal{F}$, 850
atlas for the algebraic stack $X$, 851
atom, 923
atomic diagrams, 21
atomic formula, 15
augmentation, 336
automorphic cuspidal representation, 1545
automorphic forms, 1497
automorphic functions, 1499
automorphic L-period map, 1640
automorphic representation, 1545
Azumaya algebra, 99, 870
Azumaya Brauer group, 870

Bézout domain, 54
baby Monster group, 44
Baer-Specker group, 34
Baire space, 251
balanced, 954
balanced $\Gamma_1(N)$-structure, 1290
bald, 1137
Banach algebra, 957
Banach space, 957
base, 146
basepoint free, 598
basis, 73
belong to $\mathcal{T}$, 492
Bergman metric, 1131
Bernoulli numbers, 944
Bessel function, 952
Betti cohomology, 1114
bi-exact bifunctor, 212
bialgebra, 158
bicommutant, 982
bicommutatant, 92
big affine étale site, 504
big affine smooth site, 505
big affine Zariski site, 503, 506
big pro-étale site, 1433
big smooth site, 505
big Zariski site, 506
big-crystalline site, 742
binary operator, 31
birational, 532
bivariate class $c$, 698
Bloch-Wigner dilogarithm, 1649
blowing up, 641
Boolean algebra, 14
Boolean connectives, 14
Boolean function, 1656
bordism group, 333
Borel measure, 924
Borel pair, 809
borel subalgebra, 125
Borel subgroup, 809

bound, 15
boundary map, 295
bounded, 894
bounded $f$-torsion, 462
bounded above, 230
bounded below, 230
bounded prism, 750
bounded symmetric domain, 1131
Braid group, 39
branch, 11
Brauer group, 870, 874
Breuil-Kisin twist, 760
Bruhat-Tits building, 1477

canonical height, 1271
canonical height pairing, 1271
canonical heights, 1206
canonical map, 680
canonical sheaf, 662
canonical topology, 494, 1353
canonical truncation, 206
CAP representations, 1554
cardinal number, 2
Cartan involution, 817
Cartan matrix, 148
Cartan subalgebra, 117
Cartan subgroup, 809
Cartan-Eilenberg resolution, 210
Cartesian arrow, 184
Cartesian closed, 177
Cartesian fibration, 349
Cartesian monoidal structure, 176
Cartier divisor, 1391
Cartier divisor group, 639
Cartier dual, 784
Casimir element, 136, 138
Casimir operator, 138
Casselman basis, 1536
Cassels-Tate pairing, 1240
Casson invariant, 1080
categorical equivalence, 344
categorical fibrations, 348
categorical quotient, 173
category, 165
category (co)fibered in
groupoids/sets/equivalence relations,
category of descent datum, 498
catenary, 274, 386
catenary scheme, 560
Cauchy filter, 251
Cayley transformation, 85
cellular homology groups, 299
cellular homotopy, 282
cellular map, 282
center, 109
central $k$-algebra, 99
central character, 1595
central series, 41
central value, 1604
central/multiplicative isogeny, 794
chain complex, 205
chain equivalent, 1174
character, 780, 1014, 1442, 1456
character of $G$, 1004
characteristic class, 327
Chern character, 704
Chern class, 1058
Chern classes, 330, 703
Chern connection, 1113
Chern polynomials, 52
Chern-Weil, 1058
Chevalley group, 1469
choice function, 9
Chow cohomology group, 699
Chow group, 773
Chow group of $k$-cycles, 695
Chow group of codimension $p$ cycle, 696
Chow motives, 772
Chow ring of $X$, 708
Christoffel symbol, 1064
class formation, 1184
class function, 1015
class group, 397
classifying space, 323, 324
cleavage, 184
closed, 177, 955
closed Cartier divisor, 1392
closed Hurewicz cofibration, 290
closed immersion, 528, 574, 1357, 1365
closed immersion defined $I$, 529
closed subfunctor, 836
closed subscheme, 574
CM-algebra, 1280
CM-field, 1280
CM-pair, 1280
CM-type, 1280, 1285
CNOT gate, 1657
coa-action, 159
co-module, 159
coalgebra, 158
coCartesian arrow, 184
coCartesian fibration, 349
cocommutative, 158
cocontinuous functor, 491
code, 1040
codimension, 273
coen, 174
cofibered category, 184
cofibrantly generated model category, 260
cofibration, 289, 339
cofibrations, 254
cofinal, 11
cofinality, 3
Cohen-Macaulay ring, 408
Cohen-Macaulay scheme, 560
coherator, 647
coherent sheaf, 520
coherentor, 205
cohomological dimension, 727, 883
cohomological dimension bounded by $N$, 220
cohomological operator, 300
cohomology of $F$ with supports in $Z$, 725
cohomology ring of $X$, 770
cimage, 197
coinduced module, 58
cokernel, 197
cokernel Hopf algebra, 162
combinatorial model category, 260
comma category, 167
commutative, 233
commutative group scheme, 777
commutative ring, 48
commutator, 982
compact, 203, 237, 816
compact dimension, 555
compact generating functor, 241
compact Lie algebra, 125
compact object, 198
compact operator, 969
compact planar gluing diagram, 252
compact real algebraic group, 815
compact representation, 1460
compact symplectic group, 1099
compact-open topology, 241
compactly generated space, 241
compactly generated triangulated category, 217
compactly induced representation, 1457
compactly supported smooth functions, 1544
companion matrix, 77
compatible, 4
compatifications of $X/S$, 643
complementary series representations, 1541
complete, 5, 17, 37, 230, 908
complete intersection, 623
complete intersection local ring, 434
complete linear series, 599
complete tensor product, 895
complete uniform space, 251
completed Artin $L$-function, 1634
completed de Rham complex, 760
completed $L$-function, 1635
completed residue field, 1383
completed tensor product, 1138
completion, 5
completion curve, 667
completion/Henselization/Zariski localization, 910
complex inner space, 81
complex manifold, 1109
complex measure, 923
complex multiplication, 1284
complex part, 933
complex places, 1156
complex reductive Lie group, 818
complex torus, 1121
component group of $A$, 1248
composite homotopy, 279
composite series, 41
composition law, 165
composition of correspondences, 767
composition series of $G$, 794
condensed objects, 891
condition of moderate growth, 1497
conductor, 1188, 1513
conductor of $\alpha$, 398
conductor of $E$, 1236, 1237
conductor of $L/F$, 1196
conductor of $R$, 397
cone, 280
cone over $X$, 234
congruence subgroup, 1219, 1555
conjugate, 1072
Conne complex, 353
Conne cyclic category, 351
Conne double complex, 353
connected, 235, 493
connected complex reductive Lie group, 818
connected component, 236
connected Shimura datum, 1318
connected Shimura variety attached to $(G, D)$, 1319
connected Shimura variety relative to $(G, D)$, 1319
connected sum, 306
connection, 716
conormal sheaf, 605
consistent, 17
constant sheaf, 495
constant symbol, 14
constructible, 269, 271
constructible $m$-adic sheaf, 734
constructible étale sheaf, 728
constructible topology, 271
continued fraction, 1673
continuous functor, 491
contractible, 279
cotragradient, 103, 1546
cotragradient $(g, K)$-module, 1481
cotragradient smooth representation, 1444
cotrivialant cofibration, 346
cotrivialant equivalence, 346
cotrivialant fibration, 346
cotrivialant functor, 166
cotrivialant model structure, 346
converge, 942
converge absolutely, 942
convergence in measure, 924
converges, 230, 235
convex subgroup, 69
convolution, 995, 1019
convolution distribution, 1020
coprimary, 393
COPY gate, 1656
corestriction, 878
correspondences, 767
correspondence, 359
cosimplicial object, 336
cosmooth $C^\infty$ $(X)$-module, 1450
cotangent bundle, 1050
cotangent complex, 862
cotensored, 180
countable, 2
course quotient for $R$, 852
course quotient in schemes for $R$, 852
covariant cofibration, 345
covariant equivalence, 345
covering space, 316
covering space action, 268
coverings, 491
cowedge, 174
coxeter graph, 148
Coxeter root, 152
critical, 1048
critical point for $L(s)$, 1604
critical value, 1604
cross product map, 300
cross ratio, 933
crystal, 744
crystal in finite locally free modules, 745
crystal in quasi-coherent modules, 744
crystalline prism, 750
crystalline representations, 1348
crystalline site, 742
cup product map, 300
curvature, 1065
curve, 660
cusp, 679, 1497
 cusps, 1545
cuspidal, 1498, 1499, 1544
cuspidal representation, 1520
cuspidal supports, 1528
cut, 5
CW approximation, 289
CW complex, 281
CW complex of finite dimension, 281
CW complex of finite type, 281
cycle class maps, 770
Cyclic Homotopy Group, 353
cyclic object, 351
cyclotomic character, 1331
cylinder object, 255
de Rham complex, 744
decay rapidly, 1499
decidable, 17
decomposed generically, 1336
decomposition field, 1148
decomposition group, 1148
Dedekind cut, 5
Dedekind domain, 396
Dedekind eta function, 825
Dedekind scheme, 562
Dedekind zeta function, 1608
Dedekind-finite, 48
definable, 16
definable subsets, 29
definably arcwise connected, 28
definably connected, 28
definably interpreted, 16
deformation retraction, 279
degenerate, 1137
degenerate complex, 855
degenerate correspondences, 769
degree, 632, 672
degree of $A$, 870
degree of $L$, 1654
degree of $\pi$ at $p$, 572
degree of $D$, 672
degree of $f$, 574, 1054
degree of a locally free sheaf, 673
degree of a zero cycle, 696
degrees of $\alpha$, 769
Dehn invariant, 1666
Deligne-Fourier transform, 1308
Deligne-Lustig Induction map, 1470
Deligne-Mumford stack, 851
Deligne-Weil representations, 1333
dense, 4, 13
def Rham representations, 1348
derivation, 427
derivative transformation, 1041
derived $I$-completion, 468
derived category, 218
derived category of Frobenius $B$-modules, 766
derived colimit, 229
derived complete, 466
derived de Rham cohomology, 766
derived limit, 229
derived pullback, 545
derived series, 110
derived tensor product, 544
desingularization, 659
destabilization, 193
determinant, 87
determinential $\iota$-weights, 1296
Deuring normal form, 1260
Deutsch-Jozsa algorithm, 1658
Deutsch-Jozsa problem, 1658
devided power structure, 473
dg-category, 233
diagonal group, 814
diagonalizable, 803, 1464
diamond, 1425, 1435
different of $f$, 656
different of $K/L$, 399
differentiable singular cohomology, 554
differential graded singular algebra, 233
differential module, 233
differentiation, 1019
dihedral Weil representation, 1335
dimension, 73, 385, 833
dimension function, 274
dinatural transformation, 174
Dirac sequence, 991
direct image, 526
direct sum, 197
direct sum dévissage, 59
directed set, 4
Dirichlet character modulo $m$, 1614
Dirichlet density, 1198
Dirichlet $L$-function, 1616
discrete, 205, 219
discrete series, 1487
discrete topology, 491
discrete valuation ring, 898
discriminant function, 1571
discriminant of $E$, 1256
discriminant of $f$, 655
discriminant of $L/K$, 400
discriminant of the basis, 65
dissection of a polytope $P$, 1665
distal, 1037
distinguished element, 457
distribution, 1449
distributions, 1019
distributions on $\mathcal{F}$, 1449
divergence, 1067
divided power ring, 473
division ring, 49
divisor, 1413
divisor functor, 843
divisor-stable, 449
Dolbeault cohomology group, 1113
domain, 48
dominant map, 570
dominates, 896
Donaldson invariants, 1081
double complex, 206
doubly periodic w.r.t. $\Lambda$, 950
Drinfeld curve, 1475
dual Abelian scheme, 1246
dual Abelian variety, 1225
dual basis, 75
dual category, 165
dual complex, 464
dual complex torus, 1122
dual Coxeter number, 152
dual group, 1004
dual lattice, 1156
dual measure, 1006
dual module, 399
dual of Hopf bundle, 322
dual representation, 137
dual segment, 1517
dual space, 75, 1004
dual system, 145
dual variety, 618
dualizing complex, 472, 650, 654
dualizing module, 472
Dynkin diagram, 150
Earring group, 38
edge morphisms, 230
edges, 1663
effaceable \(\delta\)-functor, 224
effective, 1338
effective Chow motives, 772
effective Grothendieck motives, 772 
Eilenberg-Maclane space, 312 
Eilenberg-Steenrod homology theory, 295
Eisenstein integers, 1158
Eisenstein manifold, 1069
Eisenstein polynomial, 1147
Eisenstein series, 1569
Eisenstein series of mixed type, 1620
Eisenstein series of weight \(k\), 1569
elementary automorphisms, 109
elementary class, 15
elementary diagrams, 21
elementary embedding, 21
elementary equivalent, 15
elementary matrix, 77
elementary polynomials, 52
elementary row operation, 77
elliptic, 1029, 1495
elliptic curve, 1256
elliptic dilogarithm, 1650
elliptic point, 1556
elliptic regulator, 1271
elliptic scheme, 1256
embedded Lie subgroup, 1087
embedded point, 587
embedded prime, 392
embedded submanifold, 1047
embedding of algebraic groups, 793
empty set, 1
end, 174
energy, 1072
enriched category, 180
epimorphism, 167
equicontinuous, 1037
equivalence, 166, 233, 264, 356
equivalence relation, 167
equivalence relation on \(X_0\), 167
equivalent, 78, 182
equivalent objects, 165
equivariant sheaf, 1443
ergodic, 1042
essential, 203
essential singularity, 939
essentially small, 13
essentially square-integrable, 1539
essentially surjective functor, 166
essentially tempered representation, 1540
Euler character, 308
Euler characteristic, 630, 708
Euler class, 1058
Euler classes, 329
Euler function, 1673
even, 1584
even/odd line bundle, 1223
exact, 212, 362
exact category, 199
exact functor, 170
exact sequence, 197
excellent model category, 264
excellent ring, 416
exceptional divisor, 641, 642, 1251
excisive triad, 279
exhaustive, 230
expansive, 1036
expansiveness constant, 1036
exponent, 1167
exponential map, 1085
exponential period number, 1202
exponentiation, 3
exponentiation of ordinals, 7
exponents of \(g\), 116
ext groups, 226
extended Period ring, 1201
extension by zero, 518
extension functor of sheaves, 498
extension of valuation rings, 897
exterior algebra, 365
exterior product, 365
exterior product map, 707
exterior square L-functions, 1618
extremally disconnected, 237
F-space, 954
factorial scheme, 562
faithful, 92
faithful representation, 1462
faithfully flat, 419
faithfully normed, 1138
Faltings height, 1321
family of effective epimorphisms, 494
family of quotients of $\mathcal{E}$ parametrized by $T$, 838
family of universal effective epimorphisms, 494
Fano variety, 666
Fargues-Fontaine curve, 1409
fast Fourier transform algorithm, 1658
fat subfunctor, 837
fiber bundle, 314
fiber functor, 179, 196
fiber homotopic, 279
fiber homotopy equivalence, 279
fibered category, 184
fibered presurface, 1249
fibrations, 254
field, 48
field formation, 1184
field of moduli, 1224
filter, 10
filtered $(\varphi,N,\text{Gal}(L/K))$-module, 1340
filtered $\varphi$-modules (isocrystals), 1340
filtered category, 166
filtration, 189
final object, 166, 167, 176
finite, 2, 571
finite $I$-completely Tor amplitude, 469
finite $R$-module, 56
finite étale, 1403
finite étale sheaf, 728
finite adeles, 1161
finite continued fraction, 1673
finite CW complex, 281
finite group of Lie type, 1469
finite group scheme, 783
finite ideles, 1162
finite injective dimension, 210, 228
finite intersection property, 10
finite locally free group scheme, 783
finite locally free of rank $d$, 611
finite places, 1156
finite type, 519, 570
finite type, of finite presentation, coherence, 1363
finitely generated, 203
finitely presented module, 414
first category, 251
first Chern class, 700
first Chern class map, 331
first order logic, 15
First Variation of Energy, 1072
fitting ideal, 589
Fitting ideal of $A$, 373
fixed subscheme, 797
fixed subspace, 1463
flag Variety, 1092
flag variety, 800
flask sheaf, 550
flat, 419, 519, 1065
flat dimension, 405
flat morphism, 519
flat sections, 1531
Floer homology, 1081
flow, 1055
Fontaine’s functor, 447
Fontaine’s ring, 447
forest, 1663
formal $R$-model, 1371
formal $R$-module, 825
formal adjoint, 980
formal completion, 833, 1369
formal curve, 823
formal differential forms, 1110
formal differential operator, 823
formal exponential, 821
formal group, 831
formal group law, 825
formal Lie group, 833
formal logarithm, 821, 829
formal power exponential, 829
formal product, 820
formal schemes, 1369
formal sum, 820
formally étale, 440
formally smooth, 434
formally unramified, 439
formally unramified/smooth/étale, 658
Fourier transform, 1005, 1020
Fourier transformation, 1022
Fourier-Whittaker coefficients, 1552
fppf topology, 506
fpqc topology, 506
Fréchet space, 954
fractional ideal, 396
fractional part of $\alpha$, 1671
Fredholm operator, 973
Fredkin gate, 1657
free, 857
free $\delta$-ring, 456
free group, 37
free Lie algebra, 135
free pd-algebra, 475
free resolution, 858
free variable in a formula, 15
Frey curve, 1647
Frobenius action on compact étale cohomologies, 730
Frobenius fixed pts, 766
Fubini-Study metric, 1117
full subcategory, 167
full/faithful functor, 166
function field, 1156
function field of $X$, 559
function symbol, 14
functor, 165
functorial lifting, 1577
fundamental class, 1184
fundamental class of $X$, 696
fundamental domain, 997
fundamental homology class mod 2, 307
fundamental representation, 1594
fundamental solution, 1028
G-ring, 416
GAGA functor, 1361
Galois closure, 66
Galois cover, 719
Galois field extension, 66
Galois symbol map, 157
Gamma function, 951
gap, 5
gap sequence, 684
Gauss sum, 1614
Gauss transformation, 1674
Gaussian integers, 1158
general linear group, 814, 1096
general symplectic group, 814
generalization of $x$, 271
generalized Hodge-Tate weights, 1347
generalized $L$-function, 1295
generated subgroup scheme, 778
generator of $\mathcal{D}$, 217
generic, 1407
generic fiber, 532
generic fiber functor, 190
generic representation, 1521
generically finite morphism, 573
geodesic equations, 1064
Geodesic flow, 1070
geometric exact category, 199
geometric Frobenius, 534
geometric genus, 663
geometric irreducible/semisimple, 1293
geometric monodromy group, 1300
geometric point, 661
geometric quotient, 853
geometric structure, 200
geometrically (almost-)simple algebraic group, 811
geometrically conjugate, 1470
geometrically integral/reduced/separated/irreducible..., 562
geometrically irreducible/semisimple, 736
geometrically reduced/integral/connected..., 413
geometrically regular, 413, 562
geremetrization, 338
gerbe, 503
ghost components, 450
global $\varepsilon$-factor, 1613
global canonical character, 1168
global field, 1156
global Hecke algebra, 1546
global Hecke $L$-function, 1613
global intersection, 433
global section, 535
global section functor, 598
global zeta function, 1608
glueable module, 427
gluing pair, 427
going-down property, 271
going-up property, 271
good, 1414
good cylinder object, 255
good quotient, 852
good reduction, 1254, 1267
Goodstein sequence, 8
Gorenstein, 408
graded module, 379
graded ring, 379
gradient, 1067
Gram matrix, 86
graph, 1663
Grassmannian, 283
Grassmannian manifold, 1092
Grassmannian variety, 800
greatest lower bound property, 4
Gromov-Hausdorff metric, 270
Grothendieck Abelian category, 204
Grothendieck correspondences, 767
Grothendieck group, 646
Grothendieck group of $k$-cycles, 711
Grothendieck group of coherent sheaves, 646
Grothendieck motives, 772
Grothendieck ring of $X$, 711
Grothendieck-Witt ring, 1175
group algebraic space, 852
group cohomology, 877
group formation, 189
group of Adele points of $G$, 1217
group of compact type, 1216
group schemes, 777
group variety, 791
group-like, 158
group-like element, 162
groupoid, 166
Gyn map, 697
Gysin homomorphism, 697
H-space, 302
H-very ample, 602
Haar measure, 992
Hadamard gate, 1657
halting computation, 14
Hankel determinants, 822
happy family, 44
Hauptmodul, 1559
Harder-Narasimhan category, 193
Harder-Narasimhan filtration, 192, 194
Harder-Narasimhan formalism, 190
Harish-Chandra module, 1483
harmonic, 947
harmonic Maass form, 1505, 1507
Hartogs number, 8
Hattoris-Stallings trace, 717
Hauptmodul, 1557
Hausdorff, 230
Hausdorff distance, 270
have order $n$, 657
heart, 362
Hecke algebra, 1454, 1490, 1560
Hecke character, 1162
Hecke eigenforms, 1562
Heegner condition, 1637
Heegner point, 1637
Heegner point of $E$, 1637
height, 11, 69, 385, 1338
height of $L$, 1654
height of formal group law, 832
height of homomorphism, 832
height of roots, 147
Heine-Borel, 954
Heisenberg group, 1585
Henselian, 417, 908
Henselian pair, 418
Henselian valued field, 1140
Herbrand function, 1150
Hermitian, 981
Hermitian form, 81
Hermitian manifold, 1112
Hermitian matrix, 86
Hermitian metric, 1112
Hermitian space, 85
Hermitian symmetric domain, 1131
Hermitian symmetric space, 1130
Hermitian transpose, 85
Hermitian vector bundle, 1111
Hessian, 1067
higher block presentation, 1040
higher direct image with compact support, 731
highest weight representation, 1592
highest weight vector, 1592
Hilbert basis, 958
Hilbert class field, 1195
Hilbert class field tower, 1196
Hilbert functor, 838
Hilbert Polynomial, 382
Hilbert polynomial, 631, 632
Hilbert scheme, 679
Hilbert symbol, 1178
Hilbert-Schmidt, 986
Hilbert-Schmidt inner product, 987
Hochschild complex, 351
Hochschild complex of $M$, 353
Hochschild homology group, 351
Hochschild-Mostow group, 1467
Hodge classes, 1327
Hodge cohomology, 717
Hodge cycle, 1327
Hodge manifold, 1129
Hodge-Tate complex, 758
Hodge-Tate degree, 191
Hodge-Tate representation, 1347
Hodge-Tate weight, 1338
holomorphic, 934, 953
holomorphic cotangent bundle, 1112
holomorphic cusp forms, 1557
holomorphic map, 1111
holomorphic modular form, 1557
holomorphic tangent bundle, 1112
holomorphic vector bundle, 1111
holonomy group, 1070
Hom complex, 206
homogeneous space, 798, 1091
homogenous ideal, 380
homological dimension, 626
homological dimension bounded by $N$, 220
homomorphism of Lie groups, 1084
homotopic, 279, 356
homotopy, 279
homotopy category, 258, 263, 337, 344
homotopy category of complexes, 206
homotopy category of spaces, 337
homotopy equivalence, 279
homotopy extension property, 289
homotopy fiber square, 460
homotopy fibers, 244
homotopy groups, 284, 855
homotopy relative to $A$, 279
Hopf algebra, 158
Hopf bundle, 322
Hopf fibration, 315
Hopf ideals, 161
Hopf invariant, 1082
horizontal divisor, 1250
Huber, 906
Huber category, 1390
Huber pair, 908
Hurewicz fibration, 291
Hurewicz homomorphism, 298
Hurewicz-Strøm model structure, 265, 293
Hurewicz space, 683
hyperbolic, 1172
hyperbolic plane, 1172
hypercohomologies, 225
hyperelliptic curve, 682
hyperelliptic map, 682
hyperelliptic Weierstrass point, 685
hyperplane line bundle, 1112
hyperplane reflection, 1175
hyperspecial compact subgroups, 1217
ideal, 10, 109, 363
ideal class group, 1162
ideal group defined mod $m$, 1195
ideal groups defined mod $m$, 1195
ideal of definition, 364, 894, 906
ideal sheaf, 528
idele group, 1161
idelic norm, 1162
idempotented algebra, 102
identify local rings, 367
image, 197
immediate specializations/generalizations, 271
immersed submanifold, 1047
immersion, 574
inconsistent, 17
ind-(Zariski localization), 740
ind-Zariski/smooth/étale, 740
indecomposable representation, 1441
index, 973
index of $L$, 1228
index of a w.r.t $\gamma$, 936
index of $M$, 307
index of a subgroup, 32
induced admissible formal subscheme, 1370
induced module, 58
induced reduced scheme structure, 558
induced representation, 1018
induction pair for $G(F_q)$, 1470
inductive, 1
inert, 350
inertia degree, 398, 1139, 1157
inertia field, 1148
inertia group, 1148
infinite adeles, 1161
infinite Grassmannian, 283
infinite ideles, 1162
infinite places, 1156
infinite projective space, 283
infinite sphere, 283
infinite Stiefel Manifold, 283
infinite symmetric product, 284
infinite vector space, 283
infinitesimal deformation, 657, 866
infinitesimal deformation of $Y$ in $X$, 657
infinitesimal equivalent, 1483
infinitesimal extension, 657
infinitesimal generator, 1055, 1090
infinitesimal group scheme, 783
inflation, 878
initial object, 166
initial ordinal, 7
initial segment, 4
injection, 201
injective, 567
injective amplitude, 210
injective amplitude in $[a, b]$, 228
injective cofibration, 261
injective dimension, 405
injective model category, 261
injective object, 167, 209
inner anodyne, 339
inner fibration, 339
inner regular, 924
inseparable degree, 63
integrable, 717, 1110
integral, 559, 571
integral curve, 1055
integral part of $\alpha$, 1671
integral perfectoid ring, 754
integral ring, 48
integral sheaf, 1311
integral stalk, 1388
integral structure sheaf, 1389
integral weight, 1592
integration, 965
internal Ext groups, 549
internal Hom, 226, 548
internal Hom sheaf, 522
interpretable, 16
interpretations, 15
intersection pairing, 307
intersection with Chern classes, 702
intertwining operators, 1001
intrinsic property, 517
invariant, 109
invariant differential form, 826
invariant differential operator, 827
invariant factor decomposition, 59
invariant factors, 59
Invariant polynomial, 1058
inverse Fourier transform, 1658
inverse image, 526
inverse morphism, 165
inverse system, 170
invertibility hypothesis, 264
invertible object, 179
invertible sheaf, 525
involution of first kind, 102
involution of second kind, 102
involution on $G$, 817
involutive Hopf algebra, 158
IP-system, 1039
irreducible, 54, 272, 558
irreducible cusp, 1497
irreducible representation, 1441
irreducible/semisimple, 736
irrelevant ideal, 379
isocrystal, 1338
isocrystal decomposition, 1339
Isocrystal with $G$-structures over $K_0$, 1373
isogeny, 793
isomorphism, 165
isotropic, 1172
isotropic subgroup, 36
isotropy group scheme, 798
Iwahori factorizations, 1514
Iwahori fixed, 1514
Iwahori subgroup, 1514
Jacobi field equation, 1071
Jacobian, 1123
Jacobian variety, 1244
Jacobson, 272, 394, 560
Jacobson radical, 96
Jacobson semisimple, 96
Jacquet functor, 1443, 1518
James reduced product, 284
Janko groups, 44
Japanese, 416
Japanese bracket, 1029
Japanese scheme, 561
join, 338
Jordan decomposition, 115
Jordan form, 76
Joyal model structure, 348
K-adapted class, 222
K-Bessel function, 952
K-finite function, 1544
K-group, 332
K-group of \( D \), 217
K-injective, 220
K-projective, 221
Kähler class, 1117
Kähler cone, 1129
Kähler different, 656
Kähler manifold, 1117
Kähler metric, 1117
Kähler normal coordinate, 1118
Kähler form, 1112
Kan fibration, 339
Kaplansky dévissage, 60
Karoubian category, 198
kernel, 197
kernel group scheme, 778
kernel of the reduction, 1268
Killing equation, 1067
Killing field, 1067
Killing form, 109
Kirillov model, 1525
Klein bottle, 253
Kleinian Integers, 1158
Kolyvagin cohomology classes, 1638
Kolyvagin derivative, 1638
Kolyvagin index, 1638
Kolyvagin number, 1638
Kolyvagin prime, 1638
Kolyvagin system, 1638
Kostant’s partition function, 148
Koszul complex, 431
Koszul-regular, 432
Krull dimension, 273
Kummer extension, 67
L-packet, 1579
Lagrangian decomposition, 36
Lang map, 819
Langlands L-functions, 1577
language, 14
Laplace-Beltrami operator, 1478
Laplacian, 1067
lattice, 1155, 1158
Laurent covering, 1355
Laurent domain, 1354
least upper bound property, 4
Lebesgue space, 923
Lefschetz number, 738
Lefschetz operator, 1118
left anodyne, 339
left coset, 32
left derived functor, 259, 860
left dual, 178
left dual map, 178
left exact functor, 170
left fibration, 339
left global dimension, 406
left homotopic over \( Z \), 255
left Kan extension, 175
left lifting property, 181
left module, 484
left proper, 255
left Quillen bifunctor, 261
left regular action, 991
left-closed, 177
left/right cone, 338
Legendre form, 1260
length, 11, 147, 203, 368
Levi subalgebra, 113
Levi subgroup, 813
Levi-Cevita connection, 717
lexicographical ordering, 4
Lie p-algebra, 142
Lie algebra, 108
Lie algebra associated to G, 1093
Lie bracket, 108, 1051
Lie group, 1084
Lie subgroup, 1087
limit ordinal, 6
limits of discrete series, 1487
Line bundle associated to D, 599
linear action, 799
linear algebraic group, 1464
linear operator, 73
linear ordering, 4
linear series, 679
linear system functor, 843
linear torus, 804
linearly reductive, 810
linked segments, 1517
lisse m-adic, 734
lisse \( \mathcal{O}_k \)-sheaves, 735
lisse Weil sheaf, 1292
local, 508
local G-ringed K-space, 1360
local along Z, 278
local complete intersection, 433
local diffeomorphism, 1045
local dimension, 273
local fibration, 264
local field, 1151
local isomorphism, 740
local on the target, 371
local property, 371
local restriction problem, 1640
local ring, 364, 406
local ring map, 364
local ringed site, 515
local ringed space, 517
local ringed topoï, 516
local zeta functions, 1608, 1623
localization, 359
localization of X along Z, 278
locally bounded, 1210
locally Cartesian fibration, 350
locally closed, 235
locally closed immersion, 1357
locally compact, 240
locally complete intersection, 623
locally connected, 235
locally constructible, 271
locally fibrant, 264
locally finite CW complex, 281
locally integrable, 924
locally nilpotent, 97, 393
locally nilpotent ideal, 364
locally Noetherian, 559
locally Noetherian space, 270
locally of finite type, 570
locally of topologically finite type/finite presentation/admissible, 1370
locally path-connected, 236
locally profinite, 245
locally profinite group, 1000
locally projective, 582
locally projective Qco sheaf, 586
locally Qco, 744
locally spectral, 275
locally symmetric, 1130
locally symmetric variety, 1133
locally trivial bundle, 314
logical consequence, 16
loop space, 280
lower central series, 110
lower semicontinuous, 234
loxodromic, 1495
Lubin-Tate character, 1189
Lubin-Tate module, 829
Lubin-Tate power series, 829
Lustig series, 1470
Lyons group, 44
M-regular sequence, 406
Möbius band, 253
Möbius function, 1673
Maass differential operators, 1504
Maass Form, 1505
magma, 31
manifold, 251
Manin constant, 1647
mapping cone, 206, 234
mapping cylinder, 206, 234
mapping graph, 172
matrices, 73
matrix coefficient, 94
matrix coefficient map, 1013
maximal, 17
maximal $\iota$-weight, 1297
maximal $S$-torsion-free quotient, 364
maximal compact subgroup, 1000
maximal tree, 1663
maximal unramified extension, 1146
mean-value property, 947
measurable cardinal, 12
measurable map, 923
measurable space, 923
measure, 923
measure algebra, 995
measure space, 923
Mellin transformation, 1022
meromorphic along, 1392
meromorphic function, 940
meromorphic modular forms, 1557
meromorphic/holomorphic/vanishes, 1499
metabelian, 43
metrized line bundle, 1654
microbial, 900
Milnor K-group, 155
minimal discriminant, 1271
minimal model, 1252
minimal model for $C$, 1254
minimal polynomial, 79
minimal set, 1035
minimal surface, 1252
minimal Weierstrass equation, 1267
Minkowski functional, 959
minuscule, 152
mirabolic subgroup, 1543
Mittag-Leffler condition, 171
mixed complex, 353
mixing, 1042
Mock modular form, 1507
mod 2 degree of $f$, 1054
model, 15
model complete, 23
model over $S$, 1254
model structure, 254
moderate growth, 1507
modification, 580
modular elliptic curve, 1646
modular forms mod $p$ of weight $k$, 1575
modular function, 993, 1557
modular height, 1322
moduli space of curves, 679
modulus, 1194
Moishezon manifold, 1116
monad, 189
monoid, 31
monoid scheme, 777
monoidal category, 176
monoidal functor, 177
monoidal model category, 262
monoidal transformations, 805
monomorphism, 167
Monster group, 44
Monstrous module, 143
Moore chain complex, 855
Morita equivalent, 373
morphism compatible with the geometric structure, 200
morphism of local ringed topoi, 516
morphism of sites, 491
morphism of topoi, 496
morphisms from $x$ to $y$, 165
motivic L-function, 1604
multiplication, 3
multiplication of ordinals, 7
multiplicative Arakelov heights, 1207
multiplicative canonical heights, 1206
multiplicative group, 814
multiplicative Herbrand quotient, 209
multiplicative reduction, 1268
multiplicative structure sheaf, 515
multiplicative valuation, 899
Mumford curve, 1372
Mumford line bundle, 1225
N-1, 416
N-2, 416
Néron differential, 1267
Néron model, 1246
Néron-Severi group, 847, 1113
Néron-Tate height, 1240
Néron-Tate pairing, 1242
Nagata, 416
Nagata scheme, 561
natural density, 1198
natural transformation, 166
NDR-pair, 289
nef line bundle, 715
negative roots of $R$, 146
nerve, 337
neutral Tannakian category, 196
new forms of level $N$, 1563
Newton Identities, 52
Newton polygon, 1144
nilpotent, 108, 110
nilpotent group scheme, 779
nilpotent radical, 113
nilradical, 394
node, 679
Noetherian, 203, 367, 491, 559
Noetherian ring, 367
Noetherian space, 270
non-Abelian Čech cohomology, 542
non-Archimedean, 899
non-Archimedean field, 899
non-degenerate, 92, 1171
non-degenerate $F$-crystal, 749
non-degenerate critical point, 1079
non-degenerate line bundle, 1227
non-holomorphic Eisenstein series, 1619
non-isotropic kernel, 1174
non-singular measurable map, 923
non-singular projective model, 669
non-split in $L$, 398
non-split multiplicative reduction, 1268
non-wandering points, 1035
non-derogatory, 79
norm, 954
norm group, 1152, 1164
norm map, 64
Norm operator topology, 957
norm residue symbol, 1184, 1187, 1191
normal, 561, 981
normal closure, 62
normal coordinate frame, 1113
normal covering space, 311
normal domain, 409
normal extension, 62
normal sheaf, 605
normal subgroup, 32
normal subobject, 189
normal Weierstrass point, 685
normalization, 409, 855
normalized, 828
normalized Eisenstein series, 1569
normalized invariant differential form, 1258
normalized Jacquet functor, 1518
normalized spherical vector, 1535
normed group, 1137
normed module, 1138
normed(valued) $K$-space, 957
NOT gate, 1656
null system, 734
number field, 1156
number field of $f$, 1574
numerical locally trivial bundle, 314
numerical polynomial, 1673
numerically effective line bundle, 715
numerically equivalent, 711, 714
O'Nan group, 44
objects, 337
objects of $C$, 165
observables, 1655
of at most linear exponential growth, 1499
of finite branched, 11
of finite presentation, 415, 519, 607
of locally finite presentation, 607
of moderate growth, 1499
of topologically finite presentation, 896
of topologically finite type, 896
old forms of level $N$, 1563
one-parameter subgroup, 1085
one-point compactification, 240
open covering of a functor, 836
open immersion, 528, 574, 1357, 1365, 1391
open subfunctor, 836
open subscheme, 574
open subspace, 528
open/closed subgroup scheme, 777
opposed category, 176
OR gate, 1656
orbit map, 797
orbit scheme, 797
orbit space for $R$, 852
order, 401, 1019, 1023
order of vanishing, 939, 1413
orderable ring/field, 69
ordered field, 69
ordered ring, 69
ordinal number, 6
ordinary elliptic curve, 1264
ordinary homology theory, 297
ordinary reduced homology theory, 297
orientable, 750
orientation of $E$, 319
oriented, 750
oriented bordism group, 334
orthogonal group, 814, 1175
orthohedron, 1665
outer regular, 924
overconvergent elements, 1144
parabolic, 1495
parabolic induction, 1519
parabolic subgroup, 809
paracompact, 247
parallelizable, 1050
pariah groups, 44
Parseval equality, 958
partial L-function, 1615
partial ordering, 3
path, 11
path object, 255
path space, 244, 280
path-connected, 236
path-connected component, 236
Pauli Observables, 1655
pd-A-derivation, 479
pd-de Rham complex, 480
pd-differential, 479
pd-envelope, 475
pd-scheme, 742
pd-structure, 473
pd-thickening, 742
perfect, 445, 447, 552, 1351
perfect $\delta$-ring, 458
perfect closure, 63
perfect complex, 220
perfect complex of $O$-modules, 552
perfect module, 464
perfect object relative to $S$, 552
perfect prism, 750
perfect prismatic site, 758
perfection, 1351
perfection of prisms, 754
perfectly finitely presented, 446
perfectly finitely presented morphism, 1351
perfectoid affinoid $K$-algebra, 921
perfectoid affinoid field, 921
perfectoid algebra, 917
perfectoid field, 914
perfectoid spaces, 1398
period number, 1201
Pfaffian, 89
Picard functor, 841
Picard group, 525
Picard number, 847, 1113
Picard scheme, 844
Picard-Fuchs differential operator, 1265
planer glueing diagram, 252
Poincaré series of weight $2k$ and character $n$
for $\Gamma$, 1572
point of a site, 493
pointed CW complex, 283
pointwise almost periodic, 1037
pointwise equivalence, 347
polar, 967
polar density, 1198
polarizable integral Hodge structure, 1233
polarization, 1231
polarization function, 34
pole, 939
polydisc, 953
polygon, 1664
polyhedron, 1664
polyhomogenous symbols of degree $d$, 1029
Polylogarithm function, 1649
polytope, 1664
Pontryagin class, 1058
Pontryagin dual, 405
<table>
<thead>
<tr>
<th>Term</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Pontryagin numbers</td>
<td>331</td>
</tr>
<tr>
<td>positive</td>
<td>981</td>
</tr>
<tr>
<td>positive elements</td>
<td>69</td>
</tr>
<tr>
<td>positive involution</td>
<td>1283</td>
</tr>
<tr>
<td>positive linear functional</td>
<td>992</td>
</tr>
<tr>
<td>positive roots of $R$</td>
<td>146</td>
</tr>
<tr>
<td>positive semi-definite</td>
<td>34</td>
</tr>
<tr>
<td>positive-definite</td>
<td>34</td>
</tr>
<tr>
<td>positively expansive</td>
<td>1036</td>
</tr>
<tr>
<td>potentially good reduction</td>
<td>1268</td>
</tr>
<tr>
<td>potentially unramified</td>
<td>1345</td>
</tr>
<tr>
<td>power bounded elements</td>
<td>1141</td>
</tr>
<tr>
<td>pre Artin-Rees category</td>
<td>734</td>
</tr>
<tr>
<td>pre-equivalence relations on $X_0$</td>
<td>167</td>
</tr>
<tr>
<td>pre-relations on $X_0$</td>
<td>167</td>
</tr>
<tr>
<td>pre-Weil cohomology theory</td>
<td>770</td>
</tr>
<tr>
<td>preadditive</td>
<td>197</td>
</tr>
<tr>
<td>preimage orientation</td>
<td>1054</td>
</tr>
<tr>
<td>presentable</td>
<td>360</td>
</tr>
<tr>
<td>presheaf</td>
<td>168</td>
</tr>
<tr>
<td>presheaf of affinoid functions</td>
<td>1356</td>
</tr>
<tr>
<td>prespectrum</td>
<td>311</td>
</tr>
<tr>
<td>prestack</td>
<td>498</td>
</tr>
<tr>
<td>previety</td>
<td>660</td>
</tr>
<tr>
<td>prime</td>
<td>54</td>
</tr>
<tr>
<td>prime ideal</td>
<td>10</td>
</tr>
<tr>
<td>prime number</td>
<td>1671</td>
</tr>
<tr>
<td>prime Weil divisor</td>
<td>694</td>
</tr>
<tr>
<td>primitive CM-field</td>
<td>1281</td>
</tr>
<tr>
<td>primitive cohomology class</td>
<td>1120</td>
</tr>
<tr>
<td>primitive Dirichlet character</td>
<td>1614</td>
</tr>
<tr>
<td>primitive of degree $d$</td>
<td>1415</td>
</tr>
<tr>
<td>primitive of weight $\lambda$</td>
<td>1590</td>
</tr>
<tr>
<td>principal $\mathfrak{sl}_2$-subalgebra</td>
<td>116</td>
</tr>
<tr>
<td>principal $G$-bundle</td>
<td>323</td>
</tr>
<tr>
<td>principal congruence subgroup</td>
<td>1514</td>
</tr>
<tr>
<td>principal polarization</td>
<td>1231</td>
</tr>
<tr>
<td>principal series</td>
<td>1486</td>
</tr>
<tr>
<td>principal series representation</td>
<td>1528</td>
</tr>
<tr>
<td>principally-CM Abelian variety</td>
<td>1287</td>
</tr>
<tr>
<td>principle divisor associated to $f$</td>
<td>694</td>
</tr>
<tr>
<td>principle Weil divisor</td>
<td>694</td>
</tr>
<tr>
<td>prism</td>
<td>750</td>
</tr>
<tr>
<td>prismatic envelope</td>
<td>752</td>
</tr>
<tr>
<td>prismatic site</td>
<td>759</td>
</tr>
<tr>
<td>pro-$p$-group</td>
<td>47</td>
</tr>
<tr>
<td>pro-étale</td>
<td>1431</td>
</tr>
<tr>
<td>pro-Zariski localization</td>
<td>277</td>
</tr>
<tr>
<td>probabilistic measure</td>
<td>923</td>
</tr>
<tr>
<td>product subgroup</td>
<td>32</td>
</tr>
<tr>
<td>profinite cohomology</td>
<td>881</td>
</tr>
<tr>
<td>profinite formation</td>
<td>1184</td>
</tr>
<tr>
<td>profinite group</td>
<td>45</td>
</tr>
<tr>
<td>profinite space</td>
<td>245</td>
</tr>
<tr>
<td>progenerator</td>
<td>373</td>
</tr>
<tr>
<td>projection along $p$</td>
<td>678</td>
</tr>
<tr>
<td>projection map</td>
<td>547</td>
</tr>
<tr>
<td>projective</td>
<td>402</td>
</tr>
<tr>
<td>projective dimension</td>
<td>405</td>
</tr>
<tr>
<td>projective fibration</td>
<td>261</td>
</tr>
<tr>
<td>projective metric on $\mathbb{P}^n$</td>
<td>1207</td>
</tr>
<tr>
<td>projective model category</td>
<td>261</td>
</tr>
<tr>
<td>projective object</td>
<td>167</td>
</tr>
<tr>
<td>projective representation</td>
<td>1441</td>
</tr>
<tr>
<td>projective space</td>
<td>597</td>
</tr>
<tr>
<td>projective unitary representation</td>
<td>1442</td>
</tr>
<tr>
<td>proof</td>
<td>17</td>
</tr>
<tr>
<td>proper</td>
<td>579</td>
</tr>
<tr>
<td>proper action</td>
<td>268</td>
</tr>
<tr>
<td>proper direct image</td>
<td>526</td>
</tr>
<tr>
<td>proper discontinuous</td>
<td>268</td>
</tr>
<tr>
<td>proper inverse image</td>
<td>527</td>
</tr>
<tr>
<td>proper map</td>
<td>238</td>
</tr>
<tr>
<td>proper over a Noetherian affine scheme</td>
<td>601</td>
</tr>
<tr>
<td>proximal</td>
<td>1037</td>
</tr>
<tr>
<td>pseudo $G$-torsor</td>
<td>493</td>
</tr>
<tr>
<td>pseudo uniformizer</td>
<td>906</td>
</tr>
<tr>
<td>pseudo-Abelian variety</td>
<td>1222</td>
</tr>
<tr>
<td>pseudo-coherent $O_X$-module</td>
<td>551</td>
</tr>
<tr>
<td>pseudo-coherent module</td>
<td>463</td>
</tr>
<tr>
<td>pseudo-differential operator of symbol $a$</td>
<td>1029</td>
</tr>
<tr>
<td>pseudo-reductive group</td>
<td>811</td>
</tr>
<tr>
<td>pseudo-uniformizer</td>
<td>914</td>
</tr>
<tr>
<td>pseudo-unitary groups</td>
<td>1096</td>
</tr>
<tr>
<td>pullback</td>
<td>518</td>
</tr>
<tr>
<td>pullback bundle</td>
<td>1337</td>
</tr>
<tr>
<td>pullback filtration</td>
<td>314</td>
</tr>
<tr>
<td>pullback space</td>
<td>234</td>
</tr>
<tr>
<td>pure braids</td>
<td>39</td>
</tr>
</tbody>
</table>
pure of weight \( w \), 1297
pure tensor, 1176
pure (isotypical) of slope, 1339
purely inseparable, 63
pushforward, 517, 526
pushforward filter, 10
pushforward filtrations, 190
pushforward map of cohomology, 770
Quco vector bundle, 596
quadratic character, 1188
quadratic form, 34, 1171
quadratic spaces, 1171
quadratically closed, 1171
qualifier symbol, 15
quantifier elimination, 23
quantization, 1657
quantum correspondence principle, 1655
quantum Fourier transform, 1658
quantum logic gate, 1657
quasi-affine, 569
quasi-algebraically closed, 1204
quasi-central homomorphism, 791
quasi-character, 1004
quasi-coherent, 520, 1359
quasi-compact, 237, 491
quasi-compact morphism, 237
quasi-cuspidal representation, 1520
quasi-excellent ring, 416
quasi-fibration, 184
quasi-functor, 186
quasi-isogenies, 1230
quasi-pro-étale, 1435
quasi-separated, 270, 577
quasi-split torus, 805
quasisplit, 1447
Quaternion algebra, 1176
qubit, 1655
Quillen adjunction, 259
Quillen equivalence, 259
Quot functor, 838
quaternionic orthogonal group, 1096
quotient group, 32
quotient group scheme, 778
quotient map, 234, 778
quotient ring, 363
quotient topology, 234
quotient triangulated category, 216
radical, 110, 810, 1171
radius of convergence, 928, 941
Radon measure, 924
Ramanujan \( \tau \)-function, 1571
ramification degree, 398, 670, 1139
ramification field, 1148
ramification group, 1148
ramified in over \( p \), 399
rank, 56
rank class, 703
rank of \( \mathcal{F} \) at \( p \), 587
rank of \( g \), 117
rank of a group variety, 813
rank of a valuation, 897
Rankin-Selberg L-function, 1618
Rankin-Selberg method, 1617
rapidly decreasing, 1507
rational covering, 1355
rational curve, 667
rational domain, 1354
rational equivalent, 695
rational function, 532
rational map, 532
rational subset, 1382, 1385
rationally connected, 666
ray class field, 1195
ray class group, 1195
ray mod \( m \), 1195
real, 70
real algebraic envelope, 1467
real closed, 70
real closure, 70
real form, 815, 816
real inner space, 81
real part, 933
real places, 1156
real projective space, 253
real quaternion algebra, 89
reciprocity isomorphism, 1184
recursive, 17
recursively enumerable, 14
reduced, 48, 558
reduced degree, 101
reduced Eilenberg-Steenrod homology theory, 296
reduced root system, 145
reduction map, 901
reduction modulo of $E$, 1268
reduction of $X$, 1254
reduction map, 901
reduction modulo of $E$, 1268
reduction of $X$, 1254
reductive, 124
reductive group, 811
Ree Groups, 1469
reflection, 144
reflection group, 152
reflex CM-pair, 1282
reflex field, 1282, 1286
reflexive, 969
reflexive object, 177
region, 933
regular, 12, 230, 561
regular action, 268, 797
regular category, 181
regular cusp, 1497
regular element, 117
regular embedding, 623
regular local, 411
regular locus, 561
regular model, 1252
regular points, 1111
regular ring, 411
regular semiperfect ring, 766
regular sequence, 406
regular value, 1048
regular with respect to $A_\bullet$, 859
regulator, 973, 1242
regulator map, 1650
relation symbol, 14
relations on $X_0$, 167
relative cup product, 545
relative CW complex, 283
relative de Rham complex, 716
relative dimension, 389
relative dimension $n$, 613
relative dualizing complex, 651
relative effective (Cartier)divisor, 640
relative Frobenius, 445, 534
relative Grassmannian of $E$, 840
relative homotopy groups, 285
relative identity component, 1247
relative Morse index, 1081
relative Picard functor, 841
relative Proj, 595
relative tangent space, 617
relatively compact, 1367
relatively minimal surface, 1252
relevant, 815, 816
removable singularity, 939
representable, 187, 188
representable by algebraic spaces, 851
representation, 1441
representation of a Lie $p$-algebra, 142
representation of a Lie algebra, 136
representation of complex type, 1441
representation of Galois-type, 1333
representation of quaternion type, 1441
representation of real type, 1441
reproducing kernel, 979
residual representation, 1332
residue, 940
resolution property, 648
restricted étale site, 504
restricted direct product, 1160
restricted power series, 894
restricted product measure, 1160
restricted smooth site, 505
restricted tensor module, 104
restricted tensor product, 104
restricted tensor representation, 1546
restricted Zariski site, 503
restriction, 58, 878
restriction sheaf, 498
resultant, 51
retract, 167
retraction, 279
retrocompact, 271
reverse ordering, 3
reversible, 1656
Ricci curvature, 1068
Riemann form, 1122
Riemann L-function, 1616
Riemann pair, 1121
Riemann surface, 1129
right anodyne, 339
right coset, 32
right derived functor, 222, 225
right derived functors, 259
right exact functor, 170
right fibration, 339
right homotopic under $X$, 255
right hyper-derived functor, 225
right Kan extension, 175
right lifting property, 181
right proper, 255
right regular action, 991
right-closed, 177
right-lax monoidal functor, 177
rigid, 178, 657, 866
rigid (analytic) space, 1360
rigid fibered category, 186
rigid monoidal category, 178
ring, 48
ring of definition, 906
ring of integers, 1156
ring of integral elements, 908
ringed site, 515
ringed space, 516
ringed topos, 515
Robba ring, 1144
root lattice, 151
root system, 145
root system associated to $(g, h)$, 119
roots, 145
row equivalent, 77
Rudvalis group, 44
Runge immersion, 1357
s-free, 336
Satake parameter, 1513
satisfiable, 15
satisfies, 15
saturated localizing system, 172
saturated triangulated subcategory, 216
saturation, 190
saturation of $S$, 172
scalar curvature, 1068
Schauder basis, 972
schematic morphism, 850
schematic support, 592
schematically dense, 563
scheme-theoretic closure, 575
scheme-theoretic image, 575
scheme-theoretically dense, 576
schemes, 529
Schrödinger representation, 1007
Schwartz functions, 961
Schwartz-Bruhat function, 1167
Schwartz-Bruhat functions, 1168
scissors-congruent, 1665
second category, 251
section functor, 535
sectional curvature, 1068
Segal category, 350
Segre embedding, 597
self sequentially compact, 238
self-dual Haar measure, 1010
self-Dual Lattice, 1584
semi-algebraic, 28
semi-ample holomorphic line bundle, 1126
semi-direct product group scheme, 778
semi-direct product Lie algebra, 108
semi-local, 96
semi-normed group, 1137
semi-perfect, 445
semi-primary, 96
semilocally simply connected, 286
seminorm, 954, 959
semisimple, 94, 108, 111
semisimple $k$-rank, 813
semisimple $R$-module, 92
semisimple algebraic group, 810
semisimple or unipotent element, 1466
semisimple rank, 813
semisimple/nilpotent element, 115
semisimple/solvable/nilpotent/simple Lie group, 1107
semisimple/unipotent element, 818
semistable of slope $\lambda$, 191, 193
semistable reduction, 1254, 1268
semistable union of curves, 1254
Sen’s operator, 1346
sentence, 15
separable, 234, 417
separable closure, 66
separable degree, 62
separable extension, 62
separable over $K$, 62
separable polynomial, 62
separable/purely inseparable morphism, 574
separably generated, 417
separate $R$-orbits, 852
separated, 577
separated presheaf, 494
separating, 954
sequentially compact, 238
Serre derivation, 1573
Serre fibration, 291
Serre subcategory, 202
Serre twisting sheaf, 595
Serre twisting sheaves, 595
Serre-Quillen model structure, 265, 293
sesquilinear form, 90
set of generator, 32
set of natural numbers, 1
set of real numbers, 5
set-theoretically $R$-invariant, 852
setoid, 166
Severi-Brauer variety, 875
Shafarevich-Tate group, 1239
sharp map, 447
sheaf, 494
Sheaf Hom complex, 547
sheaf of $R$-invariant functions, 852
sheaf of differentials, 523, 524
sheaf of rigid analytic functions, 1360
sheaf-cohomology presheaves, 535
sheafification functor, 494
sheafy, 1389
Siegal upper half plane $H_g$, 1132
Siegel sets, 1218
sieve, 492
sign of functional equation, 1604
sign of functional equation of $A$, 1643
sign of functional equation of $E$, 1642
signature, 1174
signature operator, 1060
simple, 109
simple $R$-module, 92
simple Abelian variety, 1229
simple algebraic group, 811
simple balanced covering, 1395
simple group, 32
simple Laurent covering, 1395
simple prism, 1666
simple ring, 48
simple topological space, 285
simplicial category, 336
simplicial categories, 343
simplicial model category, 345
simplicial module, 855
simplicial nerve, 344
simplicial object, 336
simplicial realization functor, 337
simplicial resolution, 858
simply closed, 23
simply connected, 286
simply equivalent, 1174
simply-connected group variety, 809
singular cohomology groups, 299
singular complex functor, 338
singular locus, 561
singular trace, 988
singularity, 939
site, 491
skew field, 49
slice chart, 1047
slope, 191, 193
slope morphism, 1373
small, 13, 181
small étale site, 504
small smooth site, 505
small Zariski site, 503
smash product, 280
smash products, 279
Smith normal form, 78
smooth, 436
smooth $\mathcal{H}$-module, 103
smooth covering space, 1046
smooth curve, 688
smooth embedding, 1046
smooth functions, 1544
smooth immersion, 1045
smooth induced representation, 1457
smooth morphism, 614
smooth representation, 1443, 1545
smooth submersion, 1045
smooth topology, 505
smooth vector bundle, 1049
smooth vector field, 1049
smooth vectors, 1479
smooth/flat/separated/… group scheme, 777
sober, 273, 274
Sobolev Space, 960
Sobolev space, 1023
sofic, 1041
solid Abelian group, 892
solid complex, 892
solvable, 110
solvable group scheme, 779
space of left morphisms, 358
space of right morphisms, 357
special automorphism, 109
special cocontinuous functor, 497
special divisor, 676
special fiber, 532, 754
special linear group, 814
special maximal compact subgroups, 1580
special orthogonal groups, 814
special unitary group, 1096
special unitary groups, 814
specialization map, 156, 1383, 1385
specialization of y, 271
spectral, 275
spectral radius, 975
spectrum, 529, 975, 978
sphere spectrum, 311
spherical character, 104
spherical function, 1539
spherical idempotent, 103
spherical representation, 1515
spherical vectors, 104
spherical Whittaker function, 1537
spherical(unramified) module, 104
spherically complete, 900
Spin representation, 1595
split, 100
split Cartan subalgebra, 120
split fibered category, 184
split group variety, 809
split multiplicative reduction, 1268
split reductive, 813
split reductive pair, 813
split semisimple Lie algebra, 120
split solvable(resp. nilpotent) group, 779
split torus, 804
splits completely in L, 398
splitting field, 100, 875, 1179
sporadic simple groups, 44
square integrable, 1494
square-integrable, 1539
stabilizer group scheme, 1462
Stable $\infty$-category, 362
stable cohomological operator, 300
stable Faltings height, 1321
stable filtration, 381
stable reduction, 1267
stable union of curves, 1254
stabilizer subgroup of $Y$, 790
stably equivalent, 332
stably framed manifold, 335
stably uniform, 1389
stack, 498
stackification, 502
stalk, 527, 723
stalks of an affinoid adic space, 1388
standard étale, 442
standard étale morphism, 621
standard binary rational covering, 1395
standard Borel subgroup, 814
standard fpqc covering, 506
standard rational covering, 1395
standard smooth algebra, 435
standard smooth morphism, 614
standard syntomic algebra, 623
standard unipotent subgroup, 814
standard y-topology, 508
state, 1655
states of particles, 1655
states of particles of $\Sigma$, 1660
Steenrod Powers, 313
Steinberg Groups, 1469
Steinberg representation, 1472, 1528
Stiefel manifold, 1092
Stiefel-Whitney class, 328
Stiefel-Whitney number, 329
stimulate, 1657
Stone-Čech Compactification, 239
straightening functor, 347
strict $m$-adic sheaves, 734
strict $p$-cohomological dimension, 883
strict $p$-ring, 448
strict cohomological dimension, 883
<table>
<thead>
<tr>
<th>Term</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>strict Henselian</td>
<td>417</td>
</tr>
<tr>
<td>strict monoidal category</td>
<td>176</td>
</tr>
<tr>
<td>strict morphism</td>
<td>894</td>
</tr>
<tr>
<td>strict subobject</td>
<td>190</td>
</tr>
<tr>
<td>strict transform</td>
<td>642</td>
</tr>
<tr>
<td>strictly commutative</td>
<td>233</td>
</tr>
<tr>
<td>strictly full subcategory</td>
<td>167</td>
</tr>
<tr>
<td>strictly perfect complex of O-modules</td>
<td>551</td>
</tr>
<tr>
<td>strictly totally disconnected</td>
<td>1399, 1429</td>
</tr>
<tr>
<td>strictly w-local</td>
<td>740</td>
</tr>
<tr>
<td>strong approximation</td>
<td>1218</td>
</tr>
<tr>
<td>strong desingularization</td>
<td>659</td>
</tr>
<tr>
<td>strong Grothendieck category</td>
<td>1355</td>
</tr>
<tr>
<td>strong limit</td>
<td>12</td>
</tr>
<tr>
<td>Strong operator topology</td>
<td>957</td>
</tr>
<tr>
<td>strongly connected group</td>
<td>793</td>
</tr>
<tr>
<td>strongly contradicting semi-stability</td>
<td>192</td>
</tr>
<tr>
<td>strongly equivalent</td>
<td>337</td>
</tr>
<tr>
<td>strongly finite étale</td>
<td>1403</td>
</tr>
<tr>
<td>strongly holomorphic</td>
<td>966</td>
</tr>
<tr>
<td>strongly identity component</td>
<td>793</td>
</tr>
<tr>
<td>strongly inaccessible(SI)</td>
<td>12</td>
</tr>
<tr>
<td>strongly minimal</td>
<td>24</td>
</tr>
<tr>
<td>strongly Noetherian</td>
<td>904</td>
</tr>
<tr>
<td>structure extension</td>
<td>15</td>
</tr>
<tr>
<td>structure presheaf</td>
<td>1389</td>
</tr>
<tr>
<td>structure sheaf</td>
<td>515, 742</td>
</tr>
<tr>
<td>stupid truncation</td>
<td>205</td>
</tr>
<tr>
<td>sub-comodule</td>
<td>159</td>
</tr>
<tr>
<td>subcanonical topology</td>
<td>494</td>
</tr>
<tr>
<td>subcategory</td>
<td>167</td>
</tr>
<tr>
<td>subcomplex</td>
<td>281</td>
</tr>
<tr>
<td>subgraph</td>
<td>1663</td>
</tr>
<tr>
<td>sublinear functional</td>
<td>959</td>
</tr>
<tr>
<td>subnormal series</td>
<td>41</td>
</tr>
<tr>
<td>subshift</td>
<td>1040</td>
</tr>
<tr>
<td>subshift of finite type</td>
<td>1041</td>
</tr>
<tr>
<td>subtree</td>
<td>11</td>
</tr>
<tr>
<td>successor</td>
<td>1</td>
</tr>
<tr>
<td>successor ordinal</td>
<td>6</td>
</tr>
<tr>
<td>sum</td>
<td>3</td>
</tr>
<tr>
<td>supersingular elliptic curves</td>
<td>1264</td>
</tr>
<tr>
<td>supersolvable group</td>
<td>42</td>
</tr>
<tr>
<td>support</td>
<td>390, 517, 1019</td>
</tr>
<tr>
<td>surjection</td>
<td>201</td>
</tr>
<tr>
<td>surnatural number</td>
<td>46</td>
</tr>
<tr>
<td>suspension</td>
<td>280</td>
</tr>
<tr>
<td>suspension prespectrum</td>
<td>311</td>
</tr>
<tr>
<td>Suzuki Groups</td>
<td>1469</td>
</tr>
<tr>
<td>Swan conductor</td>
<td>1635</td>
</tr>
<tr>
<td>Sylow pro-p-subgroup</td>
<td>47</td>
</tr>
<tr>
<td>symbol</td>
<td>14</td>
</tr>
<tr>
<td>symbol class</td>
<td>1029</td>
</tr>
<tr>
<td>symbolic power</td>
<td>394</td>
</tr>
<tr>
<td>symmetric algebra</td>
<td>365</td>
</tr>
<tr>
<td>symmetric monoidal category</td>
<td>177</td>
</tr>
<tr>
<td>symmetric monoidal functor</td>
<td>177</td>
</tr>
<tr>
<td>symmetric space</td>
<td>1130</td>
</tr>
<tr>
<td>symmetric square L-functions</td>
<td>1618</td>
</tr>
<tr>
<td>symmetrized tensors</td>
<td>86</td>
</tr>
<tr>
<td>symplectic form</td>
<td>1083</td>
</tr>
<tr>
<td>symplectic group</td>
<td>814</td>
</tr>
<tr>
<td>symplectic manifold</td>
<td>1083</td>
</tr>
<tr>
<td>syntomic morphism</td>
<td>623</td>
</tr>
<tr>
<td>syntomic topology</td>
<td>506</td>
</tr>
<tr>
<td>system of parameters</td>
<td>386</td>
</tr>
<tr>
<td>tacnode</td>
<td>679</td>
</tr>
<tr>
<td>Tamagawa measure</td>
<td>1168</td>
</tr>
<tr>
<td>Tamagawa number</td>
<td>1248</td>
</tr>
<tr>
<td>tame character</td>
<td>1149</td>
</tr>
<tr>
<td>tamely ramified extension</td>
<td>1147</td>
</tr>
<tr>
<td>tamely unramified at P</td>
<td>670</td>
</tr>
<tr>
<td>tangent bundle</td>
<td>1050</td>
</tr>
<tr>
<td>tangent sheaf</td>
<td>662</td>
</tr>
<tr>
<td>tangent space of formal curve</td>
<td>823</td>
</tr>
<tr>
<td>tangent vector</td>
<td>1049</td>
</tr>
<tr>
<td>Tannakian category</td>
<td>179, 196</td>
</tr>
<tr>
<td>Tate algebra</td>
<td>901</td>
</tr>
<tr>
<td>Tate comodule</td>
<td>833</td>
</tr>
<tr>
<td>Tate curve</td>
<td>1274</td>
</tr>
<tr>
<td>Tate Huber ring</td>
<td>906</td>
</tr>
<tr>
<td>Tate module</td>
<td>833, 1189, 1231</td>
</tr>
<tr>
<td>Tate twist</td>
<td>1331</td>
</tr>
<tr>
<td>Tate twist isocrystal</td>
<td>1339</td>
</tr>
<tr>
<td>Tate weist sheaf</td>
<td>735</td>
</tr>
<tr>
<td>Tate’s normalized trace</td>
<td>1154</td>
</tr>
<tr>
<td>tautological bundles</td>
<td>322</td>
</tr>
<tr>
<td>Teichmüller lifts</td>
<td>448, 451</td>
</tr>
<tr>
<td>Teichmüller section</td>
<td>1423</td>
</tr>
<tr>
<td>tempered</td>
<td>1021</td>
</tr>
<tr>
<td>tempered representation</td>
<td>1540</td>
</tr>
</tbody>
</table>
tensor algebra, 365
tensor category, 179
tensor functor, 179
tensor product, 57, 517
tensor product of correspondences, 767
tensored over $\mathcal{C}$, 180
terms, 15
test functions, 1019, 1449
tetrahedron, 1665
theory, 15
theory of $M$, 15
Theta function, 1615
theta function, 1584
thickening, 657
Thom class, 321
tilt, 1399
tilting, 446
tilting, 918
Todd characteristic, 708
Todd class, 705
Todd polynomials, 53
Toffoli gate, 1657
topological Abelian group, 894
topological category, 337
topological dynamic system, 1035
topological entropy, 1038
topological group, 267
topological Markov chain, 1041
topological module, 894
topological nerve, 344
topological quantum field theory, 1660
topological ring, 894
topological surface, 252
topological vector space, 954
topologically mixing, 1036
topologically nilpotent, 894, 900, 1138
topologically of finite presentation, 1370
topologically of finite type, 1370
topologically transitive, 1036
topologist's Hopf algebra, 159
topology, 491
topos, 496
Tor dimension, 406
Tor modules, 544
torsion component, 789
torsion sheaf, 592, 726
torsion tensor, 1064
torsion-free, 58
total Chern class, 703
total complexes, 206
total de Rham complex, 716
total derived functor, 259
total ordering, 3
total ring of fractions, 366
total transform, 642
totally acyclic sheaf, 550
totally bounded, 249, 955
totally disconnected, 236, 1399, 1429
totally integrally closed, 379
totally ramified over $p$, 399
trace, 89
trace class, 987
trace element, 655
trace element of $f$, 655
trace form, 64, 137, 399
trace map, 64, 770
trace of $f$, 655
trace pairing, 655
transcendental degree, 65
transitive, 6
translation, 1019
transporter, 790
transpose, 75
transpose isomorphism, 768
transpose matrix, 75
tree, 11, 1663
triad of spaces, 279
triangularizable algebraic group, 808
triangularizable space, 252
triangulated subcategory, 212
trigonal curve, 683
trigonometric functions, 943
triple point, 679
trivial (co)fibration, 254
trivial fibration, 339
trivial vector bundle, 319
truncation functor, 362
twist, 508
twist group, 1469
twisted $L$-function, 1629
twisted Jacquet functor, 1518
twisted-linear subvariety, 875
type I, 1442
 type II, 1442

UFD, 54
 ultrafilter, 10
 ultranormed Banach algebra, 1141
 ultrapower, 18
 ultraproduct, 18
 uncountable, 2
 undercategories, 339
 underlying degeneracy map, 336
 underlying reduced subscheme, 558
 uniform, 1137, 1391
 uniformizer at p, 668
 uniformly almost finitely generated, 485
 unimodular, 138, 993
 unipotent algebraic group, 1468
 unipotent radical, 811
 unipotent representations, 1470
 unit ideles, 1162
 unit/counit maps, 169
 unital binary operator, 31
 unital magma, 31
 unitary, 981
 unitary group, 1096
 unitary groups, 814
 unitary representation, 1442
 universal, 1657
 universal δ-functor, 224
 universal aximatization, 22
 universal categorical quotient, 173
 universal cover, 318
 universal cover of Lubin-Tate formal group, 1423
 universal covering, 809
 universal enveloping p-algebra, 142
 universal enveloping algebra, 131
 universal finite group, 1469
 universal norm residue symbol, 1184, 1187, 1191
 universal object, 175
 universal quadratic form, 1171
 universal sentence, 22
 universally catenary, 560
 universally Japanese, 416
 unramified, 439, 1146, 1162, 1166, 1623
 unramified class, 886
 unramified extension, 399, 1146
 unramified in L, 399
 unramified over p, 399
 unramified principal series, 1535
 unramified quasi-character, 1513
 unstable reduction, 1268
 unstraightening functor, 347
 untilting, 918
 upper numbering, 1150
 upper semicontinuous, 234

v-covering, 508
 v-topology, 508
 vacuum state defined by M, 1660
 vacuum-vacuum expectation value, 1660
 valence ν, 769
 valuation, 897
 valuation ring, 896
 valuation spectrum, 1381
 value group, 897
 valued module, 1138
 valued ring, 1137
 vanishing order of κ, 1638
 variety, 660
 variety over S, 666
 vector bundle, 318
 vector bundle homomorphism, 318
 vector bundle of finite type, 320
 Verma module, 1593
 vertical divisor, 1250
 vertically nef, 1251
 vertices, 1663
 very ample holomorphic line bundle, 1127
 very good cylinder object, 255
 virtual number of coincidence, 769
 von Neumann Algebra, 982

w-local, 277, 740
 weak equivalence, 261, 263, 856
 weak equivalences, 254
 weak Goodstein sequence, 7
 weak Grothendieck category, 1355
 weak homotopy equivalence, 285, 338
 weak Maass form, 1505
 weak mixing, 1042
 Weak operator topology, 957
weak product, 280
weak Serre subcategory, 202
weak topology, 453
weakly admissible \(\varphi\)-modules, 1340
weakly associated point of \(\mathcal{F}\), 587
weakly associated points of \(X\), 587
weakly associated primes, 391
weakly Cartesian, 1139
weakly compact cardinal, 11
weakly converges, 230
weakly embedded submanifold, 1047
weakly final, 167
weakly holomorphic, 966
weakly inaccessible, 12
weakly saturated, 181
weakly unramified at \(P\), 670
Weber L-function, 1615
wedge, 174
wedge sum, 280
Weierstrass \(\wp\)-function, 950
Weierstrass class, 1271
Weierstrass domain, 1354
Weierstrass equations, 1256
Weierstrass model, 1267
Weierstrass point, 685
Weierstrass semigroup, 684
weight decomposition, 1592
weight lattice, 151
Weil \(q\)-integer, 1284
Weil cohomology theory, 770
Weil divisor class associated to \(\mathcal{L}\), 599
Weil group, 1188
Weil height, 1208
Weil representation, 1472

Weil restriction, 514
Weil sheaves, 1292
Weil-Châtelet Group, 1277
well-ordering, 4
well-pointed space, 280
Weyl chamber, 147
Weyl denominator, 1597
Weyl group, 145
Whittaker functional, 1508, 1521, 1551
Whittaker model, 1508, 1521, 1551
witness property, 17
Witt coordinate, 450
Witt index, 1174
Witt polynomial, 449
Witt ring, 1175
Witten \(\zeta\)-functions, 1606
Witten complex, 1080
Wu class, 329

Yoneda extension, 227
Zariski, 908
Zariski localization, 277, 740
Zariski open subset, 1382
Zariski pair, 395
Zariski site, 503
Zariski space, 273
Zariski topology, 503
Zelevinsky condition, 1518
Zelevinsky segment, 1517
zero, 939
zero element, 197, 198
zero object, 166
Zeta function, 1601
Zeta-function, 1294